User Guide

AWS Cost Management

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Cost Management: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Use AWS Billing and Cost Management for AWS 1
Features of AWS Billing and Cost Management 1
Billing and payments 1
Cost analysis 2
Cost organization 2
Budgeting and planning 3
Savings and commitments 3
Related services 3
AWS Billing Conductor 3
IAM 4
AWS Organizations 5
Billing transfer 5
AWS Price List API 6
Getting started with AWS Cost Management 6
Sign up for an AWS account 6
Attach the required IAM policy to an IAM identity 6
Reviewing your bills and usage 6
Setting up your AWS Cost Management features 7
What do I do next? 7
Using the console home page 9
Managing Billing and Cost Management widgets 10
Cost summary 10
Cost monitor 11
Cost breakdown 12
Recommended actions 13
Cost allocation coverage 14
Savings opportunities 15
Top trends 15
Knowing the differences between Billing and Cost Explorer data 16
Understanding recommended action types 18
Controlling cost management data access with Billing View 25
Getting started with custom billing views 31
Creating custom billing views 32
Sharing custom billing views 35

Managing custom billing views ... 37
Accessing data using custom billing views ... 43
Visualizing and analyzing cost and usage data using Dashboards ... 48
Getting started with dashboards ... 50
Managed Dashboards ... 54
Creating custom dashboards ... 58
Adding widgets to dashboards ... 59
Exporting dashboards ... 64
Scheduling email delivery of dashboard reports ... 66
Sharing dashboards ... 74
Managing dashboards ... 75
Analyzing your costs and usage with AWS Cost Explorer ... 79
Enabling Cost Explorer ... 80
Getting started with Cost Explorer ... 85
Exploring your data using Cost Explorer ... 86
Asking questions about your costs using Amazon Q Developer ... 111
Comparing your costs between time periods ... 115
Exploring more data for advanced cost analysis ... 124
Using the AWS Cost Explorer API ... 132
Understanding your costs using Cost Explorer reports ... 134
Using the default Cost Explorer reports ... 134
Creating a Cost Explorer report ... 142
Viewing a Cost Explorer report ... 143
Editing a Cost Explorer report ... 143
Deleting a Cost Explorer report ... 144
Saving your configuration ... 145
Downloading the cost data CSV file ... 145
Managing your costs with AWS Budgets ... 146
Best practices for AWS Budgets ... 148
Creating a budget ... 153
Viewing your budgets ... 175
Editing a budget ... 177
Downloading a budget ... 178
Copying a budget ... 178
Deleting a budget ... 179
Configuring budget actions ... 179

Creating an Amazon SNS topic for budget notifications ... 185
Adding email recipients to a budget notification ... 188
Receiving budget alerts in chat applications ... 192
Reporting your metrics with AWS Budgets Reports ... 195
Creating an AWS Budgets report ... 196
Editing an AWS Budgets report ... 197
Copying an AWS Budgets report ... 197
Deleting an AWS Budgets report ... 198
Detecting unusual spend with AWS Cost Anomaly Detection ... 198
Setting up your anomaly detection ... 200
Controlling access for Cost Anomaly Detection ... 201
Getting started with AWS Cost Anomaly Detection ... 204
Transitioning from customer to AWS managed monitors ... 217
Editing your alert preferences ... 219
Creating an Amazon SNS topic for anomaly notifications ... 220
Receiving anomaly alerts in chat applications ... 226
Using EventBridge with Cost Anomaly Detection ... 229
Using AWS User Notifications with Cost Anomaly Detection ... 230
Opting out of Cost Anomaly Detection ... 234
Investigating anomaly root causes with Amazon Q Developer ... 235
Identifying opportunities with Cost Optimization Hub ... 239
Getting started with Cost Optimization Hub ... 241
Customizing your Cost Optimization Hub preferences ... 250
Viewing your cost optimization opportunities ... 253
Understanding your cost efficiency metric ... 255
Prioritizing your cost optimization opportunities ... 257
Understanding cost optimization strategies ... 258
Viewing your savings opportunities ... 263
Estimating monthly savings ... 266
Supported resources ... 267
Optimizing your cost with rightsizing recommendations ... 268
Getting started with rightsizing recommendations ... 269
Using your rightsizing recommendations ... 269
Sharing your rightsizing recommendations ... 271
Understanding rightsizing recommendations calculations ... 273
Understanding reservations in Cost Explorer ... 275

Accessing reservation recommendations ... 276
Generating estimates with Pricing Calculator ... 290
In-console AWS Pricing Calculator and the public Pricing Calculator ... 290
Features of the in-console AWS Pricing Calculator ... 290
Pricing for AWS Pricing Calculator ... 291
Getting started with AWS Pricing Calculator ... 292
Understanding AWS Pricing Calculator concepts ... 293
Understanding rates, discounts, and purchase commitments ... 295
Workload estimates ... 300
Bill estimates ... 306
Exporting your estimates ... 319
Using EventBridge with AWS Pricing Calculator ... 320
Managing your costs with Amazon Q Developer ... 323
Overview ... 323
How it works ... 331
Security and privacy ... 336
Managing your costs with Savings Plans ... 341
Using AWS Billing and Cost Management console with our new AWS experience ... 342
Use a budget ... 343
Budget considerations ... 344
Budget actions ... 344
Best practices ... 345
Create a budget ... 346
Update a budget ... 347
Budget methods ... 348
Budget filters ... 349
View your budget ... 352
Use Cost Explorer ... 354
Forecasting your data for Cost Explorer with our new AWS experience ... 354
Considerations ... 355
Access your cost data ... 356
Explore your data ... 357
Filter your data ... 358
Download the cost data CSV file ... 368
Ask questions about your costs using Amazon Q Developer ... 369
Cost comparisons ... 370

Troubleshoot Cost Explorer ... 371
View your savings opportunities ... 372
Supported resources ... 373
Download your recommendations ... 374
Security ... 375
Data protection ... 376
Identity and Access Management ... 377
User types and billing permissions ... 377
Audience ... 377
Authenticating with identities ... 379
Managing access using policies ... 381
Overview of managing access ... 382
How AWS Cost Management works with IAM ... 385
Identity-based policy examples ... 390
Using IAM policies for AWS Cost Management ... 393
AWS Cost Management policy examples ... 419
Migrating access control ... 441
Cross-service confused deputy prevention ... 456
Troubleshooting ... 457
Service-linked roles ... 460
Using service-linked roles ... 460
AWS managed policies ... 472
Logging and monitoring ... 473
AWS Cost and Usage Reports ... 473
AWS Cost Explorer ... 474
AWS Budgets ... 474
AWS CloudTrail ... 474
AWS Pricing Calculator ... 474
Logging AWS Cost Management API calls with AWS CloudTrail ... 475
Compliance validation ... 492
Resilience ... 492
Infrastructure security ... 493
Quotas and restrictions ... 494
Budgets ... 494
Budget reports ... 495
Cost Explorer ... 495

AWS Cost Anomaly Detection 495
AWS Pricing Calculator 497
Billing View 497
AWS Billing and Cost Management Dashboards 497
Document history 499

Use AWS Billing and Cost Management for AWS

Welcome to the AWS Cost Management User Guide.

AWS Billing and Cost Management provides a suite of features to help you set up your billing, retrieve and pay invoices, and analyze, organize, plan, and optimize your costs.

To get started, set up your billing to match your requirements. For individuals or small organizations, AWS will automatically charge the credit card provided.

For larger organizations, you can use AWS Organizations to consolidate your charges across multiple AWS accounts. You can then configure invoicing, tax, purchase order, and payment methods to match your organization's procurement processes.

If you have multiple AWS Organizations, use billing transfer to centrally manage and pay for all your organizations from a single account.

You can allocate your costs to teams, applications, or environments by using cost categories or cost allocation tags, or using AWS Cost Explorer. You can also export data to your preferred data warehouse or business intelligence tool.

See the following overview of features to help you manage your cloud finances.

Features of AWS Billing and Cost Management

Topics

- Billing and payments
- Cost analysis
- Cost organization
- Budgeting and planning
- Savings and commitments

Billing and payments

Understand your monthly charges, view and pay invoices, and manage preferences for billing, invoices, tax, and payments.

- **Bills page** – Download invoices and view detailed monthly billing data to understand how your charges were calculated.
- **Purchase orders** – Create and manage your purchase orders to comply with your organization's unique procurement processes.
- **Payments** – Understand your outstanding or past-due payment balance and payment history.
- **Payment profiles** – Set up multiple payment methods for different AWS service providers or parts of your organization.
- **Credits** – Review credit balances and choose where credits should be applied.
- **Billing preferences** – Enable invoice delivery by email and your preferences for credit sharing, alerts, and discount sharing.
- **Billing transfer** – Separates billing and financial management from security and governance management. This enables a single AWS organization to get centralized access to cost data and AWS invoices across multiple AWS organizations.

Cost analysis

Analyze your costs, export detailed cost and usage data, and forecast your spending.

- **AWS Cost Explorer** – Analyze your cost and usage data with visuals, filtering, and grouping. You can forecast your costs and create custom reports.
- **Data exports** – Create custom data exports from Billing and Cost Management datasets.
- **Cost Anomaly Detection** – Set up automated alerts when AWS detects a cost anomaly to reduce unexpected costs.
- **AWS Free Tier** – Monitor current and forecasted usage of free tier services to avoid unexpected costs.
- **Split cost allocation data** – Enable detailed cost and usage data for shared Amazon Elastic Container Service (Amazon ECS) resources.
- **Cost Management preferences** – Manage what data that member accounts can view, change account data granularity, and configure cost optimization preferences.

Cost organization

Organize your costs across teams, applications, or end customers.

- **Cost categories** – Map costs to teams, applications, or environments, and then view costs along these dimensions in Cost Explorer and data exports. Define split charge rules to allocate shared costs.
- **Cost allocation tags** – Use resource tags to organize, and then view costs by cost allocation tag in Cost Explorer and data exports.

Budgeting and planning

Estimate the cost of a planned workload, and create budgets to track and control costs.

- **Budgets** – Set custom budgets for cost and usage to govern costs across your organization and receive alerts when costs exceed your defined thresholds.
- **In-console Pricing calculator** – Use this feature to estimate your planned cloud costs using your discount and purchase commitments.
- **Public Pricing calculator website** – Create cost estimates for using AWS services with On-Demand rates.

Savings and commitments

Optimize resource usage and use flexible pricing models to lower your bill.

- **AWS Cost Optimization Hub** – Identify savings opportunities with tailored recommendations including deleting unused resources, rightsizing, Savings Plans, and reservations.
- **Savings Plans** – Reduce your bill compared to On-Demand prices with flexible pricing models. Manage your Savings Plans inventory, review purchase recommendations, run purchase analyses, and analyze Savings Plans utilization and coverage.
- **Reservations** – Reserve capacity at discounted rates for Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon DynamoDB, and more.

Related services

AWS Billing Conductor

Billing Conductor is a custom billing service that supports the showback and chargeback workflows of AWS Partners reselling AWS services, solutions, and AWS customers purchasing cloud services

directly through AWS. You can customize a second, alternative version of your monthly billing data. The service models the billing relationship between you and your customers or business units.

Billing Conductor doesn't change the way that you're billed by AWS each month. Instead, you can use the service to configure, generate, and display rates to specific customers over a given billing period. You can also use it to analyze the difference between the rates that you apply to your groupings relative to the actual rates for those same accounts from AWS.

As a result of your Billing Conductor configuration, the management account can also see the custom rate that's applied on the billing details page of the AWS Billing and Cost Management console. The management account can also configure AWS Cost and Usage Reports per billing group.

When billing transfer users sign in to the bill transfer account, Billing Conductor enables the management account of the AWS organization that transfers their bills (bill source account) to view only their usage priced with the rates from the bill transfer account.

For more information about Billing Conductor, see the AWS Billing Conductor User Guide. For more information about billing transfer, see Transfer billing management to external accounts.

IAM

You can use AWS Identity and Access Management (IAM) to control who in your account or organization has access to specific pages on the Billing and Cost Management console. For example, you can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits. IAM is a feature of your AWS account. You don't need to do anything else to sign up for IAM and there's no charge to use it.

When you create an account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform.

For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

By default, IAM users and roles in your account can't access the Billing and Cost Management console. To grant access, enable the **Activate IAM Access** setting. For more information, see About IAM Access.

If you have multiple AWS accounts in your organization, you can manage linked account access to Cost Explorer data by using the **Cost Management preferences** page. For more information, see Controlling access to Cost Explorer.

For more information about IAM, see the IAM User Guide.

AWS Organizations

You can use the consolidated billing feature in Organizations to consolidate billing and payment for multiple AWS accounts. Every organization has a *management account* that pays the charges of all the *member accounts*.

Consolidated billing has the following benefits:

- **One bill** – Get one bill for multiple accounts.
- **Easy tracking** – Track charges across multiple accounts and download the combined cost and usage data.
- **Combined usage** – Combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instances discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts. For more information, see Volume discounts.
- **No extra fee** – Consolidated billing is offered at no additional cost.

For more information about Organizations, see the AWS Organizations User Guide.

Billing transfer

You can use billing transfer to centrally manage and pay for multiple AWS Organizations from a single account.

Billing transfer allows a management account to designate an external management account to manage and pay for its consolidated bill. This centralizes billing while maintaining security management autonomy. To set up billing transfer, an external account (bill transfer account) sends a billing transfer invitation to a management account (bill source account). If the invitation is accepted, the external account becomes the bill transfer account. The bill transfer account then manages and pays for the bill source account's consolidated bill, starting on the date specified in the invitation.

For more information, see Transfer billing management to external accounts.

AWS Price List API

AWS Price List API is a centralized catalog that you can programmatically query AWS for services, products, and pricing information. You can use the bulk API to retrieve up-to-date AWS service information in bulk, available in both JSON and CSV formats.

For more information, see What is AWS Price List API?.

Getting started with AWS Cost Management

This section provides information that you need to get started with using the AWS Cost Management console. As a first step, you need to sign up for an AWS account and set up IAM users.

Sign up for an AWS account

To get started with AWS, you need an AWS account. For information about creating an AWS account, see Getting started with an AWS account in the *AWS Account Management Reference Guide*.

Attach the required IAM policy to an IAM identity

AWS account owners can provide permissions to specific users who need to view or manage the Billing and Cost Management data for an AWS account. To start activating access to the Billing and Cost Management console, see IAM tutorial: Delegate access to the billing console in the *IAM User Guide*.

For more information about IAM policies specific to Billing and Cost Management, see Using identity-based policies (IAM policies) for Billing and Cost Management.

For a list of Billing and Cost Management policy examples, see Billing and Cost Management policy examples.

Reviewing your bills and usage

Use features in the Billing and Cost Management console to view your current AWS charges and AWS usage.

To open the Billing and Cost Management console and view your usage and charges

1. Sign into the AWS Management Console and open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Choose **Bills** to see the details for your current charges.

   Choose **Payments** to see your historical payment transactions.

   Choose **Data Exports** to create exports of your billing and cost management data, such as cost and usage or cost optimization recommendations.

For information about Billing console features, see the AWS Billing User Guide.

For more information about setting up and using AWS Data Exports, see the AWS Data Exports User Guide.

Setting up your AWS Cost Management features

Review the process that's needed to activate your AWS Cost Management features.

- **AWS Cost Explorer**: Enabling Cost Explorer
- **AWS Budgets**: Best practices for AWS Budgets
- **AWS Budgets reports**: Reporting your metrics with AWS Budgets Reports
- **AWS Cost Anomaly Detection**: Setting up your anomaly detection
- **Cost Optimization Hub**: Getting started with Cost Optimization Hub
- **Savings Plans**: Getting started with Savings Plans in the *Savings Plans User Guide*
- **AWS Pricing Calculator**: Generating estimates with Pricing Calculator

What do I do next?

Now that you have AWS Cost Management set up, you're ready to use the features available to you. The rest of this guide helps you navigate your journey using the console.

Using the Billing and Cost Management API

Use the AWS Billing and Cost Management API Reference to programmatically use some AWS Cost Management features.

Learn more

You can find more information about AWS Cost Management features including presentations, virtual workshops, and blog posts on the Cloud Financial Management with AWS page.

You can find virtual workshops by choosing the **Services** drop-down and selecting your feature.

Getting help

There are several resources that you can use if you want to learn more about or need help with any of the AWS Cost Management features.

AWS Knowledge Center

All AWS account owners have access to account and billing support free of charge. You can find answers to your questions quickly by visiting the AWS Knowledge Center.

To find your question or request

1. Open AWS Knowledge Center.
2. Choose **Billing Management**.
3. Scan the list of topics to locate a question that is similar to yours.

Contacting Support

Contacting Support is the fastest and most direct method for communicating with an AWS associate about your questions. Support doesn't publish a direct phone number for reaching a support representative. You can use the following process to have an associate reach out to you by email or phone instead.

Only personalized technical support requires a support plan. For more information, visit Support.

To open an Support case where you specify *Regarding: Account and Billing Support*, you must either be signed into AWS as the root account owner, or have IAM permissions to open a support case. For more information, see Accessing Support in the *Support User Guide*.

If you closed your AWS account, you can still sign in to Support and view past bills.

To contact Support

1. Sign in and navigate to the Support Center.

2. Choose **Create case**.
3. On the **Create case** page, choose **Account and billing** and fill in the required fields on the form.
4. After you complete the form, under **Contact options**, choose either **Web** for an email response or **Phone** to request a telephone call from an Support representative. Instant messaging support isn't available for billing inquiries.

To contact Support when you can't sign in to AWS

1. Recover your password or submit a form at AWS account support.
2. Choose an inquiry type in the **Request information** section.
3. Fill out the **How can we help you?** section.
4. Choose **Submit**.

> **Note**
>
> When you use billing transfer, contact the bill transfer account owner first because they control your cost data and receive your AWS invoices. To find the bill transfer account information, go to the **Bill transfer** page, **Outbound billing** tab.

Using the AWS Billing and Cost Management home page

Use the Billing and Cost Management home page for an overview of your AWS cloud financial management data and to help you make faster and more informed decisions. Understand high-level cost trends and drivers, quickly identify anomalies or budget overruns which require your attention, review recommended actions, understand cost allocation coverage, and identify savings opportunities.

The data on this page comes from AWS Cost Explorer. If you haven't used Cost Explorer before, it's *automatically* enabled for you once you visit this page. It can take up to 24 hours for your data to appear on this page. When available, your data will be refreshed at least once every 24 hours. The Cost Explorer data on the home page is tailored for analytical purposes. This means the data can differ from your invoices and the **Bills** page due to differences in how data is grouped into AWS services; how discounts, credits, refunds, and taxes are displayed; differences in timing for the current month's estimated charges; and rounding.

For more information, see Knowing the differences between Billing and Cost Explorer data.

For more information about AWS Cloud Financial Management, see the Getting started page in the AWS Billing and Cost Management console. You can choose a topic and then follow the links to that specific console page or the documentation.

Managing Billing and Cost Management widgets

You can customize how the widgets appear by moving or resizing the widgets.

To manage the Billing and Cost Management widgets

1. Open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement.
2. (Optional) To customize the Billing and Cost Management home page, drag and drop a widget to move it, or change the widget size.
3. To take action on each recommendation or to learn more, review the data in the widget and then follow the links in the widget.
4. To reset the layout, choose **Reset layout** and then choose **Reset**.

You can use the following widgets:

- Cost summary
- Cost monitor
- Cost breakdown
- Recommended actions
- Savings opportunities
- Top trends

Cost summary

The cost summary widget provides a quick view of your current cost trends compared to your spending in the last month.

To view your month-to-date estimated charges on the **Bills** page, choose **View bill**.

All metrics shown in the cost summary widget exclude credits and refunds. This means you might see different numbers on the home page compared to the **Bills** page or your invoices. The widget shows the following metrics that you can choose to view in Cost Explorer:

- **Month-to-date cost** – Your estimated costs for the current month. The trend indicator compares the current month's costs to last month's cost for the same time period.
- **Last month's cost for same time period** – Your costs for last month, for the same time period. For example, if today is February 15, the widget also shows last month's cost for January 1–15.

> **Note**
>
> Trend calculations might be influenced by the number of days in each month. For example, on July 31, the trend indicator will look at costs from July 1–31 and compare it to costs for June 1–30.

- **Total forecasted cost for current month** – A forecast of your estimated total costs for the current month.
- **Last month's total cost** – The total costs for last month. For more information, choose each metric to view the costs in Cost Explorer, or choose **View bill** to view your month-to-date estimated charges on the **Bills** page.

> **Note**
>
> The metrics in this widget exclude credits and refunds. The costs here might differ from the costs on the **Bills** page or your invoices.

For more information about Cost Explorer, see Forecasting with Cost Explorer.

Cost monitor

This widget provides a quick view of your cost and usage budgets and any cost anomalies that AWS detected, so that you can fix it.

- **Budgets status** – Alerts you if any of your cost and usage budgets were exceeded.

  The status can be the following:

- **OK** – Cost and usage budgets haven't been exceeded.

- **Over budget** – A cost and usage budget has been exceeded. Your actual cost is greater than 100%. The number of exceeded budgets and a warning icon will appear.
- **Setup required** – You haven't created any cost and usage budgets.

Choose the status indicator to go to the **Budgets** page to review details of each budget or to create one. The budgets status indicator only shows information about cost and usage budgets. Budgets that you created to track the coverage or utilization of your Savings Plans or reservations won't appear in this widget. Cost anomalies status alerts you if AWS detected any anomalies with your costs since the first day of the current month. The status can be the following:

- **OK** – Cost anomalies haven't been detected in the current month.
- **Anomalies detected** – A cost anomaly has been detected. The number of anomalies detected and a warning icon will appear.
- **Setup required** – You haven't created any anomaly detection monitors.

Choose the status indicator to go to the **Cost Anomaly Detection** page to review details of each anomaly detected, or to create an anomaly detection monitor. The cost anomalies status indicator only displays information about cost anomalies detected in the current month. To view your full anomaly history, go to the **Cost Anomaly Detection** page.

For more information about budgets, see Managing your costs with AWS Budgets.

For more information about anomaly detection monitors, see Detecting unusual spend with AWS Cost Anomaly Detection.

Cost breakdown

This widget provides a breakdown of your costs for the last six months, so you can understand cost trends and drivers. To break down your costs, choose an option from the dropdown list:

- Service
- AWS Region
- Member account (for AWS Organizations management accounts)
- Cost allocation tag
- Cost category

If you choose cost category or cost allocation tag key, hover over the chart to see the values.

To dive deeper into your cost and usage, choose **Analyze your costs in Cost Explorer**. Use Cost Explorer to visualize, group, and filter your costs and usage, with additional dimensions, such as Availability Zone, instance type, and database engine.

For more information about Cost Explorer, see Exploring your data using Cost Explorer.

Recommended actions

This widget helps you implement AWS cloud financial management best practices and optimize your costs. It displays your recommended actions, ranked by priority. Critical alerts appear at the top, followed by advisory warnings and informational recommended actions.

As a best practice, we recommend that you monitor any critical alerts daily, focusing on immediate actions like payment issues or budget overruns. Review any advisory warnings on a weekly basis.

To use the recommended actions widget

1. For each recommendation, follow the link to take action on your account. By default, the widget shows up to four recommended actions.
2. To load additional recommended actions, choose **Load more actions**.
3. To dismiss a non-critical recommended action, choose the **X** icon on the top right corner. Critical alerts remain visible until addressed. Dismissed non-critical recommended actions will reappear after 7 days.

> **Note**
>
> You will need IAM permissions to the AWS service in order to see the recommended actions. For example, if you have access to all Billing and Cost Management actions except `budgets:DescribeBudgets`, you can view all recommendations on the page except for budgets. See the error message about adding the missing IAM action to your policy.
> You will need the new IAM permission `bcm-recommended-actions:ListRecommendedActions` to view all recommended actions. For more information, see Understanding recommended action types.
> For a full list of the different recommended action types and the corresponding IAM policy permissions needed in order to see the recommended actions, refer to Billing and Cost Management recommended actions policies.

For full details on the categorization of recommended actions, see Understanding recommended action types.

Cost allocation coverage

To create cost visibility and accountability in your organization, it's important to allocate costs to teams, applications, environments, or other dimensions. This widget shows unallocated costs for your cost categories and cost allocation tags, so that you can identify where to take action to organize your costs.

Cost allocation coverage is defined as the percentage of your costs that don't have a value assigned to the cost category or cost allocation tag keys that you've created.

Example

- Your month-to-date spend is $100, and you created a cost category (named *Teams*) to organize costs by individual teams.
- You have $40 in the *Team A* cost category value, $35 in the *Team B* cost category value, and $25 that are unallocated.
- In this case, your cost allocation coverage is 25/100 = 25%.

A lower unallocated cost metric means that your costs are properly allocated along the dimensions important to your organization. For more information, see Building a cost allocation strategy in the *Best Practices for Tagging AWS Resources* whitepaper.

This widget compares the month-to-date unallocated cost percentage to all of last month's unallocated cost percentage. The widget shows up to five cost allocation tag keys or five cost categories. If you have more than five of either cost allocation tag keys or cost categories, use the widget preferences to specify the ones that you want.

To analyze your unallocated costs in more detail by using Cost Explorer, choose the cost category or cost allocation name.

To improve cost allocation coverage for your cost categories or cost allocation tags, you can edit your cost category rules or improve resource tagging by using AWS Tag Editor.

For more information, see the following topics:

- Managing your costs with AWS cost categories

- Using AWS cost allocation tags
- Using Tag Editor

Savings opportunities

This widget shows recommendations from Cost Optimization Hub to help you save money and lower your AWS bill. This can include:

- Deleting unused resources
- Rightsizing over-provisioned resources
- Purchasing Savings Plans or reservations

For each savings opportunity, the widget shows your estimated monthly savings. Your estimated savings are *de-duplicated* and *automatically* adjusted for each recommended savings opportunity.

Example

- Let's say that you have two Amazon EC2 instances, *InstanceA* and *InstanceB*.
- If you purchased a Savings Plan, you could reduce the cost for *InstanceA* by $20 and the cost of *InstanceB* by $10, for a total of $30 savings.
- However, if *InstanceB* is idle, the widget might recommend that you terminate it instead of purchasing a Savings Plan. The savings opportunity would tell you how much you could save by terminating the idle *InstanceB*.

To view the savings opportunities in this widget, you can opt in by visiting the Cost Optimization Hub page or using the Cost Management preferences page.

When you use billing transfer, savings opportunities are calculated based on On-Demand costs (costs without negotiated discounts, AWS Partner Network program discounts, or Reserved Instance and Savings Plans discounts). To learn about cost optimization best practices while billing transfer is active, see Transfer billing management to external accounts.

Top trends

This widget provides a quick overview of your most significant cost changes between the previous two months.

- Shows the top 10 cost variations, sorted by absolute dollar difference
- Displays both percentage and absolute value changes
- Highlights specific services, accounts, or Regions where changes occurred
- Allows you to choose any trend to analyze it further in Cost Explorer's Compare view

To dive deeper into your cost trends, choose **View your cost trends in Cost Explorer**.

For more information about comparing costs, see Comparing your costs between time periods.

Knowing the differences between Billing and Cost Explorer data

Billing data

Your billing data appears on the **Bills** and **Payments** pages of the AWS Billing and Cost Management console, and in the invoice that AWS issues to you. Billing data helps you understand the actual invoiced charges for previous billing periods, and the estimated charges that you've accrued for the current billing period, based on your month-to-date service usage. Your invoice represents the amount that you owe to AWS.

Cost Explorer data

Your Cost Explorer data appears in the following places:

- The Billing and Cost Management home page
- The pages for Cost Explorer, Budgets, and Cost Anomaly Detection
- Your reports for coverage and usage

Cost Explorer supports deep-dive analysis so that you can identify savings opportunities. Cost Explorer data provides more granular dimensions (such as Availability Zone or operating system) and includes features that might show differences when compared to billing data. On the **Cost Management** preferences page, you can manage your preferences for Cost Explorer data, including linked account access and historical and granular data settings. For more information, see Controlling access to Cost Explorer.

Amortized costs

Billing data is always presented on a *cash* basis. It represents the amount that AWS charges you each month. For example, if you purchase a one-year, all-upfront Savings Plan in September, AWS

will charge you the full cost for that Savings Plan in the September billing period. Your billing data will then include the full cost of that Savings Plan in September. This helps you understand, validate, and pay your AWS invoices on time.

In contrast, you can use Cost Explorer data to view amortized costs. When costs are amortized, an upfront charge is spread, or *amortized* over the life of that agreement. In the previous example, you can use Cost Explorer for an amortized view of your Savings Plan. A one-year, all-upfront Savings Plan purchase will be spread evenly across the 12 months of the commitment term. Use amortized costs to gain insight into the effective daily costs associated with your portfolio of reservations or Savings Plans.

AWS service grouping

With billing data, your AWS charges are grouped into AWS services on your invoice. To help with deep-dive analysis, Cost Explorer will group some costs differently.

For example, let's say that you want to understand compute costs for Amazon Elastic Compute Cloud compared to ancillary cost, such as Amazon Elastic Block Store volumes or NAT gateways. Instead of a single group for Amazon EC2 costs, Cost Explorer will group costs into **EC2 - Instances** and **EC2 - Other**.

In another example, to help analyze data transfer costs, Cost Explorer groups your transfer costs by service. In billing data, data transfer costs are grouped into a single service named **Data Transfer**.

Estimated charges for the current month

Your billing data and Cost Explorer data are refreshed at least once per day. The cadence when they're refreshed might differ. This can result in differences for your month-to-date estimated charges.

Rounding

Your billing data and Cost Explorer data are processed at different granularities. For example, Cost Explorer data is available with hourly and resource-level granularity. Billing data is monthly and doesn't offer resource-level details. As a result, your billing data and Cost Explorer data might vary due to rounding. When these data sources are different, the amount on your invoice is the final amount that you owe to AWS.

Presentation of discounts, credits, refunds, and taxes

The billing data on the **Bills** page (for example, in the **Charges by service** tab) excludes refunds, while Cost Explorer data includes refunds. When a refund is issued, this might cause differences in other charge types.

For example, let's say that a portion of your taxes was refunded. On the **Bills** page, the **Taxes by service** tab will continue to show the full tax amount. The Cost Explorer data will show the post-refund tax amount.

If you use billing transfer and sign in to the Billing and Cost Management console with a bill source account, you can't view credits, refunds, or taxes in the **Bills** page, Cost Explorer, or AWS Cost and Usage Report."

Understanding recommended action types

Recommended actions automatically identify and prioritize the most important actions you should take related to Billing and Cost Management, regarding budgets, payments, cost optimization, cost anomalies, IAM permissions, and tax settings.

Recommended actions are categorized into three levels based on urgency, financial impact, and account relevance.

1. **Critical alerts**: These are high-priority items that could impact your account standing, such as past due payments or expired payment methods.
2. **Advisory warnings**: These are important notifications about your configured resources like budgets, tax settings, and credits that help you identify opportunities to save costs.
3. **Informational**: These are best practices and optimization opportunities to improve your cloud financial management.

The following table provides an overview of the different recommended actions, organized by severity and feature.

> **Note**
>
> * These action types are always visible. Additional action types require the `bcm-recommended-actions:ListRecommendedActions` permission. For more information, see Billing and Cost Management recommended actions policies.

Severity	Feature	Action type	Recommended action	Example
Critical alerts	PAYMENTS	Payments past due	Make a payment	You have USD $603.23, EUR €50.02 past due. To avoid potential disruption in using AWS services, please make a payment.
	PAYMENTS	Invalid payment method	Verify payment method	Your default payment method is invalid. To avoid payment failures and potential disruption in using AWS services, please contact your bank to determine the reason and visit the payments page to verify your payment method.
	PAYMENTS	Expired payment method	Review your payment configurations and update your	Your default payment method expired. To avoid failed payments

Severity	Feature	Action type	Recommended action	Example
			default payment method.	for invoices and potential disruption to your AWS services, update the card information or switch to a different payment method.
	IAM	Update permissions for recommended actions*	Contact your administrator to add new IAM permissions for your role.	You need a new IAM permission to view the full list of recommended actions: `bcm-recommended-actions:ListRecommendedActions` .
Advisory warnings	TAX_SETTINGS	Fix tax registration information	Review your tax settings and update your tax registration number.	Your tax registration ID is invalid.

Severity	Feature	Action type	Recommended action	Example
	TAX_SETTINGS	Update tax exemption certificate	Review your tax settings and update your tax exemption certificate.	You have 2 tax exemption certificates that are expired or expiring within 30 days.
	IAM	Migrate to granular permissions*	Migrate to Billing and Cost Management granular permissions.	Migrate to the new IAM permissions to avoid losing access to future Billing and Cost Management launches.
	BUDGETS	Review budget alerts*	Review your budgets and alert thresholds. You can also identify cost savings opportunities by visiting Cost Optimization Hub.	5 of your budget alerts have exceeded their threshold.

Severity	Feature	Action type	Recommended action	Example
	BUDGETS	Review budgets exceeded*	Review your budgets values. You can also identify cost savings opportunities by visiting Cost Optimization Hub.	7 of your budgets have exceeded their threshold and 2 of your budgets are forecasted to exceed their threshold.
	FREE_TIER	Review Free Tier usage alerts*	Review your Free Tier usage to prevent any cost surprises.	You have exceeded 85% of the Free Tier usage limit for 3 services.
	COST_ANOMALY_DETECTION	Review anomalies*	Review your cost anomaly monitors and associated thresholds. You can also identify cost savings opportunities by visiting Cost Optimization Hub.	2 cost anomalies detected in the last 90 days with a total cost impact of $1,000.

Severity	Feature	Action type	Recommended action	Example
	RESERVATIONS	Review expiring reservations*	Review your expiring reserved instances and plan to make new purchases to optimize your workloads.	2 reservations expiring within 30 days.
	SAVINGS_PLANS	Review expiring Savings Plans*	Review your expiring Savings Plans and add any future purchases to the queue.	2 Savings Plans expiring within 30 days.
Informational	PAYMENTS	Payments due	Make a payment.	You have USD $603.23, EUR €50.02 due. To avoid potential disruption in using AWS services, please make a payment.
	COST_OPTIMIZATION_HUB	Review savings opportunity recommendations*	Review your savings opportunities by visiting Cost Optimization Hub.	Save $1000.00 by following savings opportunity recommendations.

Severity	Feature	Action type	Recommended action	Example
	COST_OPTIMIZATION_HUB	Enable Cost Optimization Hub*	Opt in to Cost Optimization Hub to start generating savings opportunity recommendations.	Opt in to start generating savings opportunity recommendations.
	BUDGETS	Create a budget*	Create a budget to monitor your cost and usage as well as commitment coverage and utilization.	Create a cost budget to receive alerts when your costs and usage exceed your budgeted amounts.
	BUDGETS	Create a Savings Plans budget*	Create a Savings Plans budget to monitor your commitment coverage and utilization.	Create a Savings Plans budget to monitor your Savings Plans commitment coverage and utilization.

Severity	Feature	Action type	Recommended action	Example
	BUDGETS	Create a reservation budget*	Create a reservation budget to monitor your commitment coverage and utilization.	Create a reservation budget to monitor your reserved instance commitment coverage and utilization.
	ACCOUNT	Add an alternate billing contact*	Add an additional billing contact.	Add an additional billing contact.
	COST_ANOMALY_DETECTION	Create an anomaly monitor*	Create a cost anomaly monitor to proactively identify any cost anomalies.	Create a cost anomaly monitor to automatically detect cost anomalies.

Controlling cost management data access with Billing View

Billing View is a feature that helps you manage and control access to cost management data within your AWS environment. With Billing View, cost management data is represented as an AWS resource. Through resource-based policies, you can configure what data is accessible to an account when using AWS Billing and Cost Management tools. A billing view is identified by a unique Amazon Resource Name (ARN), which can be referenced in identity-based policies to perform specific IAM actions on the cost management data contained in that billing view.

There are four different types of billing views:

Type	Description	Managed by	Shareable?
Primary billing view	By default, each account has access to its primary billing view, which contains all the cost management data associated with that account. For the management account of an organization, this includes all cost managemen t data incurred by all accounts within the organizat ion. For standalon e AWS accounts not using AWS Organizations, as well as for member accounts within an organization, the primary billing view contains all cost management data incurred within the individual account. When your account is part of a billing group (standard or billing transfer) , your primary view shows cost data	AWS	Not shareable with other accounts

Type	Description	Managed by	Shareable?
	controlled by either your management account or the bill transfer account.		
Billing group billing view	Accounts that have enabled AWS Billing Conductor also have access to billing group billing views, which correspond to each billing group. For more information about billing groups, see Billing groups in the *AWS Billing Conductor User Guide*.	AWS	Not shareable with other accounts

Type	Description	Managed by	Shareable?
Custom billing view	Customers can create and delete custom billing views that provide cost visibility across organizations. These billing views can be derived from primary billing views or other custom billing views, and combines cost management data from multiple accounts belonging to multiple organizations. Apply filters to specify which subset of cross-organizational data to include in your view.	Customer	Shareable with accounts within and outside your organization

Type	Description	Managed by	Shareable?
Billing transfer view	When you use billing transfer as a bill transfer account, you have access to billing transfer views from the time the transfer begins. Billing transfer includes two view types: - My view: Shows the billing data that your bill transfer account is financial ly responsible for - Showback/ chargeback view:Shows billing data configured for showback or chargeback purposes	AWS	Not shareable with other accounts

By using billing view, you can create custom billing views from your organization’s management (payer) account, which you can define to include a set of filtered cost management data you have access to. A custom billing view resource can then be shared with other accounts. When a custom billing view is shared with an account, that account can then access the cost management data defined in the custom billing view.

You can use custom billing views to grant end users and application owners access to relevant cost management data without requiring access to the management account. Customers with AWS Organizations enabled can create custom billing views containing a subset of cost management data from the management account's primary billing view, filtered by cost allocation tags or

accounts. You can also combine cost management data from multiple organizations into a single custom billing view.

Key benefits of using custom billing views include:

- **Streamlined access**: Enable business unit owners who manage multiple member accounts to access all of their cost management data without needing to access each account individually, saving end users time and eliminating the need for manual data aggregation.
- **Consolidated data:** Consolidate cost management data across multiple organizations. Enable central teams to have consolidated views of their cost management data across multiple organizations.
- **Reduced management account access**: Eliminate the need for end users to access the management account of your organization to access cost management data spanning multiple accounts.
- **Native AWS Cost Management access**: Empower end users across your organization to independently visualize, understand, and forecast their AWS spend using Cost Explorer and the AWS Billing and Cost Management home page.

By sharing custom billing views with other accounts, application owners can monitor their application-level AWS spend using Cost Explorer and AWS Budgets, and central teams can monitor their spend across multiple organizations. This eliminates the need for central teams to manually aggregate information across multiple organizations, and the need for end users to access the management account to access cost management data. The following sections guide you through the process of creating, sharing, managing, and using custom billing views.

Topics

- Getting started with custom billing views
- Creating custom billing views
- Sharing custom billing views
- Managing custom billing views
- Accessing cost management data using billing views

Getting started with custom billing views

Custom billing views in AWS Billing and Cost Management allow you to make cost management data accessible to accounts both inside and outside your organization. These views can only be created by the management account of an organization. By creating and sharing a custom billing view, you provide recipient accounts with access to specific cost management data. End users of the recipient account can then select from a list of shared custom billing views in the navigation pane. For example, you can define a custom billing view to contain all cost management data for a business unit that spans multiple member accounts. When shared with a relevant accounts, end users can monitor and analyze costs using Cost Explorer across all accounts and resources mapped to that business unit without requiring direct access to the management account. Additionally, you can consolidate cost management data across multiple organizations by creating a custom billing view that combines data from multiple shared billing views, enabling centralized cost monitoring.

Prerequisites

To create custom billing views, you must use fine-grained AWS Cost Management actions. For AWS Organizations users, you can use the bulk policy migrator scripts to update policies from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added. For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Console Permission blog. Fine-grained actions are already in effect if you have a standalone AWS account, or you're part of AWS Organizations created on or after March 6, 2023, 11:00AM (PDT).

To share custom billing views, you must access the management account of your organization using an IAM principal that has permissions to create and share resources using AWS Resource Access Manager (AWS RAM). Permissions are not required for member accounts who receive a shared custom billing view. When sharing a custom billing view outside of your organization, you must access the recipient account using an IAM principal that has permissions to accept resource invitation shares using AWS RAM. For details about IAM actions for sharing custom billing views, see How AWS RAM works with IAM in the *AWS Resource Access Manager User Guide*.

> **Note**
>
> Appropriate IAM actions must be enabled to create, update, delete, and share custom billing views. For more information about IAM actions for managing custom billing views, see Using identity-based policies (IAM policies) for AWS Cost Management.

Accessing the console to create custom billing views

There are two ways to access Billing View in the console to create custom billing views.

- From the console navigation pane: If you haven't yet created or don't have access to any custom billing views, you can access Billing View from the navigation pane.
- From Cost Management preferences: You can also access Billing View by navigating to Cost Management preferences.

To access Billing View

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Choose either of the following methods to begin creating your custom billing view:
   - From the console navigation pane:
     a. In the navigation pane, select the **Choose billing view** menu.
     b. Choose **Create new view** from the dropdown list.
   - From Cost Management preferences:
     a. In the navigation pane, choose **Cost Management Preferences**.
     b. Choose the **Billing View** tab.

Creating custom billing views

Custom billing views allow you to grant accounts, both within and outside of your organization, specific, controlled access to cost management data. A custom billing view contains a subset of the cost management data contained in your management account's primary billing view. Once created, these custom billing view resources can then be shared with the relevant accounts, enabling tailored data visibility across your organization. Additionally, you can consolidate cost management data across multiple organizations by creating a custom billing view that combines data from multiple shared custom billing views, enabling centralized cost monitoring across your entire enterprise. If you're using AWS Billing Conductor, a custom billing view contains cost management data based on your standard AWS bill, even when being accessed by an account belonging to a billing group.

> **Note**
>
> To create custom billing views, you must use fine-grained AWS Cost Management actions. For more information, see Prerequisites.

To create a custom billing view with your organization's data

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. Choose **Create view**.
5. Choose a single dimension to filter and specify the values to include in the custom billing view.
   - **Cost allocation tags**: This filter is recommended if you use cost allocation tags to organize and manage your spend. This field is restricted to one key, but allows multiple values within that key. For example, you can create a custom billing view containing all usage records with the cost allocation tag where the key is Cost Center and the values are 80432 or 78925. For more information about cost allocation tags, see Organizing and tracking costs using AWS cost allocation tags.
   - **Accounts**: This filter allows you to include cost management data for specific accounts in the custom billing view by selecting one or more account IDs. This is useful for creating custom billing views that focus on particular accounts or groups of accounts within your organization.
   - **No filter (all data):** This filter includes all cost management data from your organization.
6. For **Custom billing view name**, enter a short, descriptive name that helps users identify the custom billing view's data content. This helps users quickly understand the custom billing view's content when selecting it from the **Choose billing view** menu in the navigation pane.
7. (Optional) For **Custom billing view description**, enter details about the custom billing view's content. This description will be visible in the **Billing View** tab.
8. (Optional) Add a tag to your custom billing view. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.
   1. Choose **Add new tag**.
   2. Enter the key and value for the tag.

3. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.

9. Review your selections and choose **Create**. Once created, the custom billing view is assigned a unique Amazon Resource Name (ARN), which serves as its identifier.

To create a custom billing view with multiple sources

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. Choose **Create multi-source view**.
5. Choose up to 20 source views. Your new view will include the cost management data from each selected source view.
6. Choose **Next**.
7. Choose a single dimension to filter and specify the values to include in the custom billing view.

   - **Cost allocation tags**: This filter is recommended if you use cost allocation tags to organize and manage your spend. This field is restricted to one key, but allows multiple values within that key. For example, you can create a custom billing view containing all usage records with the cost allocation tag where the key is Cost Center and the values are 80432 or 78925. For more information about cost allocation tags, see Organizing and tracking costs using AWS cost allocation tags.
   - **Accounts**: This filter allows you to include cost management data for specific accounts in the custom billing view by selecting one or more account IDs. This is useful for creating custom billing views that focus on particular accounts or groups of accounts within your organization.
   - **No filter (all data):** This filter includes all cost management data from your organization.

8. For **Custom billing view name**, enter a short, descriptive name that helps users identify the custom billing view's data content. This helps users quickly understand the custom billing view's content when selecting it from the **Choose billing view** menu in the navigation pane.
9. (Optional) For **Custom billing view description**, enter details about the custom billing view's content. This description will be visible in the **Billing View** tab.

10. (Optional) Add a tag to your custom billing view. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.
    1. Choose **Add new tag**.
    2. Enter the key and value for the tag.
    3. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.
11. Choose **Next**.
12. Review your selections and choose **Create**. Once created, the custom billing view is assigned a unique Amazon Resource Name (ARN), which serves as its identifier.

After creating a custom billing view, it is only available in your account. You can access it from the **Choose billing view** menu in the navigation pane from your own account to access its contents using Cost Explorer. You can also see the custom billing view definition details in the **Billing View** tab on the **Cost Management Preferences** page. You can choose to share the custom billing view with other accounts. Shared accounts can access the custom billing view from the **Choose billing view** menu, allowing them to access the cost management data defined in the custom billing view. To learn more, see Sharing custom billing views.

Sharing custom billing views

You can share custom billing views with accounts within and outside your organization. Sharing is not supported for billing views of type “Primary” or “Billing group”.

> **Note**
>
> For member accounts within an organization to access a shared custom billing view using Cost Explorer, the management account must have granted them access to Cost Explorer. Member account access to discounts, credits, and refunds when accessing a shared custom billing view is determined by current Cost Explorer preferences, including Linked Account Access, Linked Account Refunds and Credits, and Linked Account Discounts. For more information, see Controlling access using Cost Explorer preferences.

To share a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the sharing page, do one of the following:
   - Select the custom billing view you want to share, and choose **Share view**.
   - Choose the name of the custom billing view you want to share and, on the view details page, choose the **Sharing** tab.
5. Choose **Share**.
6. You can share custom billing views with accounts within and outside of your organization. From **Select**:
   - Choose **Within AWS organization** to share with accounts within your organization.
   - Choose **With any account** to manually enter an account ID to share with.
7. Select a managed permission for the custom billing view. Managed permissions define how recipient accounts can interact with the shared resource. For more information about managed permissions, see Managing permissions in AWS RAM.
8. Select which accounts you want to share the custom billing view.
   - If sharing **Within AWS organization**, select member accounts to share with.
   - If sharing **With any account**, manually enter the 12-digit AWS account ID you want to share with. If sharing with an account outside your organization, the recipient must accept the invitation to access the view.
9. Select the member accounts in your organization that you want to share the custom billing view with.
10. Choose **Share**.

> **Note**
>
> Custom billing views use AWS Resource Access Manager (AWS RAM) for sharing. When you share a custom billing view, an AWS resource share is automatically created. You can directly share custom billing view resources with specific accounts in your organization

using AWS RAM. Only the management account needs permissions to share resources with AWS RAM, with no permissions required for member accounts receiving a shared resource. For more advanced use cases such as sharing with an entire AWS Organizational Unit or defining custom managed policies, create a resource share directly through AWS RAM. When a custom billing view has been shared with IAM principals, other than an AWS account, directly through AWS RAM, these shares are displayed under **Other principals shared with** in the **Sharing** tab on the view details page. Resource shares created directly through AWS RAM can only be managed in AWS RAM.

Once a custom billing view is shared, you can see which accounts have access to it from the **Sharing** tab on the view details page. Note that if you're using AWS Billing Conductor, a custom billing view contains cost management data based on your standard AWS bill, even when being accessed by an account belonging to a billing group. Additionally, you can view a list of all resource shares you've created in AWS RAM. For more information, see Viewing resource shares you created in AWS RAM.

You have the flexibility to edit the sharing permissions of a custom billing view at any time, allowing you to maintain control over who has access to your cost management data. For details, see Managing shared access to custom billing views.

Managing custom billing views

As the creator of a custom billing view, you retain full control over the resource even after sharing it with other accounts. You can update the definition of a custom billing view to reflect changes in your organization. You can also manage which accounts can access a custom billing view, or you can delete a custom billing view, which immediately revokes access to all accounts. Accounts that have been given access to the view can't modify the definition of the custom billing view. This ensures you retain full control over which accounts can access specific cost management data.

You can change the definition of an existing custom billing view at any time. Once edited, the updated custom billing view takes immediate effect. All accounts with access, including member accounts to which the custom billing view has been shared, will immediately see the cost management data based on the updated definition.

Topics

- Editing the filters of custom billing views
- Editing the sources of custom billing views

- Editing the tags of custom billing views
- Deleting custom billing views
- Managing shared access to custom billing views in your organization
- Understanding AWS managed billing views
- Managing shared access to custom billing views outside of your organization

Editing the filters of custom billing views

To edit the filters of a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the edit filters page, do one of the following:

   - Select the custom billing view you want to edit. Choose **Actions**, and then choose **Edit view** from the dropdown list.
   - Choose the billing view you want to edit. Choose the **Configuration details** tab, and then choose **Edit** next to **Data filtered by**.
5. On the **Edit view** page, change the filter dimension.
6. Choose **Save**.

Editing the sources of custom billing views

To edit the sources of a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the edit filters page, do one of the following:

- Select the custom billing view you want to edit. Choose **Actions**, and then choose **Edit view** from the dropdown list.
- Choose the billing view you want to edit. Choose the **Configuration details** tab, and then choose **Edit** next to **Data filtered by**.

5. On the **Edit sources** page, change the sources used in the view.
6. Choose **Save**.

Editing the tags of custom billing views

To edit the tags of a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the edit filters page, do one of the following:

   - Select the custom billing view you want to edit. Choose **Actions**, and then choose **Edit view** from the dropdown list.
   - Choose the billing view you want to edit. Choose the **Configuration details** tab, and then choose **Edit** next to **Data filtered by**.

5. On the **Manage tags** page, change the tags used for the view.
6. Choose **Save**.

Deleting custom billing views

Deleting a custom billing view permanently removes access to the custom billing view for all users. This action cannot be undone. Once a custom billing view is deleted, it will no longer appear in the **Choose billing view** menu in the navigation pane for the management account and any member accounts with which the view was shared. End users attempting to access the URL of the deleted custom billing view will receive an error message.

To delete a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. Select the custom billing view you want to delete.
5. Choose **Actions**, and then choose **Delete view** from the dropdown list.
6. In the dialog box that appears, choose **Delete**.

You can control which accounts can access a custom billing view by modifying its associated resource share. Once you add an account to the resource share, the account gains access to the custom billing view. Once you remove an account from the resource share, the account loses access to the custom billing view.

Managing shared access to custom billing views in your organization

> **Note**
>
> Custom billing views use AWS Resource Access Manager (AWS RAM) for sharing. When you share a custom billing view, an AWS resource share is automatically created. You can also directly modify the resource share from the AWS RAM console. For more information about modifying the resource share in AWS RAM, see Update a resource share in AWS RAM.

To edit who can access a custom billing view in your organization

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the sharing page, do one of the following:
   - Select the custom billing view whose sharing you want to update, choose **Actions**, and then choose **Edit shared accounts** from the dropdown list.

- Choose the name of the custom billing view whose sharing you want to update and, on the view details page, choose the **Sharing** tab.

5. In the **Sharing** tab, choose **Edit**.
6. Choose which member accounts in your organization should have access to the custom billing view.
7. Choose **Share**.

> **Note**
>
> AWS RAM also supports a single resource belonging to multiple resource shares. If a custom billing view belongs to multiple resource shares, you will see a drop-down within the Edit sharing page labeled Select a share listing all resource shares the currently selected custom billing view belongs to. By selecting a resource share, you will be able to modify which accounts should be included or excluded from the selected resource share.

Understanding AWS managed billing views

AWS managed billing views are created when you map accounts to Billing Conductor billing groups or use billing transfer.

There are two types of AWS managed billing views: Billing group views, and billing transfer billing views.

The two types of billing transfer billing views:

- My view - Shows the billing data that your bill transfer account is financially responsible for
- Showback/chargeback view - Shows billing data configured for showback or chargeback purposes

AWS creates and manages these billing views, so you can't update or delete them directly. The **Cost Management Preferences** billing view tab currently shows only custom views, not AWS managed views.

To update an AWS managed view name, update the name of its associated resource (billing group or billing transfer). AWS managed views persist even if their associated resource is deleted or withdrawn.

Managing shared access to custom billing views outside of your organization

> **Note**
>
> Custom billing views use AWS Resource Access Manager (AWS RAM) for sharing. When you share a custom billing view, an AWS resource share is automatically created. You can also directly modify the resource share from the AWS RAM console. For more information about modifying the resource share in AWS RAM, see Update a resource share in AWS RAM.

To edit who can access a custom billing view outside of your organization

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. Choose the **Billing View** tab.
4. To access the sharing page, do one of the following:
   - Select the custom billing view whose sharing you want to update, choose **Actions**, and then choose **Edit external shares** from the dropdown list.
   - Choose the name of the custom billing view whose sharing you want to update and, on the view details page, choose the **Sharing** tab. Next to **Share outside of your organization**, choose **Edit**.
5. Choose which account IDs should have access to the custom billing view.
6. Choose **Share**.

> **Note**
>
> AWS RAM also supports a single resource belonging to multiple resource shares. If a custom billing view belongs to multiple resource shares, you will see a drop-down within the Edit sharing page labeled Select a share listing all resource shares the currently selected custom billing view belongs to. By selecting a resource share, you will be able to modify which accounts should be included or excluded from the selected resource share.

Accessing cost management data using billing views

Custom billing views

If your account has access to a custom billing view, you can access the cost management data defined in that custom billing view. This is in addition to the cost management data owned by your account, which is contained in your primary billing view. The primary billing view supports all AWS Billing and Cost Management tools. To access the data in a custom billing view, you can use either Cost Explorer or the AWS Billing and Cost Management home page. Cost Explorer offers additional functionality with custom billing views, allowing you to create forecasts and access Cost Explorer Saved Reports based on the data.

To choose a custom billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, select the **Choose billing view** menu. The default selection is the **Primary view**, which represents cost management data for the account you're currently logged in to.
3. From the **Custom views** section of the dropdown list, choose the custom billing view you want to use for accessing cost management data.
4. If the custom billing view you want to access is not listed, choose **See all views** to open the **Billing views** dialog box.
5. Use the **Find view name** search field to filter the custom billing views in the **Billing views** table.
6. Once you find the custom billing view you want to access, select it and choose **Choose**.

Once you choose a custom billing view, the contents of the AWS Billing and Cost Management console are refreshed to reflect the cost management data defined in the chosen custom billing view. The console navigation pane refreshes to display only those tools supported by the chosen custom billing view. Navigating to a different AWS Billing and Cost Management tool will maintain the currently chosen custom billing view.

> **Note**
>
> Not all widgets on the AWS Billing and Cost Management home page support custom billing views. Cost management data included in the selected custom billing view is shown

in the “Cost summary”, “Cost breakdown”, and “Cost allocation coverage” widgets. The “Recommended actions”, “Savings opportunities”, and “Cost monitor” widgets don't display recommended actions, savings opportunities, or cost monitors when accessing a custom billing view.

Using AWS managed views

To choose an AWS managed billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, enable **billing view** mode.
3. From the dropdown list, choose **billing transfer** view.

   The dropdown shows your 10 most recently accessed views. To see all views, choose **See all views** at the bottom of the dropdown menu.
4. From the **Billing vieBilling view** modal, choose either `billing group view` or `billing transfer views`.
5. Use the search bar to filter results across all columns in the table.

   Search for views using these parameters:

   - View name (partial match, starts with)

   - Account ID (exact match)

   - Type (exact match for `BILLING_TRANSFER` or `BILLING_TRANSFER_SHOWBACK`)

   - Billing period (choose month)
6. Select the desired billing view and select **Choose**.

You can analyze billing transfer showback/chargeback views and billing group views in AWS Cost and Usage Report (during beta, only legacy AWS Cost and Usage Report is supported), Cost Explorer, and the **Bills** page.

Viewing a Cost Explorer report using billing views

Cost Explorer provides two types of default reports: cost and usage reports and Reserved Instance reports. Only Cost Explorer reports of type “cost and usage reports” are supported by custom and AWS managed billing views; “Reserved Instance reports” can’t be used with a custom and AWS managed billing views. Cost Explorer also enables you to create your own reports by saving the results of a Cost Explorer query as a report. Cost Explorer reports can be used alongside custom billing views to access the cost management data contained in a custom billing view with the query saved as a Cost Explorer report.

When creating a new Cost Explorer report, only the Cost Explorer query is saved as part of the report definition. The currently selected custom and AWS managed billing view is not saved as part of the report. To learn more about Cost Explorer reports, see Understanding your costs using Cost Explorer reports.

To view a saved Cost Explorer report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, enable **billing view** mode. The default selection is the **Primary view**, which represents cost management data for the account you're currently logged in to.
3. From the dropdown list, choose either **Custom** or **AWS managed views** (`billing group` or `billing transfer` views). Choose the custom billing view you want to use for accessing cost management data.
4. In the navigation pane, choose **Cost Explorer Saved Reports**.
5. Select the report you want to access.

> **Note**
>
> You can save your Cost Explorer configuration and billing view selection as a favorite or bookmark in your browser. When you return to this saved link, Cost Explorer refreshes the page to display the cost management data from the billing view along with the saved configuration. This feature allows you to quickly access frequently used combinations of configurations and billings views, saving you time and effort.

Viewing and creating budgets using billing views

AWS Budgets supports primary and custom billing views, allowing you to create and manage budgets based on filtered cost and usage data across multiple accounts within your organization. This feature enables decentralized cloud cost management across your organization without requiring access to the management account.

When creating a new budget, you can select a billing view to define the scope of cost and usage data the budget will track. The selected billing view is saved as part of the budget definition.

When you create a budget using a billing view, the budget only tracks cost and usage data within the scope of that billing view. For instance, you could create a budget that tracks costs only for a specific department or project. This allows for more granular budget management aligned with your organizational structure or cost allocation strategies.

To view or create a budget using a billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, select the **Choose billing view** menu. The default selection is the **Primary view**, which represents cost management data for the account you're currently logged in to.
3. From the dropdown list, choose the billing view you want to use:
   - **Primary view**: Shows cost management data for your current account.
   - **Custom views**: Shows filtered cost management data based on defined criteria.
   - **AWS managed billing views (billing transfer view and billing group views)**: Shows cost management data for bill source accounts transferring their bills via Billing Transfer and for accounts included in billing groups via .
4. In the navigation pane, choose **Budgets**.
5. For existing budgets, the budgets list displays only the budgets created using the selected billing view.
6. For a new budget, choose **Create budget**, and then follow the budget creation workflow. The selected billing view is automatically applied to the new budget. For more details, see Creating a budget.

> **Note**
>
> Budgets created with billing views can only be viewed and managed when the corresponding billing view is selected. When you switch to a different billing view, these budgets will not be visible in the budgets list.

Viewing and creating exports using billing views

AWS Cost Management Data Export supports primary, billing group, and billing transfer views that help you generate detailed cost and usage reports. You can filter data across multiple accounts in your organization. When you create a data export, you can choose a billing view to define which cost and usage data to include. This enables you to focus on specific departments or projects without requiring access to the management account.

You can customize your exports by choosing specific data dimensions, time periods, and accounts. AWS Cost Management saves all configurations for future use. The service automatically delivers exported data to your specified Amazon Simple Storage Service bucket on a schedule, enabling integration with external analysis tools.

To view or create an export using a billing view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, enable **Billing Views**. The default selection is the **Primary view**, which represents cost management data for the account you're currently logged in to.
3. From the dropdown list, choose the billing view you want to use:
   - **Primary view**: Shows cost management data for your current account.
   - **Billing Group views**: Shows cost management data for accounts included in billing groups via .
   - **Billing Transfer views**: Shows cost management data for accounts that have transferred their AWS billing responsibility to you.
4. In the navigation pane, choose **Data Exports**.
5. For existing exports, the exports list displays only the exports created using the selected billing view.

6. For a new export, choose **Create export**, and then follow the export creation workflow. The selected billing view is automatically applied to the new export.

> **Note**
>
> Custom billing views are not currently supported for Data Exports. All other billing view types are supported.

Visualizing and analyzing cost and usage data using Dashboards

AWS Billing and Cost Management Dashboards enable you to create and share customized views of your cost and usage data in a single page. You can create collections of charts and tables, called widgets, that combine data from Cost Explorer, Savings Plans and Reserved Instance coverage and utilization, Budgets, Cost Efficiency, and Detected Anomalies. Together, these widgets provide comprehensive insights into your AWS spending patterns.

Key features of Dashboards:

- Create custom dashboards with multiple visualization types to display cost and usage data.
- Monitor budgets alongside cost and usage data, including actual spend against budget limits and forecasted spend.
- Track cost efficiency trends alongside cost and usage data to monitor optimization performance over time.
- Review cost anomalies detected alongside cost and usage data, including cost impact, top root cause, and severity.
- Customize dashboard layouts by resizing and arranging widgets to highlight key information.
- Share dashboards securely with accounts within or outside your AWS Organization.
- Pin frequently-used dashboards as favorites for quick access.
- Export dashboards as PDF reports for offline viewing and sharing with stakeholders.
- Schedule automated email delivery of dashboard PDF reports to stakeholders on a daily, weekly, or monthly basis.
- Use Managed Dashboards to get instant visibility into cost trends, service category costs, and commitment performance without any setup.

Common use cases for Dashboards include:

- Analyzing spending trends across services, Regions, and teams to identify cost patterns.
- Monitoring budget performance across multiple budgets in a single view, reducing the need to navigate between the AWS Budgets and Dashboards.
- Monitoring cost efficiency trends across accounts and regions to track optimization performance in a single view, reducing the need to navigate between the AWS Cost Optimization Hub and Dashboards.
- Monitoring cost anomalies across accounts and services in a single view, reducing the need to navigate between AWS Cost Anomaly Detection and Dashboards.
- Monitoring Savings Plans and Reserved Instance utilization and coverage to optimize commitments.
- Establishing standardized cost reporting practices to maintain consistency across your organization.
- Creating targeted financial reports for specific teams, projects, or business units.
- Automating distribution of cost reports to executives, finance teams, and other stakeholders who need regular visibility into cloud costs.
- Getting started quickly with preconfigured Managed Dashboards that provide immediate cost visibility across spending trends, compute, database, reservations, and savings plans without building dashboards from scratch.

Important

- Charges for your current billing period shown on this dashboard are estimated charges. Estimated charges shown on this dashboard, or shown on any notifications that we send to you, may differ from your actual charges for this statement period. This is because estimated charges presented on this dashboard do not include usage charges accrued during this statement period after the date you view this page. One-time fees and subscription charges are assessed separately from usage and reoccurring charges, on the date that they occur.
- Forecasted charges are estimated based on your historical charges and may differ from your actual charges for the forecast period. Forecasted charges are provided solely for your convenience and do not take into account changes to your use of services after the date on which you view this dashboard.

- Dates shown are based on Coordinated Universal Time (UTC).

Topics

- Getting started with dashboards
- Managed Dashboards
- Creating custom dashboards
- Adding widgets to dashboards
- Exporting dashboards
- Scheduling email delivery of dashboard reports
- Sharing dashboards
- Managing dashboards

Getting started with dashboards

AWS Billing and Cost Management Dashboards are collections of widgets that visualize your cost and usage data. Each dashboard can contain up to 20 widgets, which can show costs, usage, and savings plans and reserved instances coverage and utilization, budgets data, cost efficiency metrics, and detected cost anomalies. One of the powerful features of dashboards is that they can be shared within or outside your organization, allowing for collaborative cost management.

Prerequisites

Before creating or using dashboards, ensure you have:

- Activated the required IAM user and role access to the Billing and Cost Management console. For more information about IAM actions, see Using identity-based policies (IAM policies) for AWS Cost Management.
- Enabled fine-grained AWS IAM actions for AWS Billing and Cost Management. For more information, see Changes to AWS Billing, Cost Management, and Account Consoles Permissions.
- (Optional) Enabled AWS RAM sharing with AWS Organizations if you plan to share dashboards within your organization. For more information, see How AWS RAM works with IAM in the *AWS Resource Access Manager User Guide*.

- (Optional) If you are setting up email delivery for a scheduled report for a user for the first time, the user will need to verify their email address through a one time verification email before they can start receiving scheduled reports.

> **Note**
>
> Creating dashboards using AWS CloudFormation is not currently supported.

To share dashboards with member accounts in your organization, you must access the management account of your organization using an IAM principal that has permissions to create and share resources using AWS Resource Access Manager (AWS RAM). Permissions are not required for member accounts that receive a shared dashboard. To learn more, see Sharing dashboards. For details about IAM actions for sharing dashboards, see How AWS RAM works with IAM in the *AWS Resource Access Manager User Guide*.

Accessing Dashboards

You can access Dashboards from the Billing and Cost Management console.

To access Dashboards

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.

Understanding your dashboard list

Your dashboard list can contain dashboards from three sources, and what you can edit depends on where a dashboard came from.

- Dashboards that you create are fully editable. You choose which widgets to add, configure them, and arrange the layout, and you can share a dashboard that you own with other accounts.
- Managed Dashboards are preconfigured by AWS. They appear in your dashboard list automatically, are populated with your own account data, and are read-only. Managed Dashboards are identified by a lock icon. To change a Managed Dashboard, duplicate it. The copy is a dashboard that you own and can edit freely.

- Dashboards that are shared with you were created in another account and shared with you through AWS Resource Access Manager (AWS RAM). You can view them, but only the owning account can change them.

On the dashboard list page, you can use tabs to filter your list: **All dashboards**, **Managed**, and **Shared with me**.

Understanding dashboard permissions

Dashboard permissions are managed through IAM policies. To work with dashboards effectively, you need to understand both the permissions required for managing dashboards and those needed for accessing the underlying data.

Required dashboard permissions include:

- `CreateDashboard` - Create new dashboards
- `GetDashboard` - View dashboard details
- `UpdateDashboard` - Modify existing dashboards
- `DeleteDashboard` - Remove dashboards
- `ListDashboards` - View available dashboards
- `CreateScheduledReport` - Create scheduled email reports
- `GetScheduledReport` - View scheduled report details
- `UpdateScheduledReport` - Modify scheduled report configurations
- `DeleteScheduledReport` - Remove scheduled report configurations
- `ListScheduledReports` - View available scheduled reports
- `ExecuteScheduledReport` - Triggers immediate execution of a scheduled report

The following is an example IAM policy that grants all dashboard permissions:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "bcm-dashboards:CreateDashboard",
                "bcm-dashboards:GetDashboard",
                "bcm-dashboards:UpdateDashboard",
                "bcm-dashboards:DeleteDashboard",
                "bcm-dashboards:ListDashboards"
            ],
            "Resource": "*"
        }
    ]
}
```

When working with dashboards, users need permissions to access the dashboard resource itself and permissions to access the underlying cost and usage data APIs. For shared dashboards, permissions are managed through AWS RAM.

Note

To schedule email delivery of dashboard reports, you also need the following permissions:

- `iam:PassRole` – Required for passing the IAM execution role to the API.
- `bcm-dashboards:GetDashboard`, `ce:GetDimensionValues`, `ce:GetCostAndUsageWithResources`, `ce:GetCostAndUsage`, `ce:GetCostForecast`, `ce:GetTags`, `ce:GetUsageForecast`, `ce:GetCostCategories`, `ce:GetSavingsPlansCoverage`, `ce:GetReservationUtilization`, `ce:GetReservationCoverage`, `ce:GetSavingsPlansUtilization`, `ce:GetSavingsPlansUtilizationDetails`, `ce:GetAnomalyMonitors`, `ce:GetAnomalies`, `budgets:ViewBudget`, `budgets:DescribeBudgetActionsForAccount`, `cost-optimization-hub:ListEfficiencyMetrics`, `billing:ListBillingViews` – Required for the execution role to retrieve dashboard and cost data. For more information, see Execution role permissions for scheduled reports.

> **Note**
>
> Viewing AWS Managed Dashboards requires `ListDashboards` and `GetDashboard` permissions. If you attempt write operations (`UpdateDashboard`, `DeleteDashboard`) on a Managed Dashboard, the API returns a `AccessDeniedException`.

Managed Dashboards

Managed Dashboards are preconfigured, read-only dashboards authored and maintained by AWS that appear automatically in your dashboard list. They are populated with your account data and provide immediate visibility into your cost trends, service costs, and commitment performance without requiring any setup. These dashboards are built on common customer reporting patterns and FinOps best practices, combining widget types and configurations that address the most frequently needed cost analysis scenarios.

Topics

- Available Managed Dashboards
- Viewing Managed Dashboards
- Limitations of Managed Dashboards
- Building your custom dashboards from Managed Dashboards
- Exporting Managed Dashboards

Available Managed Dashboards

Five Managed Dashboards are available, organized around three layers of cloud financial visibility.

Cost and usage trends

Cost Overview & Trends serves as your financial summary. It tracks spending across services, accounts, regions, charge types, and billing entities over 12 months, and includes forward-looking cost forecasts. Use this dashboard for monthly reviews, executive briefings, or when you want to understand your overall spending trajectory.

Widgets include total monthly cost trends, current and forecasted costs, cost by top spending services, cost by service breakdown, cost by linked account, cost by region, cost by charge type, cost by billing entity, and marketplace costs.

Key service categories

Compute shows your Amazon EC2, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, AWS Lambda, and other compute costs. Costs are broken down by instance type, platform, and availability zone. It pairs these cost breakdowns with Savings Plans and Reserved Instance utilization and coverage metrics. These pairings show you where compute spend is concentrated and let you evaluate whether your commitments are well matched to your workloads. Use this dashboard to identify right-sizing opportunities, evaluate Graviton migration candidates, and assess commitment coverage gaps for compute workloads.

Database covers Amazon RDS, ElastiCache, OpenSearch, DynamoDB, Redshift, and other data services with breakdowns by database engine, instance type, purchase option, and usage type. Per-service Reserved Instance coverage and Savings Plans coverage widgets show where commitment gaps exist across your database portfolio. Use this dashboard to understand database cost composition, identify right-sizing candidates, and evaluate whether RI coverage is adequate across each database service.

Commitment reporting

Reservations gives you a consolidated view of Reserved Instance performance across all RI-eligible services: Amazon EC2, Amazon ElastiCache, Amazon RDS, Amazon OpenSearch Service, Amazon Redshift, and Amazon MemoryDB. Each service shows cost by instance type alongside coverage metrics and utilization detail. Use this dashboard to scan all services and identify coverage gaps or underutilization across your RI portfolio.

Savings Plans shows utilization and coverage for your Savings Plans portfolio across all three types: Compute, EC2 Instance, and Amazon SageMaker. It displays utilization and coverage for each type alongside on-demand spend and purchase option composition. Use this dashboard to assess whether your Savings Plans are optimally sized and identify where additional purchases would yield savings.

Viewing Managed Dashboards

To view Managed Dashboards, navigate to the Billing and Cost Management console, choose **Dashboards** from the left navigation, and select the **Managed** tab to see only AWS-authored dashboards. You can also find them in the **All dashboards** tab where they appear alongside your custom and shared dashboards, identified by a lock icon indicating read-only status.

When you open a Managed Dashboard, you see your account's cost and usage data rendered across all widgets. You can temporarily adjust the dashboard's layout while viewing. You can also change

a time range to focus on a specific period. These adjustments are not saved. The dashboard returns to its original configuration when you navigate away or refresh the page. This ensures a consistent baseline that is always available in its intended form.

Limitations of Managed Dashboards

Managed Dashboards are read-only. The following actions are not available for Managed Dashboards:

- **Editing** - You cannot modify widget configurations, add new widgets, remove widgets, or change the dashboard layout permanently.
- **Deleting** - You cannot delete Managed Dashboards. They are maintained by AWS and always available in your dashboard list.
- **Sharing** - You cannot share Managed Dashboards with other accounts. They are already available in every account automatically.
- **Tagging** - You cannot add tags to Managed Dashboards.
- **Scheduling email delivery** - You cannot schedule email delivery directly on a Managed Dashboard. To schedule reports, duplicate the Managed Dashboard as a custom dashboard first, then configure the scheduled report on your custom copy.

Building your custom dashboards from Managed Dashboards

Although you cannot edit a Managed Dashboard, you can use one to build a custom dashboard that you own, in two ways.

Duplicating a Managed Dashboard

You can duplicate any Managed Dashboard to create an independent custom copy that you fully own. The duplicated dashboard appears with "duplicate" added to the original name, which you can modify. After you duplicate a dashboard, you have full control: add or remove widgets, change time ranges, apply cost allocation tags, adjust dimensions, rearrange the layout, schedule email delivery, and share with other accounts. Changes to the original Managed Dashboard by AWS do not affect your duplicated copy.

To duplicate a Managed Dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.

2. In the navigation pane, choose **Dashboards**.
3. Select the Managed Dashboard you want to duplicate.
4. Choose **Actions**, and then choose **Duplicate dashboard**.
5. Modify the name and description for your new dashboard.
6. Choose **Duplicate**.

Adding widgets from a Managed Dashboard

You can add individual widgets from a Managed Dashboard to your existing custom dashboards without duplicating the entire dashboard. With this option, you can select specific visualizations that are relevant to your reporting needs.

To add a widget from a Managed Dashboard to a custom dashboard

1. Open the Managed Dashboard containing the widget you want to add.
2. Open the widget menu (three dots) on the widget you want to copy.
3. Choose **Add to dashboard**.
4. Select the custom dashboard where you want to add the widget, or create a new dashboard.

Exporting Managed Dashboards

You can export Managed Dashboards using the same export options available for custom dashboards:

- **PDF export** – Export an entire Managed Dashboard as a PDF file for offline viewing and sharing with stakeholders. You can also export a single widget visualization as a PDF file.
- **CSV export** – Export data from individual widgets in CSV format for detailed analysis in spreadsheet applications.

To export a Managed Dashboard as PDF

1. Open the Managed Dashboard you want to export.
2. Choose **Actions**, and then choose **Export PDF**.
3. Wait for the PDF preview to load, verify the layout, and choose **Export PDF**.

To export a widget as PDF

1. Open the Managed Dashboard containing the widget you want to export.
2. Open the widget menu (three dots) and choose **Export**, then **PDF**.
3. Wait for the PDF preview to load, and choose **Export PDF**.

To export widget data as CSV

1. Open the Managed Dashboard containing the widget you want to export.
2. Open the widget menu (three dots) on the widget.
3. Choose **Export**, then **CSV**.

Creating custom dashboards

Dashboards help you visualize and monitor your AWS costs and usage data by combining multiple widgets into a single view. You can create custom dashboards to track specific metrics, compare costs across services or Regions, and share standardized views within or outside your organization.

> **Tip**
>
> Rather than starting with an empty dashboard, you can duplicate a Managed Dashboard. The copy is yours to edit freely, so you begin with widgets that are already configured and populated with your data. For more information, see Managed Dashboards.

To create a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Choose **Create dashboard**.

   A dashboard is created with a default name. You can change the name or add an optional description.

   - The name must be unique within your account and can contain up to 50 characters.
   - The optional description can contain up to 200 characters.

> **Note**
>
> Autosave is enabled by default, so all changes are saved automatically.

After you create a dashboard, it's assigned a unique Amazon Resource Name (ARN) and is initially empty. The dashboard is only available in your account. You can add widgets to display your cost and usage data. For more information, see Adding widgets to dashboards.

After configuring your dashboard, you can share it with other accounts within or outside your organization. For more information, see Sharing dashboards.

Adding widgets to dashboards

Dashboards help you visualize data through widgets - configurable components that display your cost and usage information. Each dashboard can contain up to 20 widgets, combining multiple visualizations into a single view. Widgets help you analyze cost and usage through charts and tables.

You can create custom widgets to display specific data or add predefined widgets. Each widget can be customized using filters and time ranges. For dashboard-level control, you can apply a global date range filter that affects all widgets simultaneously. Alternatively, you can configure individual widgets to use different time ranges, providing flexibility in how you view and compare data. The dashboard layout is also customizable - you can adjust widget sizes and positions to create your ideal view.

For example, you might create a dashboard to track cost optimization efforts by combining Savings Plans coverage and utilization charts with cost and usage data across different services and Regions. These combined visualizations help you analyze spending patterns and make data-driven financial decisions.

To add a widget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Create a new dashboard or choose an existing dashboard.
4. Choose **Add widget**, and then choose one of the following:

- **Custom widget** - Create a new visualization.
- **Predefined widget** - These widgets are preconfigured for the most common use cases and can be further customized to serve your reporting needs.

5. In the widget panel, drag the widget onto the dashboard.

> **Note**
>
> The default visualization is a bar chart.

6. In the **Edit widget parameters** panel, configure the following:

- Time period and granularity
- Group by dimensions
- Filters
- Cost aggregation and other data settings

7. To change the visualization type:

- Choose the vertical three dots in the upper right corner of the widget.
- Choose **Change visualization type**.
- Choose **Line chart**, **Bar chart**, **Stacked bar chart**, or **Table**.

> **Note**
>
> Autosave is enabled by default, so all changes are saved automatically.

Customizing dashboards

After adding widgets, you can customize your dashboard layout and settings. You can drag widgets to different positions and resize them to emphasize important information.

Time periods can be managed at both the dashboard and widget level:

- Set a dashboard-level time period that applies to all widgets. This setting affects all widgets temporarily and resets when you leave or refresh the dashboard.

- Configure individual widget time periods. These settings are saved with each widget and persist when you return to the dashboard.

> **Note**
>
> The Budget report widget displays data in table format only. Visualization type options (line chart, bar chart, stacked bar chart) do not apply to Budget report widgets. The dashboard level time period filter does not apply to Budget report widgets, as budget data is retrieved directly from the AWS Budgets service.

> **Note**
>
> The Cost Efficiency widget supports only line chart and table visualization types. In line chart view, the widget shows your efficiency score percentage over time. In table view, it shows cost efficiency percentage grouped by your selected dimension (AWS account, region, or overall).

> **Note**
>
> The Detected Anomalies widget displays data in table format only. Visualization type options (line chart, bar chart, stacked bar chart) do not apply to Detected Anomalies widgets.

Understanding widget types

Dashboards help you monitor and analyze your AWS costs, usage, and resource commitments. Two types of widgets are available: custom widgets that you configure from scratch to track costs, usage, and commitment metrics, and predefined widgets that come with preset cost breakdowns over time.

Widget type	Widget name	Widget description
Custom	Cost	Visualizes your aggregate costs across all AWS

Widget type	Widget name	Widget description
		services, including breakdown by service, Region, or custom tags.
	Usage	Visualizes your aggregate usage across all AWS services, helping you track resource consumption patterns.
	Budget	Displays your AWS Budgets in a table format. You can filter budgets by name, threshold , and type to monitor budget performance directly within your dashboard.
	Cost Efficiency	Displays your cost efficienc y score over time so that you can track how efficient ly your AWS environment is performing. You can view efficiency by AWS account, region, or overall, and adjust granularity to analyze trends.

Widget type	Widget name	Widget description
	Detected Anomalies	Displays cost anomalies detected by AWS Cost Anomaly Detection in a table, with columns such as monitor name, top root cause, cost impact, last detected, duration, expected and actual spend, severity, and assessment. You can filter anomalies by severity, assessment, service, usage type, region, monitor type, account, and anomaly ID to monitor anomalies directly within your dashboard.
	Savings Plans utilization	Shows how well you're using your Savings Plans commitments, including unused and partially used commitments.
Savings Plans coverage	Shows what percentage of your usage is covered by Savings Plans.	
Reservation utilization	Shows how well you're using your Reserved Instances.	
Reservation coverage	Shows what percentage of your usage is covered by Reserved Instances.	

Widget type	Widget name	Widget description
Predefined	Monthly costs by service	Visualizes your aggregate monthly costs across all AWS services for the last six months.
	Monthly costs by linked account	Visualizes your aggregate monthly costs across all AWS linked accounts for the last six months.
	Monthly EC2 running hour costs	Visualizes your monthly EC2 running hour costs for the last six months.
	Daily costs	Visualizes your daily AWS costs for the last six months.
	AWS Marketplace costs	Visualizes your AWS Marketplace costs for the last six months.

Each of these widgets can be customized to show the data most relevant to your needs, allowing you to create comprehensive and insightful dashboards.

Exporting dashboards

Dashboards provide flexible export options for offline analysis and sharing. You can export entire dashboards or individual widgets as PDF reports for immediate download, export individual widget data in CSV format for detailed analysis, or schedule automated email delivery of dashboard PDF reports to stakeholders.

Export options

- **PDF export:** Export your complete dashboard as a PDF file for offline viewing and sharing with stakeholders who don't have AWS console access. You can also export a single widget visualization into a PDF file.

- **CSV export:** Export data from individual widgets in CSV format file for detailed analysis in spreadsheet applications.

To export a dashboard as PDF

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to export.
4. Choose **Actions**, and then choose **Export PDF** from the dropdown list.
5. Wait for PDF preview to load, verify the layout and choose **Export PDF**.
6. The PDF file will be generated and downloaded to your device.

To export a widget as PDF

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Open the dashboard you want to export by choosing the dashboard name.
4. Locate the widget you want to export.
5. Open the widget menu (three dots) and select **Export** then **PDF**.
6. Wait for PDF preview to load, verify the layout and choose **Export PDF**.
7. The PDF file will be generated and downloaded to your device.

Note

If a widget contains a large amount of data or uses an extended time range, widget layout may be changed or some data may be excluded from the PDF export to ensure the visual fits within the page boundaries. This is necessary to maintain readability and proper formatting in the PDF document.
To ensure complete data export:

1. Review the PDF preview before finalizing the export
2. If you notice data is being truncated or excluded, cancel the PDF preview

3. Edit the widget's time range to a shorter period (e.g., change from yearly to quarterly or monthly view)
4. Adjust widget filters to reduce the data volume displayed
5. Preview the PDF again to verify all important data is now included

Note

When exporting a dashboard that contains AWS Budgets report widgets, the PDF includes the budget name, budgeted amount, actual spend, and forecasted amount columns.

Note

When exporting a dashboard that contains a Detected Anomalies widget, the PDF includes the monitor name, top root cause, cost impact, and last detected columns, along with the summary of anomalies detected and their total cost impact.

To export widget data as CSV

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Open the dashboard you want to export by choosing the dashboard name.
4. Locate the widget you want to export.
5. Open the widget menu (three dots) and select **Export** then **CSV**.
6. The CSV file will be downloaded to your device.

Scheduling email delivery of dashboard reports

You can schedule automated email delivery of your dashboard reports to stakeholders on a recurring basis. Scheduled reports generate a PDF snapshot of your dashboard at the configured time and deliver it to your specified recipients through email. This allows stakeholders who don't have AWS console access to receive regular visibility into cost and usage data.

Each scheduled report is configured with a delivery frequency (daily, weekly, or monthly), a specific delivery time, and a list of recipients. You can schedule delivery of your entire dashboard or a single widget. Report generation begins at the scheduled time and delivery follows shortly after.

When changes are made to a dashboard, they are automatically reflected in subsequent scheduled deliveries without requiring reconfiguration of the report.

> **Note**
>
> Scheduled email delivery is available only for dashboards that you create. To schedule email delivery for a Managed Dashboard, first duplicate it as a custom dashboard, then configure the scheduled report on your custom copy.
> To schedule email delivery, you need permissions for `bcm-dashboards:CreateScheduledReport`.

> **Note**
>
> AWS User Notifications is automatically configured in your account, including Notification Hubs, when you schedule email delivery of a dashboard report. For more information, see Getting started with AWS User Notifications in the *AWS User Notifications User Guide*.

Topics

- Execution role permissions for scheduled reports
- Creating a scheduled report
- Understanding scheduled report emails
- Managing scheduled reports

Execution role permissions for scheduled reports

When you create a scheduled report, you must provide an IAM execution role that grants AWS Billing and Cost Management permissions to generate and deliver reports on your behalf. The execution role requires the following permissions and trust policy.

Permissions policy

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AwsBcmDashboardsScheduleReportsDataAccess",
      "Effect": "Allow",
      "Action": [
        "bcm-dashboards:GetDashboard"
      ],
      "Resource": [
        "arn:aws:bcm-dashboards::*:dashboard/*"
      ]
    },
    {
      "Sid": "AwsBcmDashboardsScheduleReportsDataAccessCE",
      "Effect": "Allow",
      "Action": [
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostAndUsage",
        "ce:GetCostForecast",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:GetCostCategories",
        "ce:GetSavingsPlansCoverage",
        "ce:GetReservationUtilization",
        "ce:GetReservationCoverage",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForAccount",
        "billing:ListBillingViews",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

If you created an execution role before the launch of the AWS Budgets report widget, your existing role will not include the budgets API permissions. To schedule reports for dashboards that contain AWS Budgets report widgets, update your execution role to include the budgets permissions listed above. You can update your service roles from the Additional configuration section when creating or editing a scheduled report. This update will fail if a role was manually modified in IAM. To resolve this, create a new role or restore the policy version to its original state. For more information, see Setting the default version of a policy in the *IAM User Guide*.

Trust policy

The execution role must trust the `bcm-dashboards.amazonaws.com` service principal. Replace `<account-id>` with your AWS account ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBcmDashboardScheduledReportAssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": "bcm-dashboards.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "<account-id>"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:bcm-dashboards::<account-id>:*"
        }
      }
    }
  ]
}
```

Creating a scheduled report

You can create a scheduled report for a dashboard to automatically generate and deliver PDF snapshots to your recipients on a recurring basis.

To create a scheduled report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to schedule for email delivery.
4. Choose **Actions**, and then choose **Manage email reports**.
5. Choose **Create report**.
6. **Create report details** - Configure the basic information about the report:

   - **Report name** - Enter a name for the report.
   - **Description** (optional) - Enter a description to help identify your report.
   - **Widget selection** - Choose **Full dashboard** (default) to include all widgets, or **Single widget** to limit the report to one widget.
   - **Reporting period** - Choose **Widget-specific ranges** to preserve each widget's individual date range settings, or apply a unified date range for all widgets. Relative date ranges update with each delivery to provide the most relevant data based on when the report is generated.

   Use **Preview report** to verify the layout before proceeding. Choose **Next**.
7. **Select recipients** - Configure the notification settings for recipients:

   - **Email setup method** - Choose **Select from existing configurations** to use a previously configured AWS User Notifications configuration, or choose **Enter new email address** to create a new configuration that multiple reports can use for delivery.

   First-time recipients must verify their email address. For non-AWS users, you can use email distribution lists — only one team member with AWS console access needs to verify the list address, after which all members receive dashboard reports automatically. Choose **Next**.
8. **Configure report scheduling** - Configure when and how often the report will be delivered:

   - **Frequency** - Choose **Daily**, **Weekly**, or **Monthly**.

- **Delivery time (UTC)** - Specify the time when the report will be generated. Reports are usually delivered within a few minutes of the scheduled time
- **Start date** - Select when to start sending the report.
- **End date** - Select when to stop sending the report. Maximum allowed duration is three years from the start date.

Choose **Next**.

9. **Configure additional settings** - Set up service access and optional tags:

- **Service access** - Grant AWS Billing and Cost Management permissions to generate and deliver scheduled PDF reports, access permitted cost and usage data, and manage email delivery on your behalf. Choose one of the following:
  - **Create and use a new execution role** - Recommended for first-time setup. Creates a new IAM role with the permissions required for scheduled report generation and delivery. For more information, see the section called “Execution role permissions for scheduled reports”.
  - **Choose an existing execution role** - Select a previously created execution role from your account. Use this if you have already created a role for scheduled reports.
  - **Enter execution role ARN manually** - Specify the ARN of an execution role directly. Use this if the role was created in a different context or if you manage roles through infrastructure as code.
- **Resource tags** (optional) - Add tags to help search and filter your resources or track costs. You can add up to 50 tags.

Choose **Next**.

10. **Review and create** - Review all your selections across the previous steps. You can choose **Edit** next to any step to modify its settings. When satisfied, choose **Create**.

> **Note**
>
> Recipients receive an email containing a secure link to download the password-protected PDF report. The password is included in the email body. The download link expires after 15 days. No AWS permissions are required to download or view the PDF report.

Understanding scheduled report emails

When a scheduled report is generated, recipients receive an email notification containing:

- A secure, time-limited download link to access the PDF report. The link expires after 15 days.
- A unique password required to open the PDF file. Each report generation produces a new password.
- The report name, dashboard name, and generation timestamp.

PDF reports are encrypted and stored in AWS-managed Amazon S3 buckets. The download links use pre-signed URLs that grant time-limited access to the specific PDF file.

> **⚠ Controlling access to report download links and passwords**
>
> Scheduled reports are delivered through AWS User Notifications, and the notification event that AWS User Notifications creates for each delivery contains the download link and the PDF password. Permissions to read notification events are separate from permissions for AWS Billing and Cost Management and AWS Cost Explorer. For example, a principal with the `notifications:ListNotificationEvents` and `notifications:GetNotificationEvent` permissions can retrieve the link and the password even if it can't otherwise view your cost and usage data, and no AWS permissions are required to open the link.
>
> Grant permissions to read notification events only to principals that you intend to have access to the cost and usage data in your reports. For more information, see Identity and access management for AWS User Notifications in the *AWS User Notifications User Guide*.

Managing scheduled reports

You can view, edit, disable, or delete your scheduled reports from the Dashboards list page. The **Reports** column indicates which dashboards have scheduled reports configured.

To edit a scheduled report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.

3. Select the dashboard which corresponds to the scheduled report you want to edit.
4. Click on **Actions**, and then choose **Manage email reports**.
5. Select the report you want to edit.
6. Modify the report settings as needed.
7. Choose **Save**.

To disable a scheduled report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard which corresponds to the scheduled report you want to disable.
4. Click on **Actions**, and then choose **Manage email reports**.
5. Select the report you want to disable.
6. Click on **Actions**, and then choose **Disable report**.

> **Note**
>
> Disabling a scheduled report stops future report generation. Download links that were already delivered remain valid until they expire, 15 days after the report was generated. PDF reports that have already been downloaded to a local device are not affected.

To delete a scheduled report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard which corresponds to the scheduled report you want to delete.
4. Click on **Actions**, and then choose **Manage email reports**.
5. Select the report you want to delete.
6. Click on **Actions**, and then choose **Delete report**.
7. In the dialog box that appears, enter **`confirm`** and choose **Delete**.

> **Note**
>
> Deleting a scheduled report does not delete any associated resources in AWS User Notifications. To remove notification configurations and email contacts, manage them directly in the AWS User Notifications console.

Sharing dashboards

You can share dashboards with accounts in your AWS Organization or with external accounts (using AWS Resource Access Manager). When you share a dashboard, only dashboard configurations are shared, not the underlying data. Recipients receive access to the dashboard layout and widget configurations, and will see data based on their own access permissions.

The shared configuration includes all filter values, tag keys and values, and widget parameters. For example, if you have widgets filtered to show data for specific accounts, those account numbers will be visible to recipients in the filter configurations. Similarly, any tag keys and values used in your dashboard will be visible in the shared configuration.

When a dashboard is shared with "Can view" permissions, recipients can view the dashboard, export PDFs, and schedule their own email delivery configurations for the shared dashboard. Scheduled report configurations are managed independently by each user and are not shared as part of the dashboard configuration.

> **Note**
>
> Managed Dashboards cannot be shared because they are already available in every account automatically. If you want to share a customized version of a Managed Dashboard, duplicate it as a custom dashboard and then share that copy.

To share a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to share.
4. Choose **Share**.

5. Select the accounts you want to share the dashboard with:
   - Share with accounts in your AWS Organization
   - Share with external AWS accounts
6. Set permissions:
   - Read-only access ("Can view") Recipients can view the dashboard but cannot make changes
   - Edit access ("Can edit") Recipients can view and modify the dashboard configuration
7. Choose **Share**.

When you share a dashboard, new resource shares are automatically created in AWS RAM. If AWS RAM sharing with AWS Organizations is enabled, users in recipient accounts can access shared dashboards immediately (subject to their identity-based IAM permissions). If AWS RAM sharing with Organizations is not enabled, administrators in recipient accounts will need to accept the resource share invitation.

Note

- If sharing outside your organization, recipients must accept the share invitation in AWS RAM. Recipients should navigate to **Resource shares** under **Shared with me** in the AWS RAM console, ensuring they are in the same Region where the share was created. After selecting and accepting the invitation in **Resource shares**, the shared dashboard will appear in the recipient's Billing and Cost Management console under **Dashboards**. If the invitation is not immediately visible, recipients should verify they are using the correct AWS account and Region.
- To view or edit shared dashboards, users in recipient accounts must have appropriate IAM permissions (for example, `ListDashboards`, `GetDashboard`).
- To see data in shared dashboards, users must also have permissions to the underlying APIs that provide that data (for example, `GetCostAndUsage` or `GetAnomalies`).
- You can revoke access to shared dashboards at any time.

Managing dashboards

After creating and sharing dashboards, you'll need to manage them over time. This section covers how to edit, delete, and duplicate dashboards, as well as how to add tags for better organization.

Topics

- Editing dashboards
- Deleting dashboards
- Duplicating dashboards
- Adding tags to dashboards

Editing dashboards

You can modify existing dashboards to keep them relevant and useful as your needs change.

To edit a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to edit.

> **Note**
>
> Managed Dashboards cannot be edited. To modify a Managed Dashboard, duplicate it as a custom dashboard first.

Deleting dashboards

Deleting a dashboard permanently removes access to the dashboard for all users, including any accounts you've shared it with. This action cannot be undone. After a dashboard is deleted, it no longer appears in the **All dashboards** tab for owners or the **Shared with me** tab for those it was shared with. End users attempting to access the URL of the deleted dashboard will receive an error message.

When deleting a shared dashboard, especially one used as a standard reporting template across your organization, ensure all affected teams are notified in advance.

While deleting a dashboard removes the visualization configuration, it does not affect the underlying cost and usage data or other dashboards that might show similar data.

> **Note**
>
> If the dashboard you are deleting has active scheduled reports configured, those scheduled reports will also stop generating. Ensure you notify any report recipients before deleting a dashboard with active scheduled deliveries.

To delete a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to delete.
4. Choose **Actions**, and then choose **Delete dashboard** from the dropdown list.
5. In the dialog box that appears, enter **confirm** and choose **Delete**.

> **Note**
>
> Managed Dashboards cannot be deleted. They are maintained by AWS and always available in your dashboard list.

> **Note**
>
> This action cannot be undone.

Duplicating dashboards

You might want to duplicate a dashboard when you need to create variations of existing dashboards. For example, you could duplicate a dashboard that tracks costs by service, then modify the copy to track costs by a different dimension like Region or cost allocation tag. This saves time compared to creating a new dashboard from scratch.

When you duplicate a dashboard, you create an independent copy with the same widget configurations as the original. The new dashboard appears with "duplicate" added to the original

name, which you can modify at any time. Any subsequent changes to the original dashboard won't affect your duplicate, and vice versa.

To duplicate a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to duplicate.
4. Choose **Actions**, and then choose **Duplicate dashboard** from the dropdown list.
5. In the dialog box that appears, you can modify the name and description for your new dashboard.
6. Choose **Duplicate**.

You can duplicate dashboards that have been shared with you. The duplicated dashboard belongs to your account and you have full edit permissions for it, regardless of the permissions you had on the original dashboard.

You can also duplicate Managed Dashboards to create custom copies. This is the recommended way to customize a Managed Dashboard for your specific needs. The duplicated dashboard belongs to your account with full edit permissions, regardless of the read-only status of the original Managed Dashboard.

Adding tags to dashboards

Tags help you identify, organize, and manage your dashboards by adding descriptive labels. You might tag your dashboards to identify which department created them, track them by project or initiative, label their purpose, or mark them for different environments. For example, you could use tags like Department = Marketing or Project = Cost-Optimization-2025 to categorize your dashboards.

When you have many dashboards across your organization, tags become particularly valuable. They allow you to filter and search for specific dashboards, control access through IAM policies based on tag values, and track dashboards that serve similar purposes across different teams. If you use the AWS CLI or SDK, tags also help you manage related dashboards as a group.

To add tags to a dashboard

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Dashboards**.
3. Select the dashboard you want to tag.
4. Choose **Actions**, and then choose **Manage tags** from the dropdown list.
5. Choose **Add new tag**.
6. Enter the key and value (optional) for the tag.
7. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50
8. Choose **Save changes**.

After you save changes, the tags are applied to your dashboard and can be used for filtering and access control.

> **Note**
>
> Tags cannot be added to Managed Dashboards. To tag a Managed Dashboard configuration, duplicate it as a custom dashboard and then add tags to your copy.

Analyzing your costs and usage with AWS Cost Explorer

AWS Cost Explorer is a tool that enables you to view and analyze your costs and usage. You can explore your usage and costs using the main graph, the Cost Explorer cost and usage reports, or the Cost Explorer RI reports. You can also ask questions about your costs using suggested prompts or the **Ask question** button to ask in your own words, and receive detailed insights in **Amazon Q Developer** while Cost Explorer automatically updates its charts, tables, and report parameters including filters, groupings, and dates to reflect the analysis. For a deeper dive, choose **Analyze with Amazon Q** on any cost report to receive comprehensive explanations covering your cost trends, top drivers, and anomalies based on your exact filters and time period. You can view data for up to the last 13 months, forecast how much you're likely to spend for the next 18 months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API. Each paginated API request incurs a charge of $0.01. You can't disable Cost Explorer after you enable it.

In addition, Cost Explorer provides preconfigured views that display at-a-glance information about your cost trends and give you a head start on customizing views that suit your needs.

When you first sign up for Cost Explorer, AWS prepares the data about your costs for the current month and the last 13 months, and then calculates the forecast for the next 18 months. The current month's data is available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer refreshes your cost data at least once every 24 hours. However, this depends on your upstream data from your billing applications, and some data might be updated later than 24 hours. After you sign up, Cost Explorer by default can display up to 13 months of historical data (if you have that much), the current month, and the forecasted costs for the next 18 months. The first time that you use Cost Explorer, Cost Explorer walks you through the main parts of the console with an explanation for each section.

Cost Explorer uses the same dataset that is used to generate the AWS Cost and Usage Reports and the detailed billing reports. For a comprehensive review of the data, you can download it into a comma-separated value (CSV) file.

Topics

- Enabling Cost Explorer
- Getting started with Cost Explorer
- Exploring your data using Cost Explorer
- Asking questions about your costs using Amazon Q Developer
- Comparing your costs between time periods
- Exploring more data for advanced cost analysis
- Using the AWS Cost Explorer API

Enabling Cost Explorer

You can enable Cost Explorer for your account by opening Cost Explorer for the first time in the AWS Cost Management console. You can't enable Cost Explorer using the API. After you enable Cost Explorer, AWS prepares the data about your costs for the current month and the previous 13 months, and then calculates the forecast for the next 12 months. The current month's data is

available for viewing in about 24 hours. The rest of your data takes a few days longer. Cost Explorer updates your cost data at least once every 24 hours.

As part of the process of enabling Cost Explorer, AWS automatically configures Cost Anomaly Detection for your account. Cost Anomaly Detection is an AWS Cost Management feature. This feature uses machine learning models to detect and alert on anomalous spend patterns in your deployed AWS services. To get you started with Cost Anomaly Detection, AWS sets up an AWS services monitor and a daily summary alert subscription. You're alerted about any anomalous spend that exceeds $100 and 40% of your expected spend across the majority of your AWS services in your accounts. For more information, see limitations and Detecting unusual spend with AWS Cost Anomaly Detection.

Note

You can opt out of Cost Anomaly Detection at any time. For more information, see Opting out of Cost Anomaly Detection.

You can launch Cost Explorer if your account is a member account in an organization where the management account enabled Cost Explorer. Know that your organization's management account can also deny your account access. For more information, see Consolidated billing for AWS Organizations.

Note

An account's status within an organization determines what cost and usage data are visible:

- A standalone account joins an organization. After this, the account can no longer access cost and usage data from when the account was a standalone account.
- A member account leaves an organization to become a standalone account. After this, the account can no longer access cost and usage data from when the account was a member of the organization. The account can access only the data that's generated as a standalone account.
- A member account leaves organization A to join organization B. After this, the account can no longer access cost and usage data from when the account was a member of organization A. The account can access only the data that's generated as a member of organization B.

- An account rejoins an organization that the account previously belonged to. After this, the account regains access to its historical cost and usage data.

Signing up to receive the AWS Cost and Usage Reports or the Detailed Billing Report doesn't automatically enable Cost Explorer. To do so, follow this procedure.

To sign up for Cost Explorer

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Explorer**.
3. On the **Welcome to Cost Explorer** page, choose **Launch Cost Explorer**.

For more information about controlling access to Cost Explorer, see Controlling access to Cost Explorer.

Controlling access to Cost Explorer

You can manage access to your Cost Explorer in the following ways:

- Using the management account, you can enable Cost Explorer as a root user, automatically enabling all member accounts.
- After member accounts are enabled, you can change Cost Explorer settings from within the management account. You can control the information that can be accessed in Cost Explorer. This includes costs, refunds or credits, discounts, and Reserved Instance (RI) recommendations.
- After you enable Cost Explorer at the management account level, you can manage user IAM policies. For example, you can grant users full access or deny users access to Cost Explorer.

This topic provides information about how to control access in Cost Explorer.

For information about managing access to Billing and Cost Management pages, see Overview of managing access permissions.

To reference Cost Explorer IAM policies, see Using identity-based policies (IAM policies) for AWS Cost Management.

For more information about consolidated billing, see Consolidated billing for AWS Organizations.

Topics

- Granting Cost Explorer access
- Controlling access using Cost Explorer preferences
- Managing Cost Explorer access for users

Granting Cost Explorer access

If you're signed into the management account with your root account credentials, you can enable Cost Explorer access. Your root account credentials are through the Billing and Cost Management console. Enabling Cost Explorer at the management account level enables Cost Explorer for all of your organization accounts. All accounts in the organization are granted access, and you can't grant or deny access individually.

Controlling access using Cost Explorer preferences

A management account can grant access to Cost Explorer for all or none of the member accounts. Access isn’t customizable for each individual member account.

The management account in AWS Organizations has full access to all Billing and Cost Management information for costs incurred by both the management account and member accounts. Member accounts only have access to their own cost and usage data in Cost Explorer.

By default, the management account in AWS Organizations sees all costs at the chargeable rate. If an organization is onboarded to Billing Conductor, the management account also sees costs at the proforma rate. The Cost Explorer view for member accounts depends on the configuration in Billing Conductor.

The owner of a management account can do the following:

- View all costs in Cost Explorer.
- Grant all member accounts the permission to see the costs for their own member account, refunds, credits, and RI recommendations.

Member account owners can't see costs, refunds, and RI recommendations for other accounts in the Organizations. For more information about consolidated billing, see Consolidated billing for AWS Organizations.

If you're an AWS account owner and not using consolidated billing, you have full access to all Billing and Cost Management information including Cost Explorer.

If you're onboarded to Billing Conductor, the Cost Explorer view for member accounts depends on whether a member account is part of a billing group.

If a member account is part of a billing group:

- The member account sees all costs at the proforma rate.
- Cost Explorer preferences, such as **Linked Account Access**, **Linked Account Refunds and Credits**, **Linked Account Discounts**, **Hourly and Resource Level Data**, and **Split cost allocation data** are not applicable to the member account.

If a member account is not part of a billing group:

- The member account see costs at the chargeable rate.
- Cost Explorer preferences apply to the member account.

For more information about Billing Conductor, see the Billing Conductor User Guide.

Organizations account status use cases

An account's status within an organization determines what cost and usage data are visible in the following ways:

- A standalone account joins an organization. After this, the account can no longer access cost and usage data from when the account was a standalone account.
- A member account leaves an organization to become a standalone account. After this, the account can no longer access cost and usage data from when the account was a member of their previous organization. The account can only access the data that's generated as a standalone account.
- A member account leaves organization A to join organization B. After this, the account can no longer access cost and usage data from organization A. The account can access only the data that's generated as a member of organization B.
- An account rejoins an organization that it previously belonged to. After this, the account regains access to its historical cost and usage data.

Controlling member accounts' access using Cost Explorer preferences

You can grant or restrict the access to all member accounts in your Organizations. When you enable your account at the management account level, all member accounts are granted access to their cost and usage data by default.

To control member account access to Cost Explorer data

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. On the **Preferences** page, under **Member account permissions** in the **General** tab, select or clear **Linked account access**.
4. Choose **Save preferences**.

Managing Cost Explorer access for users

After you enable Cost Explorer at the management account level, you can use IAM to manage access to your billing data for individual users. This way, you can grant or revoke access on an individual level for each account, rather than granting access to all member accounts.

A user must be granted explicit permissions to view pages in the Billing and Cost Management console. With the appropriate permissions, the user can view costs for the AWS account that the user belongs to. For the policy that grants the necessary permissions to a user, see Overview of managing access permissions.

Getting started with Cost Explorer

After you enable Cost Explorer, you can launch it from the AWS Cost Management console.

To open Cost Explorer

- Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.

This opens the Cost dashboard that shows you the following:

- Your estimated costs for the month to date

- An **Analyze with Amazon Q** button for receiving comprehensive explanations of any configured cost report, powered by **Amazon Q Developer**
- Your forecasted costs for the month
- A graph of your daily costs
- Suggested prompts for one-click analysis of your cost questions, powered by **Amazon Q Developer**
- An **Ask question** button for typing custom cost questions in your own words, powered by **Amazon Q Developer**
- Your five top cost trends
- A list of reports that you recently viewed

Exploring your data using Cost Explorer

On the Cost Explorer dashboard, Cost Explorer shows your estimated costs for the month to date, your forecasted costs for the month, a graph of your daily costs, your five top cost trends, and a list of reports that you recently viewed.

All costs reflect your usage up to the previous day. For example, if today is December 2, the data includes your usage through December 1.

> **Note**
>
> In the current billing period, the data depends on your upstream data from your billing applications, and some data might be updated later than 24 hours.

- Your Cost Explorer costs
- Your Cost Explorer trends
- Your daily unblended costs
- Your monthly unblended costs
- Your net unblended costs
- Your recent Cost Explorer reports
- Your amortized costs
- Your net amortized costs

Navigating Cost Explorer

You can use the icons in the left pane to do the following:

- Go to the main Cost Explorer dashboard
- See a list of the default Cost Explorer reports
- See a list of your saved reports
- See information about your reservations
- See your reservation recommendations

Your Cost Explorer costs

At the top of the **Cost Explorer** page are the **Month-to-date costs** and **Forecasted month end costs**. The **Month-to-date costs** shows how much you're estimated to have incurred in charges so far this month and compares it to this time last month. The **Forecasted month end costs** shows how much Cost Explorer estimates that you will owe at the end of the month and compares your estimated costs to your actual costs of the previous month. The **Month-to-date costs** and the **Forecasted month end costs** don't include refunds.

The costs for Cost Explorer are only shown in US dollars.

Your Cost Explorer trends

In the ***this month*** **trends** section, Cost Explorer shows your top cost trends. For example, your costs related to a specific service have gone up, or your costs from a specific type of RI have gone up. To see all of your costs trends, choose **View all trends** in the upper-right corner of the trend section.

To understand a trend in more depth, choose it. You're taken to a Cost Explorer chart that shows the costs that went into calculating that trend.

Your daily unblended costs

In the center of the Cost Explorer dashboard, Cost Explorer shows a graph of your current unblended daily costs. You can access the filters and parameters used to create the graph by choosing **Explore costs** in the upper-right corner. That takes you to the Cost Explorer report page, enabling you to access the default Cost Explorer reports and modify the parameters used

to create the chart. The Cost Explorer reports offer additional functionality such as downloading your data as a CSV file and saving your specific parameters as a report. For more information, see Understanding your costs using Cost Explorer reports. Your daily unblended costs don't include refunds.

Your monthly unblended costs

Monthly granularity

You can view your unblended costs at the monthly granularity and see the discounts applied to your monthly bill. When forecasting costs, discounts are included by default. To view your unblended costs, open the Cost Explorer page and choose **Cost Explorer** from the navigation pane. Discounts appear as the **RI Volume Discount** in the chart. The discount amount aligns with the discount amount shown in your Billing and Cost Management console.

To see the details in your Billing and Cost Management console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Bills**.
3. To display the discount, select the arrow next to **Total Discounts**, under **Credits, Total Discounts and Tax Invoices**.

Monthly gross charges

You can view your gross monthly charges by excluding the **RI Volume Discount**.

To exclude RI volume discounts in your monthly view

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the left pane, choose **Cost Explorer**.
3. Choose **Cost & Usage**.
4. On the **Filters** pane, choose **Charge Type**.
5. Select **RI Volume Discount**.
6. To open a dropdown, select **Include only** and choose **Exclude only**.
7. Select **Apply filters**.

Your net unblended costs

This enables you to see your net costs after all applicable discounts are calculated. You should still exclude any manual adjustment such as refunds and credits as a best practice. **RI Volume Discounts** are no longer visible because these are post-discount amounts.

Your recent Cost Explorer reports

At the bottom of the Cost Explorer dashboard is a list of reports that you have accessed recently, when you accessed them, and a link back to the report. This enables you to switch between reports or remember the reports that you find most useful.

For more information about Cost Explorer reports, see Understanding your costs using Cost Explorer reports.

Your amortized costs

This enables you to see the cost of your AWS commitments, such as Amazon EC2 Reserved Instances or Savings Plans, spread across the usage of the selection period. AWS estimates your amortized costs by combining the unblended upfront and recurring reservation fees, and calculates the effective rate over the period of time that the upfront or recurring fee applies. In the daily view, Cost Explorer shows the unused portion of your commitment fees at the first of the month or the date of purchase.

Your net amortized costs

This enables you to see the cost of your AWS commitments, such as Amazon EC2 Reserved Instances or Savings Plans, after discounts with the additional logic that shows how the actual cost applies over time. Since Savings Plans and Reserved Instances usually have upfront or recurring monthly fees associated with them, the net amortized cost dataset reveals the true cost by showing how post-discount fees amortize over the period of time that the upfront or recurring fee applies.

Using the Cost Explorer chart

By default, you can view your costs at the chargeable rate as either a cash-based view with unblended costs or as an accrual-based view. In a cash-based view, your costs are recorded when cash is received or paid. In an accrual-based view, your costs are recorded when income is earned or costs are incurred. You can view data for up to the last 13 months, the current month, and forecast

how much you're likely to spend for the next 12 months. You can also specify time ranges for the data and view time data by day or by month.

By default, Cost Explorer uses the **Group by** filter for the **Daily unblended costs** graph. When using the **Group by** filter, the Cost Explorer chart displays data for up to ten values in the **Group by** filter. If your data contains additional values, the chart displays nine bars or lines and then aggregates all remaining items in a tenth. The data table that's below the chart breaks out the data for individual services that are aggregated in the chart.

If your organization is onboarded to Billing Conductor, member accounts placed in billing groups automatically see your costs in Cost Explorer at the proforma rate configured in Billing Conductor. Member accounts can view costs and usage starting from when they joined their current billing group, and will lose access to the chargeable data for the period prior to joining their current billing group. If a backfill of proforma billing data is needed, submit a support ticket requesting a proforma backfill from the Billing Conductor team.

For more information about proforma rate configurations, see the Billing Conductor User Guide.

Topics

- Modifying your chart
- Reading the Cost Explorer data table
- Forecasting with Cost Explorer

Modifying your chart

You can modify the parameters that Cost Explorer uses to create your chart to explore different sets of data.

- Selecting a style for your chart
- Choosing time ranges for the data that you want to view
- Grouping data by filter type
- Filtering the data that you want to view
- Choosing advanced options

Selecting a style for your chart

Cost Explorer provides three styles for charting your cost data:

- Bar charts (**Bar**)
- Stacked bar charts (**Stack**)
- Line graphs (**Line**)

You can set the style by choosing one of the views on the top right corner of the chart.

Choosing time ranges for the data that you want to view

You can choose to view your cost data in monthly or daily *levels of granularity*. You can use preconfigured time ranges or set custom start and end dates.

To set the granularity and time range for your data

1. Start Cost Explorer.
2. Choose a time granularity of **Daily**, **Monthly**, or **Hourly**.

   > **Note**
   >
   > To enable hourly granularity, opt in through the Cost Explorer console **Preferences** page as the management account. When hourly granularity is enabled, information is available for the previous 14 days.

3. For your monthly or daily data, open the calendar and define a custom time range for your report. Or, alternatively, choose a preconfigured time range (**Auto-select**) using the dropdowns shown below the calendar. You can choose from a number of historical or forecast time ranges. The name of the time range that you choose appears in the calendar.

   Hourly granularity is not available for billing transfer (showback/ chargeback views and billing group views).
4. Choose **Apply**.

Historical time range options

In Cost Explorer, months are defined as calendar months. Days are defined as 12:00:00 AM to 11:59:59 PM. Based on these definitions, when you choose **Last 3 Months** for a date range, you see cost data for the 3 previous months. This doesn't include the present month. For example, if you view your chart on June 6, 2017, and select **Last 3 Months**, your chart includes data for March, April, and May 2017. All times are in Universal Coordinated Time (UTC).

You can choose time ranges for both your past costs and your forecasted future costs.

The following list defines each time range option for your past costs in Cost Explorer.

- Custom

  Displays data for the **From** and **To** time range that you specify with calendar controls.
- 1D (Last 1 Day)

  Displays cost data from the previous day.
- 7D (Last 7 Days)

  Displays cost data from the day before and the previous 6 days.
- Current Month

  Displays cost data and forecast data for the current month.
- 3M (Last 3 Months)

  Includes cost data from the previous 3 months but doesn't include the current month.
- 6M (Last 6 Months)

  Includes cost data from the previous 6 months but doesn't include the current month.
- 1Y (Last 12 Months)

  Includes cost data from the previous 12 months but doesn't include the current month.
- MTD (Month to Date)

  Displays cost data from the current calendar month.
- YTD (Year to Date)

  Displays cost data from the current calendar year.

Forecast time range options

With the **Daily** or **Monthly** time granularity, you have the option to view forecast costs in Cost Explorer. The following list defines each time range option for your forecast data. You can select a **Historical** time range and a **Forecasted** time range to display together. For example, you can select a **Historical** time range of 3 months (3M) and select a **Forecasted** time range of 3 months (+3M). Your report includes historical data for the previous 3 months plus forecasted data for the next

3 months. To clear a **Historical** time range and see only the forecast, choose the **Historical** time range option again.

> **Note**
>
> If you choose any forecasted dates, your current date's cost and usage data shows as **Forecast**. The current date's cost and usage won't include historical data.

- Custom

  Displays forecast data for the **From** and **To** time range that you specify with calendar controls.
- +1M

  Displays forecast data for the next month. This option is available if you choose the **Daily** time granularity.
- +3M

  Displays forecast data for the next 3 months. This option is available if you choose the **Daily** or **Monthly** time granularity.
- +18M

  Displays forecast data for the next 18 months. This option is available if you choose the Monthly time granularity.

Grouping data by filter type

Use the **Group by** button to have Cost Explorer display the cost data groups by filter type. By default, Cost Explorer doesn't use grouping. Forecasting isn't available for charts that have grouping. If you don't select a **Group by** option, Cost Explorer displays total costs for the specified date range.

To group your data by filter type

1. Launch Cost Explorer.
2. (Optional) Use the **Filters** controls to configure a view of your cost data.
3. Choose a **Group by** option to group by the category that you want. The data table below the chart also groups your cost figures by the category that you select.

Filtering the data that you want to view

With Cost Explorer, you can filter how you view your AWS costs by one or more of the following values:

- **API operation**
- **Availability Zone (AZ)**
- **Billing entity**
- **Charge type**
- **Include all**
- **Instance type**
- **Legal entity**
- **Linked account**
- **Platform**
- **Product attribute**
- **Purchase option**
- **Region**
- **Resources**
- **Service**
- **Tag**
- **Tenancy**
- **Usage type**
- **Usage type group**

You can use Cost Explorer to see which service you use the most, which Availability Zone (AZ) most of your traffic is in, and which member account uses AWS the most. You can also apply multiple filters to look at intersecting datasets. For example, you can use the **Linked Account** and **Services** filters to identify the member account that spent the most money on Amazon EC2.

To filter your data

1. Open Cost Explorer.
2. For **Filters**, choose a value. After you make a selection, a new control appears with additional options.

3. In the new control, select the items from each list that you want to display in the chart. Or, start typing in the search box to have Cost Explorer autocomplete your selection. After you choose your filters, choose **Apply filters**.

> **Note**
>
> Each time that you apply filters to your costs, Cost Explorer creates a new chart. However, you can use your browser's bookmark feature to save configuration settings for repeated use. Forecasts aren't saved, and Cost Explorer displays the most recent forecast when you revisit your saved chart.

You can continue refining your cost analysis by using multiple filters, grouping your data by filter type, and choosing **Advanced Options** tab options.

Combining filters to show data in common

Cost Explorer displays a chart that represents the data in common to all the filters that you have selected. You can use this view to analyze subsets of cost data. For example, assume that you set the **Service** filter to show costs that are related to Amazon EC2 and Amazon RDS services and then select **Reserved** using the filter. The cost chart will show how much money **Reserved** instances on Amazon EC2 and Amazon RDS cost for each of the three months.

> **Note**
>
> - AWS Cost and Usage Reports in Cost Explorer can use a maximum of 1024 filters.
> - You can filter RI Utilization reports by only one service at a time. You can do this only for the following services:
>   - Amazon EC2
>   - Amazon Redshift
>   - Amazon RDS
>   - ElastiCache
>   - OpenSearch Service

Filters and logical operations (AND/OR)

When you select multiple filters and multiple values for each filter, Cost Explorer applies rules that emulate the logical AND and OR operators to your selections. Within each filter, Cost Explorer emulates the logical OR filter to your selection of filter types. This means that the resulting chart adds the aggregate costs for each item together. Using the previous example, you see bars for both of the selected services, Amazon EC2 and Amazon RDS.

When you select multiple filters, Cost Explorer applies the logical AND operator to your selections. For a more concrete example, assume that you use the **Services** filter and specify Amazon EC2 and Amazon RDS costs for inclusion and then also apply the **Purchase Options** filter to select a single type of purchase option. You will see *only* the **Non-Reserved** charges incurred by Amazon EC2 and Amazon RDS.

Filter and group options

In Cost Explorer, you can filter by the following groups:

API operation

Requests made to and tasks performed by a service, such as write and get requests to Amazon S3.

Availability Zone

Distinct locations within a Region that are insulated from failures in other Availability Zones. They provide inexpensive, low-latency network connectivity to other Availability Zones in the same Region.

Billing entity

Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services. Possible values include:

- AWS: Identifies a transaction for AWS services other than in AWS Marketplace.
- AWS Marketplace: Identifies a purchase in AWS Marketplace.

Charge type

Different types of charges or fees.

- **Credit**: Any AWS credits that are applied to your account.

- **Other out-of-cycle charges**: Any subscription charges that aren't upfront reservation charges or support charges.
- **Recurring reservation fee**: Any recurring charges to your account. When you purchase a Partial Upfront or No Upfront Reserved Instance from AWS, you pay a recurring charge in exchange for a lower rate for using the instance. The recurring fees can result in spikes on the first day of every month, when AWS charges your account.
- **Refund**: Any refunds that you received. Refunds are listed as a separate line item in the data table. They don't appear as an item in the chart because they represent a negative value in the calculation of your costs. The chart displays only positive values.
- **Reservation applied usage**: Usage that AWS applied reservation discounts to.
- **Savings Plan covered usage**: Any on-demand cost that's covered by your Savings Plan. In an Unblended costs view, this represents the covered usage at on-demand rates. In an Amortized costs view, this represents the covered usage at your Savings Plan rates. Savings Plan covered usage line items are offset by the corresponding Savings Plan negation items.
- **Savings Plan negation**: Any offset cost through your Savings Plan benefit that’s associated with the corresponding Savings Plan covered usage item.
- **Savings Plan recurring fee**: Any recurring hourly charges that correspond with your No Upfront or Partial Upfront Savings Plan. The Savings Plan recurring fee is initially added to your bill on the day that you purchase a No Upfront or Partial Upfront Savings Plan. After the initial purchase, AWS adds the recurring fee hourly.

  For an All Upfront Savings Plan, the line item indicates the portion of the Savings Plan unused during the billing period. For example, if a Savings Plan was 100% utilized for a billing period, this shows as “0” in your amortized costs view. Any number greater than “0” indicates an unused Savings Plan.
- **Savings Plan upfront fee**: Any one-time upfront fee from your purchase of an All Upfront or Partial Upfront Savings Plan.
- **Support fee**: Any charges that AWS charges you for a support plan. When you purchase a support plan from AWS, you pay a monthly charge in exchange for service support. The monthly fees can result in spikes on the first day of every month, when AWS charges your account.
- **Tax**: Any taxes that are associated with the charges or fees in your cost chart. Cost Explorer adds all taxes together as a single component of your costs. If you select five or fewer filters, Cost Explorer displays your tax expenses as a single bar. If you select six or more filters, Cost

Explorer displays five bars, stacks, or lines, and then aggregates all remaining items, including taxes, into a sixth bar, stack slice, or plot line that's labeled **Other**.

If you choose to omit **RI upfront fees**, **RI recurring charges**, or **Support charges** from your chart, Cost Explorer continues to include any taxes that are associated with the charges.

Cost Explorer displays your tax costs in the chart only when you choose **Monthly** drop down. When you filter your cost chart, the following rules govern the inclusion of taxes:

1. Taxes are excluded if you select non-**Linked Account** filters, either singly or in combination with other filters.
2. Taxes are included if you select the **Linked Accounts** filters.

- **Upfront reservation fee**: Any upfront fees that are charged to your account. When you purchase an All Upfront or Partial Upfront Reserved Instance from AWS, you pay an upfront fee in exchange for a lower rate for using the instance. The upfront fees can result in spikes in the chart for the days or months when you make your purchases.
- **Usage**: Usage that AWS didn't apply reservation discounts to.

Instance type

The type of RI that you specified when you launched an Amazon EC2 host, Amazon RDS instance class, Amazon Redshift node, or Amazon ElastiCache node. The instance type determines the hardware of the computer used to host your instance.

Legal entity

The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. The values might differ for third-party AWS Marketplace transactions. Possible values include:

- Amazon Web Services, Inc. – The entity that sells AWS services.
- Amazon Web Services India Private Limited – The local Indian entity that acts as a reseller for AWS services in India.

Linked account

The member accounts in an organization. For more information, see Consolidated billing for AWS Organizations.

Platform

The operating system that your RI runs on. **Platform** is either **Linux** or **Windows**.

Product attribute

Standardized attributes that describe your Amazon Bedrock usage. You can filter and group your Amazon Bedrock costs by the following attributes:

- **Provider** (`provider`) is the company that offers the model, such as Anthropic, Cohere, or OpenAI.
- **Model** (`model`) is the model name, such as Claude Sonnet 5 or Claude Haiku 4.5.
- **Inference type** (`inferenceType`) is the type of usage, such as input tokens, output tokens, or prompt cache read input tokens.
- **Feature** (`feature`) is how the model was used, such as on-demand inference.

Costs that don't have a value for the selected attribute are grouped together.

> **Note**
>
> Product attribute data is available starting September 1, 2026.

Purchase option

The method you choose to pay for your Amazon EC2 instances. This includes Reserved Instances, Spot Instances, Scheduled Reserved Instances, and On-Demand Instances.

Region

The geographic areas where AWS hosts your resources.

Resources

The unique identifier for your resources.

> **Note**
>
> To enable resource granularity, opt-in through on the Cost Explorer settings page as the management account. This is available for Amazon EC2 instances.

Service

AWS products. To learn what's available, see AWS Products and Services. You can use this dimension to filter costs by specific AWS Marketplace software, including your costs for

AMIs, web services, and desktop apps. See the What is AWS Marketplace? guide for more information.

> **Note**
>
> You can only filter RI Utilization reports by one service at a time and only for these services: **Amazon EC2**, **Amazon Redshift**, **Amazon RDS**, and **ElastiCache**.

Tag

A label that you can use to track the costs associated with specific areas or entities within your business. For more information about working with tags, see Applying User-Defined Cost Allocation Tags and User attributes for Cost Allocation, and Account tags for Cost Allocation.

Tenancy

Specifies if the Amazon EC2 instance is hosted on shared or single-tenant hardware. Some tenancy values include **Shared (Default)**, **Dedicated**, and **Host**.

Usage type

Usage types are the units that each service uses to measure the usage of a specific type of resource. For example, the `BoxUsage:t2.micro(Hrs)` usage type filters by the running hours of Amazon EC2 `t2.micro` instances.

Usage type group

Usage type groups are filters that collect a specific category of usage type filters into one filter. For example, `BoxUsage:c1.medium(Hrs)`, `BoxUsage:m3.xlarge(Hrs)`, and `BoxUsage:t1.micro(Hrs)` are all filters for Amazon EC2 instance running hours, so they are collected into the `EC2: Running Hours` filter.

Usage type groups are available for DynamoDB, Amazon EC2, ElastiCache, Amazon RDS, Amazon Redshift, and Amazon S3. The specific groups available to your account depend on what services you've used. The list of groups that might be available includes but isn't limited to the following:

- **DDB: Data Transfer - Internet (In)**

  Filters by the costs associated with how many GB are transferred to your DynamoDB databases.

- **DDB: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from your DynamoDB databases.

- **DDB: Indexed Data Storage**

  Filters by the costs associated with how many GB that you have stored in DynamoDB.

- **DDB: Provisioned Throughput Capacity - Read**

  Filters by the costs associated with how many units of read capacity that your DynamoDB databases used.

- **DDB: Provisioned Throughput Capacity - Write**

  Filters by the costs associated with how many units of write capacity that your DynamoDB databases used.

- **EC2: CloudWatch - Alarms**

  Filters by the costs associated with how many CloudWatch alarms that you have.

- **EC2: CloudWatch - Metrics**

  Filters by the costs associated with how many CloudWatch metrics that you have.

- **EC2: CloudWatch - Requests**

  Filters by the costs associated with how many CloudWatch requests that you make.

- **EC2: Data Transfer - CloudFront (Out)**

  Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a CloudFront distribution.

- **EC2: Data Transfer - CloudFront (In)**

  Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a CloudFront distribution.

- **EC2: Data Transfer - Inter AZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between your Amazon EC2 instances in different AZs.

- **EC2: Data Transfer - Internet (In)**

Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from outside the AWS network.

- **EC2: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from an Amazon EC2 instance to a host outside the AWS network.

- **EC2: Data Transfer - Region to Region (In)**

  Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a different AWS Region.

- **EC2: Data Transfer - Region to Region (Out)**

  Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a different AWS Region.

- **EC2: EBS - I/O Requests**

  Filters by the costs associated with how many I/O requests that you make to your Amazon EBS volumes.

- **EC2: EBS - Magnetic**

  Filters by the costs associated with how many GB that you have stored on Amazon EBS Magnetic volumes.

- **EC2: EBS - Provisioned IOPS**

  Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon EBS.

- **EC2: EBS - SSD(gp2)**

  Filters by the costs associated with how many GB per month of General Purpose storage that your Amazon EBS volumes use.

- **EC2: EBS - SSD(io1)**

  Filters by the costs associated with how many GB per month of Provisioned IOPS SSD storage that your Amazon EBS volumes use.

- **EC2: EBS - Snapshots**

Filters by the costs associated with how many GB per month that your Amazon EBS snapshots store.

- **EC2: EBS - Optimized**

  Filters by the costs associated with how many MB per instance hour that your Amazon EBS-optimized instances use.

- **EC2: ELB - Running Hours**

  Filters by the costs associated with how many hours that your Elastic Load Balancing load balancers ran.

- **EC2: Elastic IP - Additional Address**

  Filters by the costs associated with how many Elastic IP addresses that you attached to running Amazon EC2 instances.

- **EC2: Elastic IP - Idle Address**

  Filters by the costs associated with Elastic IP addresses that you have that aren't attached to running Amazon EC2 instances.

- **EC2: NAT Gateway - Data Processed**

  Filters by the costs associated with how many GB that your network address translation gateways (NAT gateways) processed.

- **EC2: NAT Gateway - Running Hours**

  Filters by the costs associated with how many hours that your NAT gateways ran.

- **EC2: Running Hours**

  Filters by the costs associated with how many hours that your Amazon EC2 instances ran.

  This **Usage Type Group** contains only the following **Usage Types**:

  - BoxUsage
  - DedicatedUsage
  - HostBoxUsage
  - HostUsage
  - ReservedHostUsage
  - SchedUsage

  - SpotUsage
  - UnusedBox
- **ElastiCache: Running Hours**

  Filters by the costs associated with how many hours that your Amazon ElastiCache nodes ran.
- **ElastiCache: Storage**

  Filters by the costs associated with how many GB that you stored in Amazon ElastiCache.
- **RDS: Running Hours**

  Filters by the costs associated with how many hours that your Amazon RDS databases ran.

  This **Usage Type Group** contains only the following **Usage Types**:
  - AlwaysOnUsage
  - BoxUsage
  - DedicatedUsage
  - HighUsage
  - InstanceUsage
  - MirrorUsage
  - Multi-AZUsage
  - SpotUsage
- **RDS: Data Transfer – CloudFront – In**

  Filters by the costs associated with how many GB are transferred into Amazon RDS from a CloudFront distribution.
- **RDS: Data Transfer – CloudFront – Out**

  Filters by the costs associated with how many GB are transferred from a CloudFront distribution to Amazon RDS data transfers.
- **RDS: Data Transfer – Direct Connect Locations – In**

  Filters by the costs associated with how many GB are transferred into Amazon RDS through a Direct Connect network connection.
- **RDS: Data Transfer – Direct Connect Locations – Out**

Filters by the costs associated with how many GB are transferred from Amazon RDS through a Direct Connect network connection.

- **RDS: Data Transfer – InterAZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between Amazon RDS buckets in different Availability Zones.

- **RDS: Data Transfer – Internet – In**

  Filters by the costs associated with how many GB are transferred to your Amazon RDS databases.

- **RDS: Data Transfer – Internet – Out**

  Filters by the costs associated with how many GB are transferred from your Amazon RDS databases.

- **RDS: Data Transfer – Region to Region – In**

  Filters by the costs associated with how many GB are transferred to your Amazon RDS instances from a different AWS Region.

- **RDS: Data Transfer – Region to Region – Out**

  Filters by the costs associated with how many GB are transferred from your Amazon RDS instances to a different AWS Region.

- **RDS: I/O Requests**

  Filters by the costs associated with how many I/O requests that you make to your Amazon RDS instance.

- **RDS: Provisioned IOPS**

  Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon RDS.

- **RDS: Storage**

  Filters by the costs associated with how many GB that you have stored in Amazon RDS.

- **Redshift: DataScanned**

  Filters by the costs associated with how many GB that your Amazon Redshift nodes scanned.

- **Redshift: Running Hours**

Filters by the costs associated with how many hours that your Amazon Redshift nodes ran.

- **S3: API Requests - Standard**

  Filters by the costs associated with GET and all other standard storage Amazon S3 requests.

- **S3: Data Transfer - CloudFront (In)**

  Filters by the costs associated with how many GB are transferred into Amazon S3 from a CloudFront distribution.

- **S3: Data Transfer - CloudFront (Out)**

  Filters by costs associated with how many GB are transferred from a CloudFront distribution to Amazon S3 data transfers, such as how much data was uploaded from your Amazon S3 bucket to your CloudFront distribution.

- **S3: Data Transfer - Inter AZ**

  Filters by the costs associated with how many GB are transferred into, out of, or between Amazon S3 buckets in different Availability Zones.

- **S3: Data Transfer - Internet (In)**

  Filters by the costs associated with how many GB are transferred to an Amazon S3 bucket from outside the AWS network.

- **S3: Data Transfer - Internet (Out)**

  Filters by the costs associated with how many GB are transferred from an Amazon S3 bucket to a host outside the AWS network.

- **S3: Data Transfer - Region to Region (In)**

  Filters by the costs associated with how many GB are transferred to Amazon S3 from a different AWS Region.

- **S3: Data Transfer - Region to Region (Out)**

  Filters by the costs associated with how many GB are transferred from Amazon S3 to a different AWS Region.

- **S3: Storage - Standard**

  Filters by the costs associated with how many GB that you have stored in Amazon S3.

Choosing advanced options

You can customize how you view your data in Cost Explorer using **Advanced options** to include or exclude specific types of data.

To include or exclude data

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Explorer**.
3. In the right pane, under **Advanced options**, under **Aggregate costs by**, choose between the following:

   - **Unblended costs**: This cost metric reflects the cost of the usage. When grouped by **Charge type**, unblended costs separate discounts into their own line items. This enables you to view the amount of each discount received.
   - **Amortized costs**: This cost metric reflects the effective cost of the upfront and monthly reservation fees spread across the billing period. By default, Cost Explorer shows the fees for Reserved Instances as a spike on the day that you're charged. However, if you choose to show costs as amortized costs, the costs are amortized over the billing period. This means that the costs are broken out into the effective daily rate. AWS estimates your amortized costs by combining your unblended costs with the amortized portion of your upfront and recurring reservation fees. For the daily view, Cost Explorer shows the unused portion of your upfront reservation fees and recurring RI charges on the first of the month.

     For example, suppose that Alejandro purchases a Partial Upfront `t2.micro` RI for a one-year term at $30 dollars upfront. The monthly fee is $2.48. Cost Explorer shows the costs for this RI as a spike on the first of the month. If Alejandro chooses **Amortized costs** for a 30-day month, the Cost Explorer chart shows a daily effective rate of $0.165. This is the EC2 effective rate multiplied by the number of hours in a day.

     Amortized costs aren't available for billing periods before 2018. If you want to see how much of your reservation was unused, group by purchase option.
   - **Blended costs**: This cost metric reflects the average cost of usage across the consolidated billing family. If you use the consolidated billing feature in AWS Organizations, you can view costs using *blended rates*. For more information, see Blended Rates and Costs.
   - **Net unblended costs**: This cost metric reflects the cost after discounts.

- **Net amortized costs**: This cost metric amortizes the upfront and monthly reservation fees while including discounts such as RI volume discounts.

4. Under **Additional data settings**, select from the following:

- **Show forecasted values**: Cost Explorer displays a forecast for how much AWS predicts you will spend over the forecast time period that you select, based on your past costs.
- **Show only untagged resources**: By default, Cost Explorer includes costs both for resources that have cost allocation tags and for resources that don't have cost allocation tags. To find untagged resources that add to your costs, select **Show only untagged resources**. For more information about cost allocation tags, see Organizing and tracking costs using AWS cost allocation tags.
- **Show only uncategorized resources**: By default, Cost Explorer includes costs both for resources that are mapped to a cost category and for resources that aren't mapped to a cost category. To find uncategorized resources that add to your costs, select **Show only uncategorized resources**. For more information about cost categories, see Organizing costs using AWS Cost Categories.

Reading the Cost Explorer data table

A data table follows each Cost Explorer chart. The data table displays the cost figures that the chart represents. If your chart is using a grouping, the data table displays the aggregate amounts for the filter types that you choose for your chart. If your chart isn't using a grouping, the table displays the aggregate amounts for your past and forecasted cost data. You can download the .csv file that contains the complete data set for your chart.

> **Note**
>
> For the RI Utilization and Savings report, the maximum table size is 20 rows. If the data exceeds this, it appears in a truncated form.

In the grouped data table, each row is a value for one of the filter type options: API operations, Availability Zones, AWS services, custom cost allocation tags, instance types, member accounts, purchase options, Region, usage type, or usage type group. The columns represent time intervals. For example, the data table shows the costs for selected services for the last three months in separate columns. Then, the last column of the data table shows the aggregated total for the 3 months.

> **Note**
>
> Data transfer costs are included in the services that they're associated with, such as Amazon EC2 or Amazon S3. They aren't represented as either a separate line item in the data table or a bar in the chart.

In the ungrouped data table, the row is your costs. The columns represent time intervals.

Forecasting with Cost Explorer

You create a forecast by selecting a future time range for your report. For more information, see Choosing time ranges for the data that you want to view. The following section discusses the accuracy of the forecasts created by Cost Explorer and how to read them.

A forecast is a prediction of how much you will use AWS services over the forecast time period that you selected. This forecast is based on your past usage. You can use a forecast to estimate your AWS bill and set alarms and budgets for based on predictions. Because forecasts are predictions, the forecasted billing amounts are estimated and might differ from your actual charges for each statement period.

Like weather forecasts, billing forecasts can vary in accuracy. Different ranges of accuracy have different prediction intervals. The higher the prediction interval, the more likely the forecast has a wider range. For example, suppose that you have a budget set to 100 dollars for a given month. An 80% prediction interval might forecast your spend between 90 and 100, with a mean of 95. The range in the prediction band is dependent on your historical spend volatility, or fluctuations. The more consistent and predictable the historical spend, the narrower the prediction range in forecast spend.

Cost Explorer forecasts have a prediction interval of 80%. If AWS doesn't have enough data to forecast an 80% prediction interval, Cost Explorer doesn't provide a forecast. This is common for accounts that have less than one full billing cycle.

Reading forecasts

How you read the Cost Explorer forecasts depends on the type of chart that you're using. Forecasts are available for both line charts and bar charts.

The 80% prediction interval appears differently on each type of chart:

- Line charts represent the prediction interval as a set of lines that are on either side of your costs line.
- Bar charts represent the prediction interval as two lines that are on either side of the top of your bar.

When forecasting costs, discounts are included by default.

> **Note**
>
> If you want your forecasts to include non-recurring discounts such as refunds, we encourage you to use **Show net unblended costs**. For more information about different costs, see Cost Explorer Advanced Options.

Using forecasts with consolidated billing

If you use the consolidated billing feature in AWS Organizations, the forecasts are calculated with the data from all the accounts. If you add a new member account to an organization, forecasts don't include that new member account until the new spending patterns of the organization are analyzed. For more information about consolidated billing, see Consolidated billing for AWS Organizations.

Understanding your forecasts with AI explanations

Cost Explorer provides AI-powered explanations that help you understand the key drivers behind your forecast predictions. You can access forecast explanations by configuring a future date range in Cost Explorer and clicking **Analyze with Amazon Q**. Amazon Q Developer delivers detailed forecast explanations covering projected spending trajectories, service-level breakdowns, and the factors influencing your projections. You can ask follow-up questions to understand why specific services are projected to increase or decrease. For more information, see the section called “Using Analyze with Amazon Q”.

> **Note**
>
> You can also ask questions about your forecasted costs using the suggested prompts or the **Ask question** button in Cost Explorer, powered by **Amazon Q Developer**. When viewing future dates, forecast related suggested prompts appear automatically. For more

information, see the section called “Asking questions about your costs using Amazon Q Developer”.

Asking questions about your costs using Amazon Q Developer

Cost Explorer enables you to ask questions about your AWS costs using suggested prompts or in your own words via the **Ask question** button, powered by **Amazon Q Developer**. You can receive detailed insights in **Amazon Q Developer** while Cost Explorer automatically updates its charts, tables, and report parameters including filters, groupings, and dates to reflect the analysis. This capability is available through two features: suggested prompts and the **Ask question** button.

Topics

- Using suggested prompts
- Using the Ask question button
- Understanding visualization updates
- Using Analyze with Amazon Q
- Continuing the conversation with follow-up questions
- Permissions

Using suggested prompts

Cost Explorer displays suggested prompts above your Cost & Usage Overview data. These prompts surface the most commonly asked cost questions, such as "Show me my top spending services this month" or "Show my projected database cost for next month." You can click any prompt to instantly receive insights from **Amazon Q Developer** without needing to type a question.

When you click a suggested prompt, the following occurs:

1. The **Amazon Q Developer** chat panel opens automatically.
2. The prompt is submitted to **Amazon Q Developer** without requiring additional input.
3. **Amazon Q Developer** generates detailed insights in the chat panel.
4. Cost Explorer refreshes with the corresponding visualization, and all report parameters including filters, groupings, and date ranges are automatically configured in the **Report Parameters** panel.

Each time you load the page or complete a query, the prompts refresh with new suggestions. When you click a prompt during a session, it is replaced with a new prompt, ensuring you always have fresh analytical options to explore. You can scroll horizontally through the prompt container to discover additional suggestions beyond those initially visible.

Using the Ask question button

For questions that go beyond the suggested prompts, the **Ask question** button is positioned next to the suggested prompts. When you click this button, the **Amazon Q Developer** chat panel opens and you can type any cost related question in your own words, such as "What is my current month's cost and usage compared to the previous month?" or "Show me my EC2 costs broken down by instance type for the last 3 months."

Amazon Q Developer processes your question and delivers insights in the chat panel while determining how to display the visualization. Cost Explorer automatically updates charts and tables when analysis is based on your cost and usage data. When **Amazon Q Developer** compiles insights from additional datasets such as pricing or anomaly detection, visualizations are displayed in **Amazon Q Developer**'s new artifacts panel.

Understanding visualization updates

When you interact with suggested prompts or the **Ask question** button, Cost Explorer automatically updates its charts and tables when the analysis is based on your cost and usage data. All corresponding report parameters, including filters, groupings, and date ranges, are visible in the **Report Parameters** panel so you can verify exactly which data subset is included in the analysis.

When **Amazon Q Developer** draws from additional datasets to provide richer analysis, visualizations are displayed in **Amazon Q Developer**'s artifacts panel alongside the chat.

After **Amazon Q Developer** updates your Cost Explorer view, you can:

- Save the view as a Cost Explorer report.
- Share the URL with colleagues. All filters are preserved in the URL.
- Bookmark the view for future reference.
- Export the data to CSV for further analysis.
- Manually adjust any of the filters and groupings in the **Report Parameters** panel to refine your view.

Using Analyze with Amazon Q

When you configure a cost report in Cost Explorer with your preferred filters, date range, and groupings, you can click **Analyze with Amazon Q** to receive a comprehensive explanation of what you're viewing. **Amazon Q Developer** analyzes the complete context of your current cost report and delivers detailed explanations in its chat panel.

When you click **Analyze with Amazon Q**, the following occurs:

1. The **Amazon Q Developer** chat panel opens automatically.
2. A prompt is auto-submitted based on your current view's time period.
3. **Amazon Q Developer** analyzes your cost data based on your applied Report Parameters (filters, dimensions, granularity, and date range).
4. A comprehensive explanation is delivered in the chat panel covering cost trends, top drivers, anomalies, and guidance to explore optimization opportunities.

Your Cost Explorer view remains unchanged. The analysis appears only in the **Amazon Q Developer** chat panel.

The analysis adapts based on the time period you are viewing:

- **Historical dates**: When your cost report covers past dates, **Amazon Q Developer** explains what drove your cost changes, identifies top cost drivers with specific amounts and percentages, and surfaces anomalies detected by AWS Cost Anomaly Detection with explanations of their likely causes.
- **Future dates**: When your cost report covers future dates, **Amazon Q Developer** delivers forecast explanations covering projected spending trajectories, the services expected to drive future costs with service-level breakdowns, and the factors influencing your projections. Anomalies are not included for future-only periods.
- **Mixed periods**: When your cost report spans both historical and future dates, **Amazon Q Developer** provides a unified explanation covering both what happened in the past and what is projected going forward.
- **Compare mode**: When you are using the Cost Explorer Compare feature (month over month or custom month selection), clicking **Analyze with Amazon Q** delivers a comparison analysis identifying the largest cost changes between the two selected months, with anomaly detection.

After receiving your initial analysis, you can ask follow-up questions to explore any finding in greater detail. For example, you can ask "Tell me more about the anomalies detected this month" or "What are my optimization opportunities?" **Amazon Q Developer** maintains the full context of your conversation, allowing you to progressively drill deeper into your cost data.

> **Note**
>
> **Analyze with Amazon Q** does not update your Cost Explorer visualization. Your configured view remains exactly as you set it. All analysis output appears only in the **Amazon Q Developer** chat panel.

> **Note**
>
> For historical and compare analyses, the response includes guidance to discover optimization opportunities through follow-up questions. When you ask about optimization opportunities, **Amazon Q Developer** provides recommendations from Cost Optimization Hub.

Continuing the conversation with follow-up questions

After clicking a suggested prompt or asking a question using the **Ask question** button, you can continue the dialogue in **Amazon Q Developer** to drill deeper into your costs. For example, after seeing your top spending services, you might ask "Why did my RDS costs increase last month?" or "Break this down by region." **Amazon Q Developer** maintains the conversation context, allowing natural exploration of your cost data.

Amazon Q Developer draws from extensive knowledge beyond what is visible in your current Cost Explorer view, including pricing data, budget information, and anomaly detection data, to provide richer context and more comprehensive answers. If a follow-up question produces a visualization that Cost Explorer can display, it updates automatically. Otherwise, the visualization appears in **Amazon Q Developer**'s artifacts panel while insights continue in the chat.

Permissions

To use the suggested prompts and **Ask question** button in Cost Explorer, you need the following permissions in addition to your existing Cost Explorer permissions:

- **Amazon Q Developer permissions**: `q:StartConversation`, `q:SendMessage`
- **Pass request permission**: `q:PassRequest`, which allows **Amazon Q Developer** to call AWS APIs on your behalf

For least-privilege access, create a custom IAM policy that grants only `q:StartConversation`, `q:SendMessage`, and `q:PassRequest`. Alternatively, administrators who already use **Amazon Q Developer** across multiple integrations can use the `AmazonQFullAccess` managed policy, which includes these permissions along with broader **Amazon Q Developer** access. The integration respects all existing IAM boundaries. **Amazon Q Developer** only accesses cost data you are authorized to view through Cost Explorer.

For detailed permission configurations and security considerations, see the section called "Security and privacy".

> **Note**
>
> Organizations can restrict access to the suggested prompts and **Ask question** button while maintaining Cost Explorer access using IAM condition keys. For more information, see the Amazon Q Developer security documentation.

Comparing your costs between time periods

Cost Comparison is a feature in Cost Explorer that helps you quickly identify and understand changes in your AWS spending. It automatically analyzes cost variations between two selected months, highlighting the largest cost drivers and explaining the reasons behind these changes. The feature provides both console and API access to help you analyze cost changes across your AWS spending.

Key benefits:

- Quickly identifies top cost changes across services, accounts, and Regions.
- Provides detailed breakdowns of cost drivers, including usage and discount changes.
- Reduces manual cost analysis time from hours to seconds.
- Available in Cost Explorer at no additional cost.

Permissions

To access data in the Cost Comparison feature, you need the following IAM permissions:

- `ce:GetCostAndUsageComparisons`
- `ce:GetCostComparisonDrivers`

These permissions enable you to retrieve cost and usage comparisons and cost drivers.

Accessing the console

To analyze your cost changes in the console, you can use either the **Top trends** widget or Cost Explorer.

To access the console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Do either of the following:
   - On the console home page, view the **Top trends** widget, which shows the top 10 cost variations between the previous two months.
   - In the navigation pane, choose **Cost Explorer**, and then choose **Compare** in the **Report parameters** panel.

Review the **Top Trends** widget regularly to identify significant cost changes early. For more information about this widget, see Top trends.

Understanding how a cost comparison works

You can use Cost Comparison to quickly understand your cloud spending by automatically identifying and unfolding the largest cost drivers driving the cost variations between two selected months. Cost Comparison provides a detailed breakdown for these cost variances, from usage shifts to changes in commitment-based discounts like Savings Plans coverage and applied credits, eliminating hours of manual investigation.

The **Top trends** widget on the console home page automatically applies Cost Comparison to show the top cost changes across your services, accounts, and Regions. For more information about this widget, see Top trends.

You can use Cost Comparison in two main ways:

- Query for any two months (referred to as baseline and comparison months) across any Cost Explorer dimension and cost metric. Cost Comparison analyzes your costs by:
  - Calculating the total cost for each selected dimension in the baseline month.
  - Comparing these with costs in the comparison month.
  - Ranking each resulting dimension value by the absolute cost difference.
  - Returning the top 10 increases or decreases for each dimension.

  Example:

  In the following example, Cost Comparison identified four services that demonstrated the largest change when comparing costs from March 2025 (comparison month) with April 2025 (baseline month):

Service	March 2025	April 2025	Change
Amazon RDS	$8,787.98	$72,124.46	+$63,336.48
SageMaker	$16,523.00	$31,890.00	+$15,367.00
Amazon Connect	$5,144.00	$17,902.00	+$12,758.00
EC2	$68,708.00	$60,463.00	-$8,245.00

- Request detailed cost drivers for the cost change associated with a specific service, account, Region, or other dimension value. Cost Comparison:
  - Identifies the specific usage type driving the largest change.
  - Calculates the total cost for each charge type in the baseline and comparison months.
  - Ranks the results by absolute cost difference.
  - Provides a breakdown of cost changes for each charge type, allowing for targeted cost savings opportunities.

  Example:

  In the following example, Cost Comparison identified two RDS instances in Frankfurt, Germany (Europe Region) that accounted for a $63,336.48 cost difference between the selected months. For each instance, Cost Comparison identified additional cost drivers and their impact. The first

instance (EU-InstanceUsage:db.r6g.8xl) showed increased cost and usage alongside decreased reserved capacity coverage, suggesting an opportunity to purchase additional reservations if the higher usage is expected to continue. The second instance (EU-InstanceUsage:db.t4g.xl) showed increased cost and usage with a decrease in applied credits compared to the previous month. This instance requires investigation into both the usage increase to evaluate potential reserved capacity purchases and the unexpected reduction in credits.

Cost drivers							
Service	**Usage type**		**Baseline**	**Comparison**	**Difference**	**Unit**	**Console only explanation of cost drivers**
Amazon RDS	EU-InstanceUsage:db.r6g.8xl	USAGE_CHANGE	4,599.11	36,855.11	32,256.00	USD	+32,256.00 cost change for Amazon RDS: EU-InstanceUsage:db.r6g.8xl • On-Demand usage increased by 701.4%, leading to a $32,256.00 increase in costs •
Amazon RDS		USAGE_CHANGE	995.01	8,034.73	7,039.72	Hours	
Amazon RDS		RESERVATION_APPLIED_USAGE_CHANGE	1,236.99	646.04	-590.95	Hours	

Cost drivers							
Service	**Usage type**		**Baseline**	**Comparison**	**Difference**	**Unit**	**Console only explanation of cost drivers**
							The usage covered by Reserved Instances decreased by 47.77%

Cost drivers							
Service	**Usage type**		**Baseline**	**Comparison**	**Difference**	**Unit**	**Console only explanation of cost drivers**
Amazon RDS	EU-InstanceUsage:db.t4g.8xl	USAGE_CHANGE	5,386.21	36,047.21	30,661.00	USD	+30,661.00 cost change for Amazon RDS: EU-InstanceUsage:db.t4g.8xl • On-Demand usage increased by 569.2%, leading to a $30,661.00 increase in costs • Credits applied
Amazon RDS		USAGE_CHANGE	1,074.66	7,192.18	6,117.52	Hours	
Amazon RDS		CREDIT_USAGE_CHANGE	1,157.34	737.86	-419.48	USD	

Cost drivers							
Service	**Usage type**		**Baseline**	**Comparison**	**Difference**	**Unit**	**Console only explanation of cost drivers**
							decreased from $1,157.34 to $737.86, a 36% decrease

If you need to analyze cost changes for specific areas of your business, choose filters to focus on other dimensions like tags or cost categories. Cost Comparison supports all of the available cost metrics (unblended, net unblended, net amortized, etc.) options in Cost Explorer, giving you flexibility to view the data in the way that is most meaningful for your needs. Cost Comparison dynamically updates the drivers based on the specific cost metrics or dimensions you select.

Performing a cost comparison

You can compare costs between any two months within the last 13 months to identify and understand changes in your AWS spending. If you have enabled multi-year data at monthly granularity, you can go back up to 38 months. For more information, see Configuring multi-year and granular data.

> **Note**
>
> To access data in the Cost Comparison feature, you need IAM permissions. For more information, see Permissions.

To perform a detailed cost comparison

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Explorer**.
3. In the **Report parameters** panel, choose **Compare**.
4. For **Date range**, choose between:
   - **Relative (Month over month)**: Compare current month to previous month.
   - **Absolute (Custom)**: Compare any two months within the last 13 months (or up to 38 months if you have enabled multi-year data at monthly granularity).
5. Under **Group by**, choose a **Dimension** (for example, Service, Linked account, Region, Tag).

   > **Note**
   >
   > Group by resource is not available for cost comparisons.

6. Apply additional filters to narrow your analysis to specific services, accounts, or other cost dimensions.

   > **Note**
   >
   > Filter by resource is not available for cost comparisons.

7. View the detailed breakdown of cost changes:
   - Examine the graph and table displaying the cost comparison between the two selected periods.
   - Review the top 3 cost comparison drivers automatically highlighted by Cost Explorer. These show the most significant factors contributing to cost changes, whether increases or decreases.
   - Choose **View all** to see a comprehensive list of all cost comparison drivers.
   - For each cost comparison driver, Cost Explorer provides specific reasons for the change in costs, including usage changes, discount changes, and other charge types (for example, fees, credits).

- Use the available Cost Explorer filters in **Report parameters** to analyze different aspects of your business. The graph and table are updated in real time, allowing you to analyze specific services, accounts, tags, or other dimensions to gain deeper insights into your cost changes.

Exploring more data for advanced cost analysis

Cost Explorer provides AWS cost and usage data for the current month and up to the previous 13 months at daily and monthly granularity. You can query this data in the console or using the Cost Explorer API.

You can enable multi-year data (at monthly granularity) and more granular data (at hourly and daily granularity) for the previous 14 days. Once enabled, you can use this data in the console or using the Cost Explorer API.

Topics

- Multi-year data at monthly granularity
- Granular data
- Understanding your estimated monthly usage summary
- Configuring multi-year and granular data

Multi-year data at monthly granularity

While you can use the default 14-month historical data to perform cost analysis at quarterly or monthly level, you should enable multi-year data in Cost Explorer if you want to evaluate your year-over-year cost or identify long-term cost trends.

You can enable up to 38 months of multi-year data at monthly granularity for your entire organization. Using multi-year data to perform cost analysis over a longer duration, you can track changes in your AWS costs as your business or applications mature, or after implementing infrastructure optimizations.

Once enabled, multi-year data is available within 48 hours. Note that this data is only available in Cost Explorer, as Savings Plans and Reservations utilization and coverage reports don't support this data.

To enable multi-year data in Cost Explorer, see Configuring multi-year and granular data.

> **Note**
>
> We will disable multi-year data for your organization if no one in the organization accesses it in three consecutive months. However, if you need the data, you can re-enable it in Cost Management preferences.
> Multi-year data is only available for chargeable costs in Cost Explorer. If you're onboarded to AWS Billing Conductor, you won't be able to use this feature.

Granular data

Cost Explorer provides hourly and resource-level granularity through three features:

- Resource-level data at daily granularity
- Cost and usage data for all AWS services at hourly granularity (without resource-level data)
- EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

Enable one or all of these features based on how you plan on using granular data for your in-depth cost and usage analysis.

To enable granular data in Cost Explorer, see Configuring multi-year and granular data.

> **Note**
>
> Granular data visibility is only available for billing views that show chargeable data. When you use Billing Conductor as an account in a standard billing group or billing transfer billing group, you can't view granular data in Cost Explorer.

Topics

- Resource-level data at daily granularity
- Cost and usage data for all AWS services at hourly granularity (without resource-level data)
- EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

Resource-level data at daily granularity

In Cost Explorer, you can enable resource-level data for your chosen AWS services at daily granularity for the past 14 days.

You can apply **Group by: Resource** to understand the cost of services by resource ID that you have enabled resource-level data for. Costs associated with services that you have not enabled resource-level data for appear under **No resource ID** in Cost Explorer. If you want to focus on resource-level costs for a specific service, choose the **Resource** filter in Cost Explorer, select the service you want to analyze, and then select all resources (if you don't have a specific resource in mind) or a specific resource ID to understand cost and usage driven by that specific resource.

Use resource-level data to identify your cost drivers. When analyzing variances or anomalies in your AWS costs, you can group by service to first understand which service is causing the variance or anomaly. Then you can filter for that service in Cost Explorer and group by resource to create a view of costs per resource in that service. Use the Cost Explorer table and graphs to understand which specific resource has deviated from the normal usage pattern and is contributing to the variance or anomaly. If you want to understand how your spend on a specific resource has evolved over time, such as your spend on an S3 bucket, you can filter for that resource in Cost Explorer by selecting that resource ID in the **Resource** filter. Moreover, resource-level data is useful in order to understand which specific resources are consuming your Savings Plans and Reservations commitments. To create this view, you can filter for "Savings Plan Covered Usage" or "Reservation applied usage" charge types, group by resource, and filter for specific services that you have purchased Savings Plans and Reservations for.

Once enabled, resource-level data at daily granularity is available within 48 hours. Note that this data is not available for Savings Plans and Reservations utilization and coverage reports.

> **Note**
>
> We will disable resource-level data at daily granularity for your organization if no one in the organization accesses it in three consecutive months. However, if you need the data, you can re-enable it in Cost Management preferences.
> Cost Explorer displays the top 5,000 most costly resources per service. If you have more than 5,000 resources, you might not see all of them in the console. However, you can search for those resources using the resource ID. Consider using Cost and Usage Reports (CUR) to retrieve the cost and usage associated with all resources as a CSV file.

Cost and usage data for all AWS services at hourly granularity (without resource-level data)

By default, Cost Explorer provides up to 14 months of data at daily and monthly granularity. However, you can opt in to hourly granularity for the past 14 days.

You can use hourly granularity to monitor cost and usage patterns at the most granular hourly level. Such data is especially useful to understand the peak hours for your AWS usage and how high the cost can go during those peak hours. If you're thinking about purchasing Savings Plans or Reserved Instances, hourly granularity can help you understand your average spend per hour so that you make optimal purchases. If you're thinking about fine tuning your architecture or planning to start a new project, enabling hourly granularity can help your developers monitor the performance of your architecture at hourly level and identify optimization opportunities.

Once enabled, data at hourly granularity is available within 48 hours in Cost Explorer, and in Savings Plans utilization and coverage reports.

EC2-Instances (Elastic Compute Cloud) resource-level data at hourly granularity

In Cost Explorer, you can enable EC2 resource-level data at hourly granularity for the past 14 days. Using this data, you can view your hourly cost and usage at each EC2 instance level in Cost Explorer. This helps you to understand cost and usage driven by each EC2 instance by grouping on resource and filtering your Cost Explorer view for the EC2 service.

Such data can help you analyze for variances or anomalies. For example, if you see a spike in your EC2 cost, you can use hourly granularity to pinpoint the hour when the variance started, and then group your cost by resource to understand which specific EC2 instance is causing the spike. The ability to identify the source of variance to the exact hour can help your developers understand which specific changes in their architecture caused this variance, or if this is an actual anomaly or valid spike due to increased traffic. If you're thinking about how many EC2 Reserved Instances you should buy, understanding the number and type of instances running each hour can be useful, as you can make an informed decision to ensure you get the maximum Reserved Instances utilization. If you currently have Savings Plans or Reserved Instances, enable EC2 resource-level data at hourly granularity to understand which specific instances used your Savings Plans or Reserved Instances.

Once enabled, EC2 resource-level data at hourly granularity is available within 48 hours. This data is not available for Savings Plans and Reservations utilization and coverage reports.

Understanding your estimated monthly usage summary

When you enable granular data in Cost Explorer, it increases the number of usage records Cost Explorer needs to host for your organization. To ensure Cost Explorer can respond to queries as quickly as possible, Cost Explorer limits the amount of granular data stored for your organization.

> **Note**
>
> If you enable hourly granularity for both **EC2-Instances (Elastic Compute Cloud - Compute) resource-level data** and **Cost and usage data for all AWS services at hourly granularity (without resource-level data)**, you will see a drop in the hourly usage records reported against **Cost and usage**. This is because the EC2 hourly usage records are moved and reported under **EC2-Instances**.

In Cost Management preferences, you can view the estimated usage records count for your granular data preference selections and understand how close you are to the Cost Explorer data limits. See "Understanding Cost Explorer data threshold limits".

Hourly granularity in Cost Explorer is a paid feature and the cost depends on your hourly usage records count. Understanding your estimated usage records count for hourly granularity features can help you estimate the cost of these features before enabling them. See "Estimating cost for Cost Explorer hourly granularity".

> **Note**
>
> The usage records displayed in Cost Management preferences are for your entire organization and are estimates based on your average past usage. The actual usage records in any given past, current, or future month might differ from these values. If you're a new AWS customer and haven't used AWS for at least a month, we can't estimate your usage records due to insufficient data.

Topics

- Understanding Cost Explorer data threshold limits
- Estimating cost for Cost Explorer hourly granularity

Understanding Cost Explorer data threshold limits

Cost Explorer supports up to 500 million usage records for resource-level data at daily granularity and up to 500 million usage records for hourly granularity features (EC2 resource-level data at hourly granularity and hourly granularity for all services without resources).

To make sure Cost Explorer can deliver an optimal customer experience, if your estimated usage records is above these limits, you'll receive a data threshold error and you won't be able to save your preferences.

If you receive the data threshold error while setting resource-level data at daily granularity, you can reduce the number of services you want to enable resource-level data for. If the error still persists, consider retrieving your data using Cost and Usage Reports (CUR). You can set CUR to include resource IDs.

If you receive the data threshold error while setting hourly granularity, consider choosing between hourly cost and usage data for all services without resource-level data and EC2 resource-level data at hourly granularity. If the error still persists, consider retrieving your data using Cost and Usage Reports (CUR). You can set CUR to get cost and usage information at hourly granularity with resource IDs.

Estimating cost for Cost Explorer hourly granularity

Cost Explorer offers hourly granularity data at a daily charge of $0.00000033 per usage record, which translates to $0.01 per 1,000 usage records monthly. A usage record corresponds to a line item with a specific resource and usage type.

Cost Explorer bills you daily based on the total hourly usage records hosted in Cost Explorer for the past 14 days. For example, if you run one EC2 instance all day every day for the past month, and you have hourly granularity enabled, Cost Explorer will host 336 records per day (24 hours x 14 days) and charge you $0.0001 daily ($0.00000033 per record x 336 records), resulting in a monthly bill of $0.003 ($0.0001 daily cost x 30).

For the provided estimated usage records count, you can calculate the cost yourself using the provided formula, or you can use AWS Pricing Calculator.

> **Note**
>
> Granular data visibility is only available for billing views that show chargeable data. When you use Billing Conductor as an account in a standard billing group or billing transfer billing group, you can't view granular data in Cost Explorer.

Configuring multi-year and granular data

Using the management account, you can enable multi-year data and granular data in Cost Explorer. You do this in the Cost Management preferences in the console.

However, in order to enable multi-year and granular data, you first need to manage access to view and edit your Cost Management preferences. See Controlling access using IAM.

> **Note**
>
> Granular data visibility is only available for billing views that show chargeable data. When you use Billing Conductor as an account in a standard billing group or billing transfer billing group, you can't view granular data in Cost Explorer.

To set up multi-year and granular data

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. To get historical data for up to 38 months, select **Multi-year data at monthly granularity**.
4. To enable resource-level or hourly granular data, consider the following options:

   > **Note**
   >
   > The hourly data as well as daily resource-level data is available for the past 14 days.

   - Hourly granularity
     - Select **Cost and usage data for all AWS services at hourly granularity** to get hourly data for all AWS services without resource-level data.

- Select **EC2-Instances (Elastic Compute Cloud) resource-level data** to track EC2 cost and usage at instance level at hourly granularity.

- Daily granularity
  - Select **Resource-level data at daily granularity** to get resource-level data for individual or all AWS services.
  - Choose services from the **AWS services at daily granularity** dropdown list that you want to enable resource-level data for.

> **Note**
>
> The dropdown list contains only those services that were used in your organization in the last six months. They are ranked starting with the costliest.

5. Choose **Save preferences**.

> **Note**
>
> It can take up to 48 hours for changes to your data settings to reflect in Cost Explorer. Also, after saving your preferences, you won't be able to make any additional changes for 48 hours.
> If the estimated data volume for your preferences is above the Cost Explorer limit, you'll receive an error stating that you have reached the data threshold limit and you won't be able to save your preferences. See "Understanding Cost Explorer data threshold limits".

Controlling access using IAM

You can use AWS Identity and Access Management (IAM) to manage access to your Cost Management preferences for individual users. You can then grant or revoke access on an individual level for each IAM role or user. You'll need to add the following actions in order to be able to view and edit preferences: `ce:GetPreferences`, `ce:UpdatePreferences`, `ce:GetDimensionValues`, and `ce:GetApproximateUsageRecords`.

The following is a sample IAM policy with the relevant actions that would provide you with access to view and edit your Cost Management preferences in order to enable multi-year and granular data:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences",
                "ce:GetDimensionValues",
                "ce:GetApproximateUsageRecords"
            ],
            "Resource": "*"
        }
    ]
}
```

Using the AWS Cost Explorer API

The Cost Explorer API allows you to programmatically query your cost and usage data. You can query for aggregated data such as total monthly costs or total daily usage. You can also query for granular data, such as the number of daily write operations for DynamoDB database tables in your production environment.

If you use a programming language that AWS provides an SDK for, we recommend that you use the SDK. All the AWS SDKs greatly simplify the process of signing requests and save you a significant amount of time when compared with using the AWS Cost Explorer API. In addition, the SDKs integrate easily with your development environment and provide easy access to related commands.

For more information about available SDKs, see Tools for Amazon Web Services. For more information about the AWS Cost Explorer API, see the AWS Billing and Cost Management API Reference.

Service endpoint

The Cost Explorer API provides the following endpoint:

https://ce.us-east-1.amazonaws.com

Granting IAM permissions to use the AWS Cost Explorer API

A user must be granted explicit permission to query the AWS Cost Explorer API. For the policy that grants the necessary permissions to a user, see View costs and usage.

Best practices for the AWS Cost Explorer API

The following are best practices when working with the Cost Explorer API.

Topics

- Best practices for configuring access to the Cost Explorer API
- Best practices for querying the Cost Explorer API
- Best practices for optimizing your Cost Explorer API costs

Best practices for configuring access to the Cost Explorer API

A user must be granted explicit permissions to query the Cost Explorer API. Granting a user access to the Cost Explorer API gives that user query access to any cost and usage data available to that account. For the policy that grants the necessary permissions to a user, see View costs and usage.

When configuring access to the Cost Explorer API, we recommend creating a unique role for the user. If you want to give multiple users query access to the Cost Explorer API, we recommend creating a role for each of them.

Best practices for querying the Cost Explorer API

When querying the Cost Explorer API, we recommend using filtering conditions to refine your queries so that you receive only the data that you need. You can do this by restricting the time range to a smaller interval or by using filters to limit the result set that your request returns. This enables your queries to return data more quickly than if you're accessing a larger set of data.

Adding one or more grouping dimensions to your query can increase the size of your result and can impact query performance. Depending on your use case, it can make sense to filter your data instead.

The Cost Explorer API can access up to 13 months of historical data and data for the current month. It can also provide 3 months of cost forecast data at the daily level of granularity and 12 months of cost forecast data at the monthly level of granularity.

Best practices for optimizing your Cost Explorer API costs

Because you're charged for the Cost Explorer API per paginated request, we recommend identifying the exact dataset to access before submitting queries.

AWS billing information is updated up to three times daily. Typical workloads and use cases for the Cost Explorer API anticipate a call pattern cadence ranging from daily to several times per day. To receive the most up-to-date data available, query for the time period that you're interested in.

If you're creating an application using the Cost Explorer API, we recommend architecting the application so that it has a caching layer. This enables you to regularly update the underlying data for your end users, but doesn't trigger queries every time that an individual in your organization accesses it.

Understanding your costs using Cost Explorer reports

Cost Explorer provides default reports, but also enables you to change the filters and constraints used to create the reports. Cost Explorer also provides ways to save your reports. You can save the exact configuration as a bookmark, download the CSV file of the data that Cost Explorer used to create your graphs, or save the Cost Explorer configuration as a saved report. Cost Explorer keeps your saved reports and lists them on your report page along with the default Cost Explorer reports.

Topics

- Using the default Cost Explorer reports
- Creating a Cost Explorer report
- Viewing a Cost Explorer report
- Editing a Cost Explorer report
- Deleting a Cost Explorer report
- Saving your Cost Explorer configuration with bookmarks or favorites
- Downloading the cost data CSV file

Using the default Cost Explorer reports

Cost Explorer provides you with a couple of default reports. You can't modify these reports, but you can use them to create your own custom reports.

- Cost and usage reports

- Reserved Instance reports

Cost and usage reports

Cost Explorer provides you with the following reports for understanding your costs.

- AWS Marketplace
- Daily costs
- Monthly costs by linked account
- Monthly costs by service
- Monthly EC2 running hours costs and usage

AWS Marketplace

The **AWS Marketplace** report shows how much you have spent through AWS Marketplace.

Daily costs

The **Daily costs** report shows how much you've spent in the last six months, along with how much you're forecasted to spend over the next month.

Monthly costs by linked account

The **Monthly costs by linked account** report shows your costs for the last six months, grouped by linked, or member account. The top five member accounts are shown by themselves, and the rest are grouped into one bar.

Monthly costs by service

The **Monthly costs by service** report shows your costs for the last six months, grouped by service. The top five services are shown by themselves, and the rest are grouped into one bar.

Monthly EC2 running hours costs and usage

The **Monthly EC2 running hours costs and usage** report shows how much you have spent on active Reserved Instances (RIs).

Reserved Instance reports

Cost Explorer provides you with the following reports for understanding your reservations.

The reservation reports show your Amazon EC2 coverage and utilization in either hours or normalized units. Normalized units enable you to see your Amazon EC2 usage for multiple sizes of instances in a uniform way. For example, suppose you run an `xlarge` instance and a `2xlarge` instance. If you run both instances for the same amount of time, the `2xlarge` instance uses twice as much of your reservation as the `xlarge` instance, even though both instances show only one instance-hour. Using normalized units instead of instance-hours, the `xlarge` instance used 8 normalized units, and the `2xlarge` instance used 16 normalized units. For more information, see Instance Size Flexibility for EC2 Reserved Instances.

- RI utilization reports
- RI coverage reports

RI utilization reports

The RI Utilization reports show how much of your Amazon EC2, Amazon Redshift, Amazon RDS, Amazon OpenSearch Service, and Amazon ElastiCache Reserved Instance (RIs) that you use, how much you saved by using RIs, how much you overspent on RIs, and your net savings from purchasing RIs during the selected time range. This helps you to see if you have purchased too many RIs.

The RI Utilization charts display the number of RI hours that your account uses, helping you to understand and monitor your combined usage (utilization) across all of your RIs and services. It also shows how much you saved over On-Demand Instance costs by purchasing a reservation, the amortized costs of your unused reservations, and your total net savings from purchasing reservations. AWS calculates your total net savings by subtracting the costs of your unused reservations from your reservations savings.

The following table shows an example of potential savings (all costs are in USD).

RI utilization example

Account	RI utilization	RI hours purchase	RI hours used	RI hours unused	On-Demand cost of RI hours used	Effective RI cost	Net savings	Total potential savings

Account	RI utilization	RI hours purchased	RI hours used	RI hours unused	On-Demand cost of RI hours used	Effective RI cost	Net savings	Total potential savings
Martha	0.50	100	50	50	$200	$150	$50	$250
Liu Jie	0.75	100	75	25	$300	$150	$150	$250
Saanvi	1.00	50	50	0	$200	$75	$125	$125

As shown in the preceding table, Martha, Liu Jie, and Saanvi purchase RIs at $1.50 an hour and On-Demand hours at $4.00 an hour. Breaking down this example further, you can see how much each of them saves by purchasing RIs:

- Martha purchases 100 RI hours for $150. She uses 50 hours, which would cost $200 if she used On-Demand Instances. She saves $50, which is the cost of 50 On-Demand hours minus the cost of the RI. She could optimize her savings by using more of her purchased RI hours, by converting her RI to cover other instances, or by selling her RIs on the RI Marketplace. For more information about selling an RI on the RI Marketplace, see Selling on the Reserved Instance Marketplace in the Amazon EC2 User Guide.
- Liu Jie purchases 100 RI hours for $150. He uses 75 of them, which would cost $300 if he used On-Demand Instances. So he saves $150, which is the cost of 300 On-Demand hours minus the cost of the RI.
- Saanvi purchases 50 RI hours for $75. She uses all 50 of them, which would cost $200 if she used On-Demand Instances. So she saves $125, which is the cost of 200 On-Demand hours minus the cost of the RI.

The reports allow you to define a utilization threshold, known as a *utilization target*, and identify RIs that meet your utilization target and RIs that are underutilized. The chart shows RI utilization as the percentage of purchased RI hours that are used by matching instances, rounded to the nearest percentage.

Target utilization is shown on the chart as a dotted line in the chart and in the table below the chart as a colored RI utilization status bar. RIs with a red status bar are RIs with no hours used. RIs with a yellow status bar are under your utilization target. RIs with a green status bar have met your utilization target. Instances with a gray bar aren't using reservations. You can change the utilization target in the **Display Options** section. To remove the utilization target line from the chart, clear the **Show target line on chart** check box. You can also create budgets that enable AWS to notify you if you fall below your utilization targets. For more information, see Managing your costs with AWS Budgets.

You can filter the chart to analyze the purchasing accounts, instance types, and more. RI reports use a combination of RI-specific filters and regular Cost Explorer filters. The RI-specific filters are available only for the Cost Explorer RI Utilization and RI Coverage reports. They aren't available anywhere else that AWS uses Cost Explorer filters. The following filters are available:

- **Availability Zone** – Filter your RI usage by specific Availability Zones.
- **Instance Type** – Filter your RI usage by specific instance types, such as **t2.micro** or **m3.medium**. This also applies to Amazon RDS instance classes, such as **db.m4**, and Amazon Redshift and ElastiCache node types, such as **dc2.large**.
- **Linked Account** – Filter your reservations by specific member accounts.
- **Platform** – Filter your RI usage by platform, such as **Linux** or **Windows**. This also applies to Amazon RDS database engines.
- **Region** – Filter your RI usage by specific regions, such as **US East (N. Virginia)** or **Asia Pacific (Singapore)**.
- **Scope** (Amazon EC2) – Filter your Amazon EC2 usage to show RIs that are purchased for use in specific Availability Zones or regions.
- **Tenancy** (Amazon EC2) – Filter your Amazon EC2 usage by tenancy, such as **Dedicated** or **Default**. An RI with a **Dedicated** tenancy is reserved for a single tenant, and an RI with a **Default** tenancy might share hardware with another RI.

In addition to changing your utilization target and filtering your RIs, you can choose a single RI or a group of RIs to show in the chart. To choose a single RI or a selection of RIs to see in the chart, select the check box next to the RI in the table below the chart. You can select up to 10 leases at one time.

Cost Explorer shows the combined utilization across all of your RIs in the chart and shows utilization for individual RI reservations in the table below the chart. The table also includes a

subset of the information for each RI reservation. You can find the following information for each reservation in the downloadable .csv file:

- **Account Name** – The name of the account that owns the RI reservation.
- **Subscription ID** – The unique subscription ID for the RI reservation.
- **Reservation ID** – The unique ID for the RI reservation.
- **Instance Type** – The RI instance class, instance type, or node type, such as **t2.micro**, **db.m4**, or **dc2.large**.
- **RI Utilization** – The percentage of purchased RI hours that were used by matching instances.
- **RI Hours Purchased** – The number of normalized purchased hours for the RI reservation.
- **RI Hours Used** – The number of normalized purchased hours that were used by matching instances.
- **RI Hours Unused** – The number of normalized purchased hours that weren't used by matching instances.

> **Note**
>
> RI Hours metrics are calculated using normalization factors.

- **Account ID** – The unique ID of the account that owns the RI reservation.
- **Start Date** – The date that the RI starts.
- **End Date** – The date that the RI expires.
- **Numbers of RIs** – The numbers of RIs that are associated with the reservation.
- **Scope** – Whether this RI is for a specific Availability Zone or region.
- **Region** – The region that the RI is available in.
- **Availability Zone** – The Availability Zone that the RI is available in.
- **Platform** (Amazon EC2) – The platform that this RI is for.
- **Tenancy** (Amazon EC2) – Whether this RI is for a shared or dedicated instance.
- **Payment Option** – Whether this RI is a Full Upfront, Partial Upfront, or No Upfront RI.
- **Offering Type** – Whether this RI is Convertible or Standard.
- **On-Demand Cost Equivalent** – The cost of the RI hours that you used, based on the public On-Demand prices.
- **Amortized Upfront Fee** – The upfront cost of this reservation, amortized over the RI period.

- **Amortized Recurring Charges** – The monthly cost of this reservation, amortized over the RI period.
- **Effective RI Cost** – The combined amortized upfront and amortized recurring costs of the RI hours that you purchased.
- **Net Savings** – The amount that Cost Explorer estimates that you saved by purchasing reservations.
- **Potential Savings** – The total potential savings that you might see if you use your entire RI.
- **Average On-Demand Rate** – The On-Demand rate of the RI hours that you used. When you view the On-Demand rates for an extended period of time, the On-Demand rate reflects any price changes made during that time period.

  If there isn't any usage for the given time period, the average On-Demand rate shows **N/A**.
- **Total Asset Value** – The effective cost of your reservation term. The total asset value takes both your start date and either your end date or your cancellation date into consideration.
- **Effective Hourly Rate** – The effective hourly rate of your total RI costs. The hourly rate takes both your upfront fees and your recurring fees into consideration.
- **Upfront Fee** – The one-time upfront cost of the RI hours that you purchased.
- **Hourly Recurring Fee** – The effective hourly rate of your monthly RI costs. The hourly recurring fee takes only your recurring fees into consideration.
- **RI Cost For Unused Hours** – The amount that you spent on RI hours that you didn't use.

You can use this information to track how many RI usage hours you used and how many RI hours you reserved but didn't use during the selected time range.

The Daily RI Utilization chart displays your RI utilization for the previous three months on a daily basis. The Monthly RI Utilization chart displays your RI utilization for the previous 12 months on a monthly basis.

RI coverage reports

The RI Coverage reports show how many of your Amazon EC2, Amazon Redshift, Amazon RDS, Amazon OpenSearch Service, and Amazon ElastiCache instance hours are covered by RIs, how much you spent on On-Demand Instances, and how much you might have saved had you purchased more reservations. This enables you to see if you have under-purchased RIs.

The RI coverage charts display the percentage of instance hours that your account used that were covered by reservations, helping you to understand and monitor the combined coverage across all

of your RIs. It also shows how much you spent on On-Demand Instances and how much you might have saved had you purchased more reservations.

You can define a threshold for how much coverage you want from RIs, known as a *coverage target*, which enables you to see where you can reserve more RIs.

Target coverage is shown on the chart as a dotted line, and the average coverage is shown in the table below the chart as a colored status bar. Instances with a red status bar are instances with no RI coverage. Instances with a yellow status bar are under your coverage target. Instances with a green status bar have met your coverage target. Instances with a gray bar aren't using reservations. You can change the coverage target in the **Display Options** section. To remove the coverage target line from the chart, clear the **Show target line on chart** check box. You can also create coverage budgets that enable AWS to notify you if you fall below your coverage target. For more information, see Managing your costs with AWS Budgets.

The RI coverage reports use the Cost Explorer filters instead of the RI Utilization filters. You can filter the chart to analyze the purchasing accounts, instance types, and more. RI reports use a combination of RI-specific filters and regular Cost Explorer filters. The RI-specific filters are available only for the Cost Explorer RI Utilization and RI Coverage reports, and aren't available anywhere else that AWS uses Cost Explorer filters. The following filters are available:

- **Availability Zone** – Filter your RI usage by specific Availability Zones.
- **Instance Type** – Filter your RI usage by specific instance types, such as **t2.micro** or **m3.medium**. This also applies to Amazon RDS instance classes such as **db.m4**.
- **Linked Account** – Filter your RI usage by specific member accounts.
- **Platform** – Filter your RI usage by platform, such as **Linux** or **Windows**. This also applies to Amazon RDS database engines.
- **Region** – Filter your RI usage by specific regions, such as **US East (N. Virginia)** or **Asia Pacific (Singapore)**.
- **Scope** (Amazon EC2) – Filter your Amazon EC2 usage to show RIs that are purchased for use in specific Availability Zones or regions.
- **Tenancy** (Amazon EC2) – Filter your Amazon EC2 usage by tenancy, such as **Dedicated** or **Default**. A **Dedicated** RI is reserved for a single tenant, and a **Default** RI might share hardware with another RI.

In addition to changing your coverage target and filtering your instance types with the available filters, you can choose a single instance type or a group of instance types to show in the chart. To

choose a single instance type or a selection of instance types to see in the chart, select the check box next to the instance type in the table below the chart. You can select up to 10 instances at one time.

Cost Explorer shows the combined coverage across all of your instance types in the chart and shows coverage for individual instance types in the table below the chart. The table also includes a subset of the information for each instance type. You can find the following information for each instance type in the downloadable .csv file:

- **Instance Type** (Amazon EC2), **Instance Class** (Amazon RDS), or **Node Type** (Amazon Redshift or Amazon ElastiCache) – The RI instance class, instance type, or node type, such as **t2.micro**, **db.m4**, or **dc2.large**.
- **Database Engine** (Amazon RDS) – Filter your Amazon RDS coverage to show RIs that cover a specific database engine, such as **Amazon Aurora**, **MySQL**, or **Oracle**.
- **Deployment Option** (Amazon RDS) – Filter your Amazon RDS coverage to show RIs that cover a specific deployment option, such as **Multi-AZ** deployments.
- **Region** – The region that the instance ran in, such as **us-east-1**.
- **Platform** (Amazon EC2) – The platform that this RI is for.
- **Tenancy** (Amazon EC2) – Whether this RI is for a shared, dedicated, or host instance.
- **Average Coverage** – The average number of usage hours that a reservation covers.
- **RI Covered Hours** – The number of usage hours that a reservation covers.
- **On-Demand Hours** – The number of usage hours that aren't covered by reservations.
- **On-Demand Cost** – The amount that you spent on On-Demand Instances.
- **Total Running Hours** – The total number of usage hours, both covered and uncovered.

You can use this information to track how many hours you use and how many of those hours are covered by RIs.

The daily chart displays the number of RI hours that your account used on a daily basis for the last three months. The monthly chart displays your RI coverage for the previous 12 months, listed by month.

Creating a Cost Explorer report

You can use the console to save the results of a Cost Explorer query as a report.

> **Note**
>
> Cost Explorer reports can be modified. We strongly recommend that you don't use them for auditing purposes.

To save a Cost Explorer report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Choose **Create new report**. This resets all of your Cost Explorer settings to your default settings.
4. Select a report type.
5. Choose **Create report**.
6. Customize your Cost Explorer settings.
7. Choose **Save to report library**.
8. In the **Save to report library** dialog box, enter a name for your report, and then choose **Save report**.

Viewing a Cost Explorer report

You can use the console to view saved Cost Explorer reports.

To view your saved reports

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.

Editing a Cost Explorer report

You can use the console to edit Cost Explorer reports.

To edit a report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Choose the report that you want to edit.

> **Note**
>
> You can't edit the predefined reports. If you choose one of the predefined reports as a starting point for a report, enter a new report name in the report name field and continue with this procedure.

4. Customize your Cost Explorer settings.
5. Choose **Save** to overwrite the existing report, or else choose **Save as a new report**.
6. In the **Save to report library** dialog box, enter a name for your report, and then choose **Save report**.

Deleting a Cost Explorer report

You can use the console to delete saved Cost Explorer reports.

To delete a saved report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Cost Explorer Saved Reports**.
3. Select the check box next to the report you want to delete.

> **Note**
>
> The **Reports** page contains predefined reports that cannot be deleted. These default reports are identified by a lock icon. You can, however, delete custom reports.

4. Choose **Delete**.
5. In the **Delete reports** dialog box, choose **Delete**.

Saving your Cost Explorer configuration with bookmarks or favorites

You can save your date, filter, chart style, group by, and advanced settings by saving the Cost Explorer URLs as favorites or bookmarks in your browser. When you return to the link that you saved, Cost Explorer refreshes the page using current cost data for time range you selected and displays the most recent forecast. This feature enables you to save a configuration that you're likely to refresh and return to often. You can also save a configuration for a specific, unchanging range of time by using the **Custom** time range and setting fixed start and end dates for your chart.

> **Warning**
>
> If you want to save a number of configurations, make sure to give each bookmark or favorite a unique name so that you don't overwrite older configurations when you save a new URL.

Downloading the cost data CSV file

When you want to review comprehensive detail, you can download a comma-separated values (CSV) file of the cost data that Cost Explorer uses to generate the chart. This is the same data that appears in the data table under the chart. The data table sometimes doesn't display the complete dataset that is used for the chart. For more information, see Reading the Cost Explorer data table.

To download a CSV file

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. Configure Cost Explorer to use the options that you want to see in the CSV file.
3. Choose **Download CSV**.

Note the following about the format of the CSV download:

- If you view the CSV file in a table format, the file's columns represent costs and the rows represent time. When compared to the Cost Explorer data table in the console, the columns and rows are transposed.
- The file shows data with up to 15 decimal places of precision.
- The file shows dates in the YYYY-MM-DD format.

Managing your costs with AWS Budgets

You can use AWS Budgets to track and take action on your AWS costs and usage. You can use AWS Budgets to monitor your aggregate utilization and coverage metrics for your Reserved Instances (RIs) or Savings Plans. If you're new to AWS Budgets, see Best practices for AWS Budgets.

You can use AWS Budgets to enable simple-to-complex cost and usage tracking. Some examples include:

- Setting a monthly cost budget with a fixed target amount to track all costs associated with your account. You can choose to be alerted for both actual (after accruing) and forecasted (before accruing) spends.
- Setting a monthly cost budget with a variable target amount, with each subsequent month growing the budget target by 5 percent. Then, you can configure your notifications for 80 percent of your budgeted amount and apply an action. For example, you could automatically apply a custom IAM policy that denies you the ability to provision additional resources within an account.
- Setting a monthly usage budget with a fixed usage amount and forecasted notifications to help ensure that you are staying within the service limits for a specific service.
- Setting a daily utilization or coverage budget to track your RI or Savings Plans. You can choose to be notified through email and Amazon SNS topics when your utilization drops below 80 percent for a given day.
- Setting a custom period budget that aligns with your fiscal year, project duration, or grant period. For example, you can create a budget for April 15th, 2025 through July 15th, 2025 to track a three-month project.

AWS Budgets information is updated up to three times a day. Updates typically occur 8–12 hours after the previous update. Budgets can track your blended, unblended, net unblended, amortized, and net amortized costs. Budgets can include or exclude charges such as discounts, refunds, support fees, and taxes.

You can create the following types of budgets:

- **Cost budgets**: Set spending limits for services and receive alerts when costs approach or exceed your defined threshold.
- **Usage budgets**: Establish usage limits for one or more services and get notified when usage approaches or exceeds your set threshold.

- **RI utilization budgets**: Define a utilization threshold for your RIs and receive alerts when usage falls below this level, helping you identify unused or under-utilized RIs.
- **RI coverage budgets**: Set a coverage threshold and get alerted when the percentage of your instance hours covered by RIs falls below this level, enabling you to monitor how much of your usage is reservation-covered.
- **Savings Plans utilization budgets**: Establish a utilization threshold for your Savings Plans and receive notifications when usage drops below this level, allowing you to identify unused or under-utilized Savings Plans.
- **Savings Plans coverage budgets**: Define a coverage threshold and get alerted when the percentage of your eligible usage covered by Savings Plans falls below this level, helping you track how much of your usage is covered by Savings Plans.

You can set up optional notifications that warn you if you exceed, or are forecasted to exceed, your budgeted amount for cost or usage budgets. Or if you fall below your target utilization and coverage for RI or Savings Plans budgets. You can have notifications sent to an Amazon SNS topic, to an email address, or to both. For more information, see Creating an Amazon SNS topic for budget notifications.

If you use consolidated billing in an organization and you own the management account, you can use IAM policies to control access to budgets by member accounts. By default, owners of member accounts can create their own budgets but can't create or edit budgets for other users. You can create roles with permissions that allow users to create, edit, delete, or read budgets in a specific account. However, we don't support cross-account usage.

A budget is only visible to users with access to the account that created the budget, and with access to the budget itself. For example, a management account can create a budget that tracks a specific member account's cost, but the member account can only view the same budget if they receive access to the management account. For more information, see Overview of managing access permissions. For more information about AWS Organizations, see the AWS Organizations User Guide.

> **Note**
>
> There can be a delay between when you incur a charge and when you receive a notification from AWS Budgets for the charge. This is due to a delay between when an AWS resource is used and when that resource usage is billed. You might incur additional costs or usage that exceed your budget notification threshold before AWS Budgets can notify you, and

your actual costs or usage may continue to increase or decrease after you receive the notification.

Topics

- Best practices for AWS Budgets
- Creating a budget
- Viewing your budgets
- Editing a budget
- Downloading a budget
- Copying a budget
- Deleting a budget
- Configuring budget actions
- Creating an Amazon SNS topic for budget notifications
- Adding email recipients to a budget notification
- Receiving budget alerts in chat applications

Best practices for AWS Budgets

Note the following best practices when you're working with budgets.

Topics

- Controlling access to AWS Budgets
- Understanding budget actions
- Setting budgets
- Understanding custom period budgets
- Using the advanced options when setting cost budgets
- Understanding the AWS Budgets update frequency
- Setting budget alerts
- Setting budget alerts using Amazon SNS topics
- Tagging budgets

- Reviewing budgets when organizational structure changes

Controlling access to AWS Budgets

To allow users to create budgets in the AWS Billing and Cost Management console, you must also allow users to do the following:

- View your billing information
- Create Amazon CloudWatch alarms
- Create Amazon Simple Notification Service (Amazon SNS) notifications

To learn more about giving users the ability to create budgets on the AWS Budgets console, see Allow users to create budgets.

You can also create budgets programmatically using the Budgets API. When configuring access to the Budgets API, we recommend creating a unique user role for making programmatic requests. This helps you define more precise access controls between who in your organization has access to the AWS Budgets console and the API. To give multiple users query access to the Budgets API, we recommend creating a role for each of them.

Understanding budget actions

Using managed policies

There are two AWS managed policies to help get you started with budget actions. One for the user, and the other for budgets. These policies are related. The first policy ensures a user can pass a role to the budgets service, and the second allows budgets to execute the action.

If you don't have proper permissions configured and assigned for the user and for AWS Budgets, AWS Budgets can't execute your configured actions. To ensure proper configuration and execution, we've configured these managed policies so your AWS Budgets actions work as intended. We recommend you use these IAM policies to be sure you don't have to update your existing IAM policy for AWS Budgets when a new functionality is included. We will add new capabilities to the managed policy by default.

For details about managed policies, see Managed policies.

To learn more about AWS Budgets actions, see the Configuring budget actions section.

Using Amazon EC2 Auto Scaling

If a budget action is used to stop an Amazon EC2 instance in an Auto Scaling Group (ASG), Amazon EC2 Auto Scaling restarts the instance, or launches new instances to replace the stopped instance. Therefore, "shutdown budget actions is not effective to Amazon EC2/Amazon RDS budget actions" aren't effective unless you combine a second budget action that removes permissions on the role used by the Launch Configuration managing the ASG.

Setting budgets

Use AWS Budgets to set custom budgets based on your costs, usage, reservation utilization, and reservation coverage.

With AWS Budgets, you can set budgets on a recurring basis or for a specific time frame. However, we recommend setting your budget on a recurring basis so that you don't unexpectedly stop receiving budget alerts.

Understanding custom period budgets

To get the most benefit from your custom period budget and more effectively manage your budgets, consider the following:

- **Set an appropriate budget time frame.** Choose a start and end date that aligns with your budgeting cycle. The end date must be within three years of the start date.
- **Understand your budget calculations.** Budget tracking uses the full date range, from start to end. For amount calculations, only the date (00:00 UTC) is used. The start date is included, but the end date is excluded from calculations.
- **Optimize your forecast alerts.** You can set forecasts up to 3 years in the future. Forecasting begins when the current date is within 12 months of the end date. Alert triggers are restricted to this 12-month time frame.
- **Maintain active monitoring.** Custom period budgets don't auto-renew and expire on the end date. Regularly review your budgets and extend end dates as needed to ensure continuous monitoring.
- **Consider your billing cycle.** Align your custom period budget with your billing cycle for more accurate tracking.
- **Use with other budget types.** Combine custom period budgets with monthly, quarterly, or annual budgets for comprehensive financial monitoring.

Using the advanced options when setting cost budgets

Cost budgets can be aggregated by blended, unblended, net unblended, amortized, or net amortized costs. Cost budgets can also either include or exclude refunds, credits, upfront reservation fees, recurring reservation charges, non-reservation subscription costs, taxes, and support charges.

Understanding the AWS Budgets update frequency

AWS billing data, which Budgets uses to monitor resources, is updated at least once per day. Keep in mind that budget information and associated alerts are updated and sent according to this data refresh cadence.

Setting budget alerts

Budget alerts can be sent to up to 10 email addresses and one Amazon SNS topic per alert. You can set budgets to alert against either actual values or forecasted values.

Actual alerts are only sent out once per budget, per budget period, when a budget first reached the actual alert threshold.

Forecast-based budget alerts are sent out on a per-budget, per-budget period basis. They might alert more than once in a budgeted period if the forecasted values exceed, dip below, and then exceed the alert threshold again during the budgeted period.

AWS requires approximately 5 weeks of usage data to generate budget forecasts. If you set a budget to alert based on a forecasted amount, this budget alert isn't triggered until you have enough historical usage information.

The following video highlights the importance of setting up budget alerts, which give you control over your spending. It also touches on the use of multi-factor authentication (MFA) to increase the security of your account.

How to set up AWS multi-factor authentication (MFA) and AWS Budgets alerts

Setting budget alerts using Amazon SNS topics

When you create a budget that sends notifications to an Amazon SNS topic, you must either have a preexisting Amazon SNS topic or create an Amazon SNS topic. Amazon SNS topics enable you to send notifications over SMS in addition to email.

For budget notifications to be sent successfully, your budget must have permissions to send a notification to your topic, and you must accept the subscription to the Amazon SNS notification topic. For more information, see Creating an Amazon SNS topic for budget notifications.

Tagging budgets

You can use tags to control access to your AWS Budgets resources. You can also use resource-level permissions to allow or deny access to one or more AWS Budgets resources in an AWS Identity and Access Management (IAM) policy. This allows for easy budget management and auditing, improving governance and information security. You can specify the users, roles, and actions that are permitted on the AWS Budgets resources.

To add tags to budgets, use AWS Budgets in the Billing and Cost Management console or programmatically using the Budgets API.

You can add tags when creating an AWS Budgets resource, or later using the console or the `TagResource` operation.

You can view the tags on an AWS Budgets resource using the console or by calling the `ListTagsForResource` operation.

You can remove tags from an AWS Budgets resource using the console or by calling the `UntagResource` operation.

> **Note**
>
> AWS Budgets does not support tags for cost allocation. This means you will not see tag information in cost and usage data—in Data Exports, Cost and Usage Reports, or Cost Explorer, for example.

Reviewing budgets when organizational structure changes

When a member account leaves an AWS Organization, their budget's behavior changes significantly. Keep the following points in mind:

- AWS Budgets only track costs incurred after a member account leaves the organization.
- No notification is sent when this tracking behavior changes.
- Historical cost data from before the account's departure is not included in budget calculations or alerts.

Regularly review your AWS Budgets configuration when organizational changes occur, particularly when member accounts leave the organization. Update budget thresholds and settings to reflect the new standalone account status and ensure continuous cost monitoring.

Creating a budget

You can create budgets to track and take action on your costs and usage. You can also create budgets to track your aggregate Reserved Instance (RI) and Savings Plans utilization and coverage. By default, single accounts, the management account, and member accounts in an organization can create budgets.

When you create a budget, AWS Budgets provides a Cost Explorer graph to help you see your incurred costs and usage. If you didn't enable Cost Explorer yet, this graph is blank and AWS Budgets will enable Cost Explorer when you create your first budget. You can create your budget without enabling Cost Explorer. It can take up to 24 hours for this graph to appear after you or AWS Budgets enable Cost Explorer.

You can create and set up a budget in two ways:

- Using a budget template (simplified)
- Customizing a budget (advanced)

To learn how to add email recipients to your budget notifications and how email verification works, see Adding email recipients to a budget notification.

Billing view prerequisites and monitoring

AWS Budgets supports billing views, allowing you to create and manage budgets based on filtered cost and usage data across multiple accounts within your organization. When creating a budget, you can select a billing view to define the scope of cost and usage data the budget will track. For more information on controlling access to cost management data using billing views, see Controlling cost management data access with Billing View.

> **Note**
>
> AWS doesn't support billing transfer views for bill transfer accounts.

Before you use billing views with budgets, consider the following permissions requirements:

- For cross-account billing views, the source account administrator must grant:
  - `budgets:ModifyBudget` permission on the billing view to allow target accounts/users to create budgets
  - `billing:GetBillingViewData` permission to access the billing view data
- Target accounts/users also need:
  - `iam:CreateServiceLinkedRole` permission for the Budgets service principal (budgets.amazonaws.com):
- The service-linked role monitors the health status of your billing view access:
  - `HEALTHY`: Indicates the budget has proper access to the billing view data
  - `UNHEALTHY`: Indicates the budget cannot access the billing view data, which might occur if permissions have been revoked or the view has been deleted. Reasons for unhealthy status can be:
    - `BILLING_VIEW_NO_ACCESS`: Indicates that access to the billing view associated with the budget has been removed (unshared) or the view was deleted.
    - `INVALID_FILTER`: Indicates that the budget's filter is invalid. This occurs when a management account becomes a linked account but has a budget that references an account outside their organization. In this situation, budget spend updates are paused.

Tutorials

You can also use our walk-through tutorials to learn how to achieve your objectives with AWS Budgets.

To access tutorials

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. Next to **Overview**, choose **Info**.
4. In the help panel, choose **Tutorials**.

Using a budget template (simplified)

You can create a budget using a template with recommended configurations. Budget templates are a simplified way to start using AWS Budgets, with a single page workflow, unlike the 5-step workflow that is required for Customizing a budget (advanced).

To create a budget using a template

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Use a template (simplified)**.
5. Under **Templates**, choose a template that best matches your use case:
   - **Zero spend budget**: A budget that notifies you after your spending exceeds AWS Free Tier limits.
   - **Monthly cost budget**: A monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.
   - **Daily Savings Plans coverage budget**: A coverage budget for your Savings Plans that notifies you when you fall below the defined target. This helps you to identify your on-demand spend sooner so that you can consider purchasing a new commitment.
   - **Daily reservation utilization budget**: A utilization budget for your Reserved Instances that notifies you when you fall below the defined target. This helps you to identify when you're not using some of your hourly commitment that you already purchased.
6. Update the details and settings for your specific template.
7. Choose **Create budget**.

While each template has default configurations, they can be changed later. This way, you can use it to create most of the budget, and then edit certain settings in the advanced workflow, such as adding a linked account or a cost category filter. To change any of the settings, under **Template settings**, choose **Custom**.

You can also download a template for offline use in AWS CLI or CloudFormation, for example. To download a template, under **Template settings**, choose **JSON**.

Customizing a budget (advanced)

You can customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific accounts. Creating a customized budget involves a 5-step workflow.

You can choose between four main budget types that track against the following:

- Cost (see Creating a cost budget)
- Usage (see Creating a usage budget)
- Savings Plans (see Creating a Savings Plans budget)
  - Savings Plans utilization
  - Savings Plans coverage
- Reservation (see Creating a reservation budget)
  - Reservation utilization
  - Reservation coverage

Creating a cost budget

Use this procedure to create a budget that's based on your costs.

To create a cost budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Cost budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Set budget amount**, for **Period**, choose how often you want the budget to reset the actual and forecasted spend.

- **Daily** for every day
- **Monthly** for every month
- **Quarterly** for every three months
- **Annually** for every 12 months
- **Custom** to specify your own start and end dates

> **Note**
>
> With a **Monthly** or **Quarterly** budget period, you can set future budgeted amounts using the budget planning feature. **Custom** period budgets align with time periods outside of standard reset options. For example, you can create a budget period that matches your fiscal year or project timeline.

8. For **Budget renewal type**, choose **Recurring budget** for a budget that resets after the budget period. Or, choose **Expiring budget** for a one-time budget that doesn't reset after the budget period.
9. Choose the start date or period to begin tracking against your budgeted amount. For an **Expiring budget**, choose the end date or period for the budget to end on.

   All budget times are in the UTC format.
10. For **Budgeting method**, select the way that you want your budget amount to be determined each budget period:

    - **Fixed**: Set one amount to monitor every budget period.
    - **Planned**: Set different amounts to monitor each budget period.
    - **Auto-adjusting**: Set your budget amount to be adjusted automatically based on your spending pattern over a time range that you specify.

    For more information about each method, see the section called “Budget methods”
11. Enter your budgeted amount for the selected period. This is the value the budget will track against.
12. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

> **Note**
>
> You can't use the **Linked account** filter within a linked account.

13. (Optional) **Under Budget scope**, for **Advanced options**, choose how to aggregate costs:

    - **Use blended costs**: View averaged costs across accounts with evenly distributed Reserved Instance and Savings Plans benefits. Useful for organizations sharing commitment benefits.
    - **Use unblended costs**: View actual resource costs charged at time of usage. Suitable for individual account tracking.
    - **Use net unblended costs**: View actual costs after all discounts and credits are applied. Helps with monitoring final costs.
    - **Use amortized costs**: View costs with upfront and recurring payments spread across the term. Assists in consistent month-to-month budget planning.
    - **Use net amortized costs**: View spread payments with all discounts and credits applied. Supports long-term budget planning.

14. Choose **Next**.
15. Choose **Add an alert threshold**.
16. Under **Set alert threshold**, for **Threshold**, enter the amount that must be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 dollars. To be notified at 160 dollars (80% of your budget), enter **160** for an absolute budget or **80** for a percentage budget.

    Next to the amount, choose **Absolute value** to be notified when your costs exceed the threshold amount. Or, choose **% of budgeted amount** to be notified when your costs exceed the threshold percentage.

    Next to the threshold, choose **Actual** to create an alert for actual spend. Or, choose **Forecasted** to create an alert for forecasted spend.
17. (Optional) Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.

> **Important**
>
> Email recipients must verify their email address before receiving budget notifications. For more information, see Adding email recipients to a budget notification.

18. (Optional) Under **Notification preferences**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

19. (Optional) Under **Notification preferences**, for **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts on the AWS Chatbot console.
20. Choose **Next**.
21. (Optional) For **Attach actions**, you can configure an action that AWS Budgets performs on your behalf when the alert threshold is exceeded. For more information and instructions, see To configure a budget action.
22. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following parameters for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

23. Review your budget settings, and then choose **Create budget**.

Creating a usage budget

Use this procedure to create a budget that's based on your usage.

To create a usage budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Usage budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Choose what you're budgeting against**, for **Budget against**, choose **Usage type groups** or **Usage types**. A usage type group is a collection of usage types that have the same unit of measure. For example, resources that measure usage by the hour is one usage type group.

   - For **Usage type groups**, choose the unit of measurement and the applicable service usage that you want the budget to monitor.
   - For **Usage types**, choose the specific service usage measurements that you want the budget to monitor.

8. Under **Set budget amount**, for **Period**, choose how often you want the budget to reset the actual and forecasted usage.

   - **Daily** for every day
   - **Monthly** for every month
   - **Quarterly** for every three months
   - **Annually** for every 12 months
   - **Custom** to specify your own start and end dates

> **Note**
>
> With a **Monthly** or **Quarterly** budget period, you can set future budgeted amounts using the budget planning feature. **Custom** period budgets align with time periods outside of standard reset options. For example, you can create a budget period that matches your fiscal year or project timeline.

9. For **Budget renewal type**, choose **Recurring budget** for a budget that resets at the end of each budget period. Or, choose **Expiring budget** for a one-time budget that doesn't reset after the given budget period.
10. Choose the start date or period to begin tracking against your budgeted amount. For an **Expiring budget**, choose the end date or period for the budget to end on.

    All budget times are in the UTC format.
11. For **Budgeting method**, select the way that you want your budget amount to be determined each budget period:

    - **Fixed**: Set one amount to monitor every budget period.
    - **Planned**: Set different amounts to monitor each budget period.
    - **Auto-adjusting**: Set your budget amount to be adjusted automatically based on your usage pattern over a time range that you specify.

    For more information about each method, see the section called “Budget methods”
12. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

    > **Note**
    >
    > You can't use the **Linked account** filter within a linked account.
13. Choose **Next**.
14. Choose **Add an alert threshold**.
15. Under **Set alert threshold**, for **Threshold**, enter the amount that must be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have

a budget of 200 hours. To be notified at 160 hours (80% of your budget), enter **160** for an absolute budget or **80** for a percentage budget.

Next to the amount, choose **Absolute value** to be notified when your usage exceeds the threshold amount. Or, choose **% of budgeted amount** to be notified when your usage exceeds the threshold percentage.

Next to the threshold, choose **Actual** to create an alert for actual usage. Or, choose **Forecasted** to create an alert for forecasted usage.

16. (Optional) Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.

    > **Important**
    >
    > Email recipients must verify their email address before receiving budget notifications. For more information, see Adding email recipients to a budget notification.

17. (Optional) Under **Notification preferences**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

    > **Important**
    >
    > After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

18. (Optional) Under **Notification preferences**, for **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts on the AWS Chatbot console.
19. Choose **Next**.
20. (Optional) For **Attach actions**, you can configure an action that AWS Budgets performs on your behalf when the alert threshold is exceeded. For more information and instructions, see To configure a budget action.
21. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following parameters for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

22. Review your budget settings, and then choose **Create budget**.

Creating a Savings Plans budget

Use this procedure to create a budget that's specifically for Savings Plans utilization or coverage.

> **Note**
>
> It can take up to 48 hours for Savings Plans utilization and coverage metrics to generate, which is longer than the time frame for cost and usage data.

To create a Savings Plans budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Savings Plans budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Utilization threshold**, for **Period**, choose how often you want the budget to reset the tracked utilization or coverage.

   - **Daily** for every day

- **Monthly** for every month
- **Quarterly** for every three months
- **Annually** for every 12 months
- **Custom** to specify your own start and end dates

All budget times are in the UTC format.

> **Note**
>
> **Custom** period budgets align with time periods outside of standard reset options. For example, you can create a budget period that matches your fiscal year or project timeline.

8. For **Monitor my spend against**, choose **Utilization of Savings Plans** to track how much of your Savings Plans you used. Or, choose **Coverage of Savings Plans** to track how much of your instance usage is covered by Savings Plans.

   For **Utilization threshold**, enter the utilization percentage that you want AWS to notify you at. For example, for a utilization budget where you want to stay above 90% Savings Plans utilization, enter **90**. The budget notifies you when your overall Savings Plans utilization is below 90%.

   For **Coverage threshold**, enter the coverage percentage that you want AWS to notify you at. For example, for a coverage budget where you want to stay above 80%, enter **80**. The budget notifies you when your overall coverage is below 80%.

9. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

   > **Note**
   >
   > You can't use the **Linked account** filter within a linked account.

10. Choose **Next**.
11. Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.

> **Important**
>
> Email recipients must verify their email address before receiving budget notifications. For more information, see Adding email recipients to a budget notification.

12. (Optional) For **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

13. (Optional) For **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the AWS Chatbot console.
14. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one email recipient or an Amazon SNS topic for notifications.

15. Review your budget settings, and then choose **Create budget**.

Creating a reservation budget

Use this procedure to create a budget for RI utilization or coverage.

> **Note**
>
> It can take up to 48 hours for Reservations utilization and coverage metrics to generate, which is longer than the time frame for cost and usage data.

To create a reservation budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. At the top of the page, choose **Create budget**.
4. Under **Budget setup**, choose **Customize (advanced)**.
5. Under **Budget types**, choose **Reservation budget**. Then, choose **Next**.
6. Under **Details**, for **Budget name**, enter the name of your budget. Your budget name must be unique within your account. It can contain A-Z, a-z, spaces, and the following characters:

   ```
   _.:/=+-%@
   ```

7. Under **Utilization threshold**, for **Period**, choose how often you want the budget to reset the tracked utilization or coverage.

   - **Daily** for every day
   - **Monthly** for every month
   - **Quarterly** for every three months
   - **Annually** for every 12 months
   - **Custom** to specify your own start and end dates

   All budget times are in the UTC format.

   > **Note**
   >
   > **Custom** period budgets align with time periods outside of standard reset options. For example, you can create a budget period that matches your fiscal year or project timeline.

8. For **Monitor my spend against**, choose **Utilization of reservations** to track how much of your reservation you used. Or, choose **Coverage of reservations** to track how much of your instance usage is covered by reservations.
9. For **Service**, choose the service that you want the budget to track.

10. For **Utilization threshold**, enter the utilization percentage that you want AWS to notify you at. For example, for a utilization budget where you want to stay above 90% RI utilization, enter **90**. The budget notifies you when your overall RI utilization is below 90%.

    For **Coverage threshold**, enter the coverage percentage that you want AWS to notify you at. For example, for a coverage budget where you want to stay above 80%, enter **80**. The budget notifies you when your overall coverage is below 80%.

11. (Optional) Under **Budget scope**, for **Filters**, choose **Add filter** to apply one or more of the available filters. Your choice of budget type determines the set of filters that's displayed on the console.

    > **Note**
    >
    > You can't use the **Linked account** filter within a linked account.

12. Choose **Next**.

13. Under **Notification preferences**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can be sent to a maximum of 10 email addresses.

    > **Important**
    >
    > Email recipients must verify their email address before receiving budget notifications. For more information, see Adding email recipients to a budget notification.

14. (Optional) For **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

    > **Important**
    >
    > After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

15. (Optional) For **AWS Chatbot Alerts**, you can choose to configure AWS Chatbot to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the AWS Chatbot console.
16. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one email recipient or an Amazon SNS topic for notifications.

17. Review your budget settings, and then choose **Create budget**.

Budget methods

You can set the budgeted amount of your cost or usage budget in one of the following ways. You can set one of these budgets no matter whether you're budgeting in a traditional sense—tracking to plan, for example—or if you want to monitor spend and receive alerts when costs increase beyond your threshold.

Fixed

With a fixed budget, you can monitor the same amount every budget period. For example, you can use a cost budget with the fixed method to monitor your costs against $100 every budget period.

Planned

The planned budgeting method is available for only monthly or quarterly budgets. With a planned budget, you can set a different amount to monitor each budget period. For example, you can use a monthly cost budget with the planned method to monitor your costs against $100 in the first month, $110 in the second month, and other amounts in the remaining months.

With a planned budget, you can set the budget amount for up to 12 months or 4 quarters. After 12 months or 4 quarters, your budget amount is fixed at the last budget amount.

Auto-adjusting

An auto-adjusting budget dynamically sets your budget amount based on your spending or usage over a time range that you specify. The historical or forecast time range that you select is the auto-adjustment baseline for your budget.

At the beginning of each new period, AWS Budgets calculates your budget amount from your cost or usage data within the baseline time range. Make sure to select a time range that best matches your expectations for your account's AWS costs or usage. If you select a time range with lower usage than you typically expect, then you might get more budget alerts than you need. If you select a time range with higher usage than you typically expect, then you might not get as many budget alerts as you need.

For example, you can create an auto-adjusting cost budget with a baseline time range of the last six months. In this scenario, if your average spending each budget period in the last six months was $100, your auto-adjusted budget amount in the new period is $100.

If AWS Budgets updates your budget amount based on changes in your spending or usage, all budget alert notification subscribers get a notification that the budget amount changed.

Note

- When calculating your auto-adjusted budget amount, AWS Budgets doesn't include periods at the beginning of your baseline time range that don't have cost or usage data. For example, assume that you set your baseline time range as the last four quarters. However, your account had no cost data in the first quarter. Then, in this case, AWS Budgets calculates your auto-adjusted budget amount from only the last three quarters.
- You see a temporary forecast while you're creating or editing a budget. After you save your budget, your auto-adjusted budget is set for the first time.

Budget filters

Based on your choice of budget type, you can choose one or more of the available budget filters.

API operation

Choose an action, such as `CreateBucket`.

Availability zone

Choose the `Availability zone` in which the resource that you want to create a budget for is running.

Billing entity

Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services. Possible values include:

- AWS: Identifies a transaction for AWS services other than in AWS Marketplace.
- AWS Marketplace: Identifies a purchase in AWS Marketplace.

Charge type

Different types of charges or fees.

- **Credit**: Any AWS credits that are applied to your account.
- **Other out-of-cycle charges**: Any subscription charges that aren't upfront reservation charges or support charges.
- **Recurring reservation fee**: Any recurring charges to your account. When you purchase a Partial Upfront or No Upfront Reserved Instance from AWS, you pay a recurring charge in exchange for a lower rate for using the instance. The recurring fees can result in spikes on the first day of every month, when AWS charges your account.
- **Refund**: Any refunds that you received. Refunds are listed as a separate line item in the data table. They don't appear as an item in the chart because they represent a negative value in the calculation of your costs. The chart displays only positive values.
- **Reservation applied usage**: Usage that AWS applied reservation discounts to.
- **Savings Plan covered usage**: Any on-demand cost that's covered by your Savings Plan. In an Unblended costs view, this represents the covered usage at on-demand rates. In an Amortized costs view, this represents the covered usage at your Savings Plan rates. Savings Plan covered usage line items are offset by the corresponding Savings Plan negation items.
- **Savings Plan negation**: Any offset cost through your Savings Plan benefit that’s associated with the corresponding Savings Plan covered usage item.
- **Savings Plan recurring fee**: Any recurring hourly charges that correspond with your No Upfront or Partial Upfront Savings Plan. The Savings Plan recurring fee is initially added to your bill on the day that you purchase a No Upfront or Partial Upfront Savings Plan. After the initial purchase, AWS adds the recurring fee hourly. For an All Upfront Savings Plan, the line item indicates the portion of the Savings Plan unused during the billing period. For example, if a Savings Plan was 100% utilized for a billing period, this shows as “0” in your amortized costs view. Any number greater than “0” indicates an unused Savings Plan.
- **Savings Plan upfront fee**: Any one-time upfront fee from your purchase of an All Upfront or Partial Upfront Savings Plan.

- **Support fee**: Any charges that AWS charges you for a support plan. When you purchase a support plan from AWS, you pay a monthly charge in exchange for service support. The monthly fees can result in spikes on the first day of every month, when AWS charges your account.
- **Tax**: Any taxes that are associated with the charges or fees in your cost chart. Cost Explorer adds all taxes together as a single component of your costs. If you select five or fewer filters, Cost Explorer displays your tax expenses as a single bar. If you select six or more filters, Cost Explorer displays five bars, stacks, or lines, and then aggregates all remaining items, including taxes, into a sixth bar, stack slice, or plot line that's labeled **Other**.
- **Upfront reservation fee**: Any upfront fees that are charged to your account. When you purchase an All Upfront or Partial Upfront Reserved Instance from AWS, you pay an upfront fee in exchange for a lower rate for using the instance. The upfront fees can result in spikes in the chart for the days or months when you make your purchases.
- **Usage**: Usage that AWS didn't apply reservation discounts to.

Cost category

Choose the cost category group and value to track with this budget. To learn more about setting up cost categories, see Organizing costs using AWS Cost Categories.

Instance family

Choose the family of instances to track using this budget.

Instance type

Choose the type of instance that you want to track with this budget.

Invoicing entity

The AWS entity that issues the invoice. Possible values include:

- Amazon Web Services, Inc. – The entity that issues invoices to customer globally, where applicable.
- Amazon Web Services India Private Limited – The entity that issues invoices to customers based in India.
- Amazon Web Services South Africa Proprietary Limited – The entity that issues invoices to customers in South Africa.

Legal entity

The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. The values might differ for third-party AWS Marketplace transactions. Possible values include:

- Amazon Web Services, Inc. – The entity that sells AWS services.
- Amazon Web Services India Private Limited – The local Indian entity that acts as a reseller for AWS services in India.

> **Note**
>
> Amazon Web Services EMEA SARL is the marketplace operator for your purchases if your account is located in EMEA (excluding Turkey and South Africa), and the seller is eligible in EMEA. Purchases include subscriptions. Amazon Web Services, Inc. is the marketplace operator for purchases if the seller isn't eligible for EMEA. For more information, see AWS Europe.

Linked account

Choose an AWS account that is a member of the consolidated billing family that you're creating the budget for. For more information, see Consolidated billing for AWS Organizations in the *AWS Billing User Guide*.

> **Note**
>
> Do not use this filter within a member account. If the current account is a member account, filtering by `linked account` is not supported.

Platform

Choose the operating system that your RI runs on. **Platform** is either **Linux** or **Windows**.

Product attribute

Choose an attribute and one or more values to track your Amazon Bedrock costs. You can choose from the following attributes:

- **Provider** (`provider`) is the company that offers the model, such as Anthropic, Cohere, or OpenAI.

- **Model** (`model`) is the model name, such as Claude Sonnet 5 or Claude Haiku 4.5.
- **Inference type** (`inferenceType`) is the type of usage, such as input tokens, output tokens, or prompt cache read input tokens.
- **Feature** (`feature`) is how the model was used, such as on-demand inference.

> **Note**
>
> Budgets that use a product attribute filter support actual cost alerts only. Forecasted alerts aren't supported for these budgets.

Purchase option

Choose `On Demand Instances`, `Standard Reserved Instances`, or `Savings Plans`.

Region

Choose the Region in which the resource that you want to create a budget for is running.

Savings Plans type

Choose what you want to budget for, between **Compute Savings Plans** and **EC2 Instance Savings Plans**. The Savings Plans type filter is only available for Savings Plans utilization budgets.

Scope

Choose the scope of your RI. The scope is either regional or zonal.

Service

Choose an AWS service. Combined with **Billing entity**, **Invoicing entity**, and **Legal entity**, you can also use the **Service** dimension to filter costs by specific AWS Marketplace purchases. This includes your costs for specific AMIs, web services, and desktop apps. For more information, see What Is AWS Marketplace?

> **Note**
>
> You can use this filter only for cost, Savings Plans and Reserved Instance (RI) utilization, or Savings Plans and RI coverage budgets. Cost Explorer doesn't show revenue or usage for the AWS Marketplace software seller.

The Savings Plans utilization, RI utilization, Savings Plans coverage reports, and RI coverage reports lets you filter by only one service at a time and only for the following services:

- Amazon Elastic Compute Cloud
- Amazon Redshift
- Amazon Relational Database Service
- Amazon ElastiCache
- Amazon OpenSearch Service

Tag

If you activated any tags, choose a resource tag. A tag is a label that you can use to organize your resource costs and track them on a detailed level. There are AWS generated tags and user-defined tags. User-defined tag keys must use the `user:` prefix. You must activate tags to use them. For more information, see Activating the AWS-Generated Cost Allocation Tags and Activating User-Defined Cost Allocation Tags.

Tenancy

Choose whether you share an RI with another user. **Tenancy** is either **Dedicated** or **Default**.

Usage type

Usage types are the units each service uses to measure the usage for specific types of resources. If you choose a filter such as S3 and then choose a usage type value, such as `DataTransfer-Out-Bytes (GB)`, your costs are limited to S3 `DataTransfer-Out-Bytes (GB)`. You can create a usage budget only for a specific unit of measure. If you choose **Usage type** but not **Usage type group**, the budget monitors all of the available units of measure for the usage type.

Usage type group

A usage type group is a collection of usage types that have the same unit of measure. If you choose both the **Usage type group** and the **Usage type** filters, Cost Explorer shows you usage types that are automatically constrained to the group unit of measure. For example, assume you choose the group `EC2: Running Hours (Hrs)`, and then choose the `EC2-Instances` filter for **Usage type**. Cost Explorer shows you only the usage types that are measured in hours.

Viewing your budgets

You can view the state of your budgets at a glance on the **Budgets Overview** page. Your budgets are listed in a filterable table along with the following data:

- Your current costs and usage incurred for a budget during the budget period
- Your budgeted costs or usage for the budget period
- Your forecasted usage or costs for the budget period
- A percentage that shows your costs or usage compared to your budgeted amount
- A percentage that shows your forecasted costs or usage compared to your budgeted amount
- The billing view associated with the budget and its health status:
  - `HEALTHY`: Indicates the budget has proper access to the billing view data
  - `UNHEALTHY`: Indicates the budget cannot access the billing view data, which may occur if permissions have been revoked or the view has been deleted

> **Note**
>
> When accessing budget performance history for a budget based on a cross-account billing view, you need the `billing:GetBillingViewData` permission. This permission is required because the operation provides historical cost and usage data from the source account's billing view.
> AWS doesn't support billing transfer views for bill transfer accounts.

To view your budgets

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.
3. To see the filters and cost variances for your budgets, choose the budget's name in your list of budgets.

> **Note**
>
> You can view information about multiple budgets at once by selecting the check boxes in the Overview table. This opens a split-view panel on the right-hand side, where you can sort or filter the alerts to customize a budget report.

Reading your budgets

You can view detailed information about your budgets in two ways.

- Select your budget in the table to open a split-view panel with budget history and alert status on the right-hand side. In the split-view panel, navigation buttons allow you to move between budgets without leaving the page. To use the navigation buttons, select one budget at a time. When multiple budgets are selected, the navigation buttons are hidden.
- Choose your budget's name to see the budget details page. This page includes the following information:
  - **Current vs. budgeted** – Your current incurred costs compared to your budgeted costs.
  - **Forecasted vs. budgeted** – Your forecasted costs compared to your budgeted costs.
  - **Alerts** – Any alerts or notifications about the state of your budgets.
  - **Details** – The amount, type, time period, and any other additional parameters for your budget.
  - **Budget history** tab – A chart and table that show the history of your budget. `QUARTERLY` budgets show the last four quarters of history, and `MONTHLY` budgets show the last 12 months. Budget history isn't available for `ANNUAL` budgets.

    If you change the budgeted amount for a budget period, then the budgeted amount in the table is the last budgeted amount. For example, if you have a monthly budget set for 100 in January and you change the budget to 200 in February, then the February line in the table shows only the 200 budget.
  - **Alerts** tab – More details for any alerts about the state of your budget, including a **Definition** that describes the conditions for exceeding the alert threshold.
- For budgets using **custom** time periods, you can view the following information:
  - **Current vs. budgeted costs** - Compare your current incurred costs against your total budget for the time period.
  - **Time remaining** - View the remaining duration in your custom budget period.

- **Historical data** - View historical budget data based on the following time frames:
  - For Reserved Instance (RI) and Savings Plans(SP) budgets: Up to 14 months of historical data
  - For cost and usage budgets:
    - Multi-year data enabled - up to 38 months of historical data
    - Multi-year data disabled - up to 14 months of historial data
  - For daily views: Up to 14 months of historical data
  - For monthly views: Up to 12 months of historical data

You can use this information to see how well your budget has matched your costs and usage in the past. You can also download all of the data that Budgets used to create the table through the following procedure.

To download a budget in a CSV file

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.
3. To see the filters and cost variances for your budgets, choose the budget name in your list of budgets.
4. On the **Budget history** tab, choose **Download as CSV**.
5. Follow the instructions onscreen.

Editing a budget

> **Note**
>
> You can't edit the budget name.

To add or edit email recipients on an existing budget's notifications, see Adding email recipients to a budget notification.

To edit a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.
3. On the **Budgets** page, from your list of budgets, choose the budget that you want to edit.
4. Choose **Edit**.
5. Change the parameters that you want to edit. You can't change the budget name.
6. After you make your changes on each page, choose **Next**.
7. Choose **Save**.

Downloading a budget

You can download your budgets as a CSV file. The file includes all of the data for all of your budgets, such as Budget Name, Current Value and Forecasted Value, Budgeted Value, and more.

To download a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.
3. Choose **Download CSV**.
4. Open or save your file.

Copying a budget

You can copy an existing budget to a new one. By doing this, you can retain the filters and notification settings from your original budget, or change them. Billing and Cost Management automatically populates the fields on the page that you create the new budget on. You can update the budget parameters on this page.

To copy a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.

3. From the list of budgets, select the budget that you want to copy.
4. At the top of the page, choose **Actions**, and then choose **Copy**.
5. Change the parameters that you want to update. You must change the budget name.
6. After you make any necessary changes on each page, choose **Next**.
7. Choose **Copy budget**.

Deleting a budget

You can delete your budgets and the associated email and Amazon SNS notifications at any time. However, you can't recover a budget after you delete it. If you delete a budget, all email notifications and notification subscribers that are associated with the budget are also deleted.

To delete a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. On the navigation pane, choose **Budgets**.
3. From your list of budgets, select one or more budgets that you want to delete.
4. At the top of the page, choose **Actions**, and then choose **Delete**.
5. Choose **Confirm**.

Configuring budget actions

You can use AWS Budgets to run an action on your behalf when a budget exceeds a certain cost or usage threshold. To do this, after you set a threshold, configure a budget action to run either automatically or after your manual approval.

Your available actions include applying an IAM policy or a service control policy (SCP). They also include targeting specific Amazon EC2 or Amazon RDS instances in your account. You can use SCPs so that you don't need to provision any new resources during the budget period.

> **Note**
>
> From the management account, you can apply an SCP to another account. However, you can't target Amazon EC2 or Amazon RDS instances in another account.

You can also configure multiple actions to initiate at the same notification threshold. For example, you can configure actions to initiate automatically when you reach 90 percent of your forecasted costs for the month. To do so, perform the following actions:

- Apply a custom `Deny IAM` policy that restricts the ability for a user, group, or role to provision additional Amazon EC2 resources.
- Target specific Amazon EC2 instances in `US East (N. Virginia) us-east-1`.

Topics

- Setting up a role for AWS Budgets to run budget actions
- Configuring a budget action
- Reviewing and approving your budget action

Setting up a role for AWS Budgets to run budget actions

To use budget actions, you must create a service role for AWS Budgets. A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

To allow AWS Budgets to perform actions on your behalf, you must grant the necessary permissions to the service role. The following table lists the permissions that you can grant the service role.

Permissions policy for budget actions	Instructions
Allows permission to control AWS resources	This is an AWS managed policy. For instructions on how to attach a managed policy, see To use a managed policy as a permissions policy for an identity (console) in the *IAM User Guide*
Allow AWS Budgets to apply IAM policies and SCPs	You can use this example policy as an inline policy or a customer managed policy.

Permissions policy for budget actions	Instructions
	For instructions on how to embed an inline policy, see To embed an inline policy for a user or role (console) in the *IAM User Guide*. For instructions on how to create a customer managed policy, see Creating IAM policies (console) in the *IAM User Guide*.
Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances	You can use this example policy as an inline policy or a customer managed policy. For instructions on how to embed an inline policy, see To embed an inline policy for a user or role (console) in the *IAM User Guide*. For instructions on how to create a customer managed policy, see Creating IAM policies (console) in the *IAM User Guide*.

Configuring a budget action

You can attach budget actions to an alert for either a cost budget or a usage budget. To configure a budget action on a new budget, first follow the steps for Creating a cost budget or Creating a usage budget. To configure a budget action on an existing cost or usage budget, first follow the steps for Editing a budget. Then, after you reach the **Configure alerts** step of creating or editing the budget, use the following procedure.

To configure a budget action

1. To configure a budget action on a new alert, choose **Add an alert threshold**. To configure a budget action on an existing alert, skip to step 7.
2. Under **Set alert threshold**, for **Threshold**, enter the amount that needs to be reached for you to be notified. This can be either an absolute value or a percentage. For example, say you have a budget of 200 dollars. To be notified at 160 dollars (80% of your budget), enter **160** for an absolute budget or **80** for a percentage budget.

Next to the amount, choose **Absolute value** to be notified when your costs exceed the threshold amount. Or, choose **% of budgeted amount** to be notified when your costs exceed the threshold percentage.

Next to the threshold, choose **Actual** to create an alert for actual spend. Or, choose **Forecasted** to create an alert for forecasted spend.

3. (Optional) Under **Notification preferences - Optional**, for **Email recipients**, enter the email addresses that you want the alert to notify. Separate multiple email addresses with commas. A notification can have up to 10 email addresses.
4. (Optional) Under **Notification preferences - Optional**, for **Amazon SNS Alerts**, enter the Amazon Resource Name (ARN) for your Amazon SNS topic. For instructions on how to create a topic, see Creating an Amazon SNS topic for budget notifications.

> **Important**
>
> After you create a budget with Amazon SNS notifications, Amazon SNS sends a confirmation email to the email addresses that you specified. The subject line is **AWS Notification - Subscription Confirmation**. The recipient must choose **Confirm subscription** in the confirmation email to receive future notifications.

5. (Optional) Under **Notification preferences - Optional**, for **Amazon Q Developer in chat applications Alerts**, you can configure Amazon Q Developer in chat applications to send budget alerts to an Amazon Chime or Slack chat room. You configure these alerts through the Amazon Q Developer in chat applications console.
6. Choose **Next**.
7. For **Attach actions - Optional**, choose **Add Action**.

    a. For **Select IAM role**, choose an IAM role to allow AWS Budgets to perform an action on your behalf.

> **Note**
>
> If you didn't configure and assign the appropriate permissions for the IAM role and for AWS Budgets, then AWS Budgets can't run your configured actions. For simplified permissions management, we recommend that you use the managed policy. This ensures that your AWS Budgets actions work as intended and eliminates the need to update your existing IAM policy for AWS Budgets whenever

any new functionality is added. This is because new functions and capabilities are added to the managed policy by default. For more information about managed policies, see Managed policies.

For more information and examples of IAM role permissions, see Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances.

b. For **Which action type should be applied when the budget threshold has been exceeded**, select the action that you want AWS Budgets to take on your behalf.

You can choose from applying an IAM policy, attaching a service control policy (SCP), or targeting specific Amazon EC2 or Amazon RDS instances. You can apply multiple budget actions to a single alert. Only a management account can apply SCPs.

c. Depending on the action that you chose, complete the fields related to the resources that you want to apply the action to.

d. For **Do you want to automatically run this action when this threshold is exceeded**, choose **Yes** or **No**. If you choose **No**, then you run the action manually on the **Alert details** page. For instructions, see Reviewing and approving your budget action.

e. For **How do you want to be alerted when this action is run**, choose **Use the same alert settings when you defined this threshold** or **Use different alert settings**. To use different alert settings, complete the **Notification preferences** specific to this action.

8. Choose **Next**.

> **Note**
>
> To proceed, you must configure at least one of the following for each alert:
>
> - An email recipient for notifications
> - An Amazon SNS topic for notifications
> - A budget action

9. Review your budget settings, and then choose **Create budget** or **Save**.

After you create an action, you can view its status from the AWS Budgets page on the **Actions** column. This column shows your configured actions count, actions waiting for your approval (**Requires approval**), and your successfully completed actions.

Reviewing and approving your budget action

You receive a notification to inform you that an action is pending or has already run on your behalf, regardless of your action preferences. The notification includes a link to the **Budget details** page of the action. You can also navigate to the **Budget details** page by choosing the budget name on the AWS Budgets page.

On the **Budget details** page, you can review and approve your budget action.

To review and approve your budget action

1. On the **Budget details** page, in the **Alerts** section, choose **Requires approval**.
2. In the **Actions** pop-up, choose the name of the alert that requires an action.
3. On the **Alert details** page, in the **Action** section, review the action that requires approval.
4. Select the action that you want to run, and then choose **Run action**.
5. Choose **Yes, I am sure**.

Your pending actions move from the `pending` status in **Action history**, listing the newest actions at the top. AWS Budgets shows actions configured and run in the last 60 days. You can view the full history of actions by using AWS CloudTrail or by calling the `DescribeBudgetActionHistories` API.

Reversing a previous action

You can review and undo previously completed actions from the **Action history** table. Each status is defined as follows:

- **Standby** - AWS Budgets is actively evaluating the action.
- **Requires approval** - The action was initiated, and is waiting for your approval.
- **Completed** - The action successfully completed.
- **Reversed** - The action was undone, and AWS Budgets will no longer evaluate the action for the remaining budgeted period.

If you want AWS Budgets to re-evaluate the reversed action during the same period, you can choose **Reset**. You can do this, for example, if you initiated a read-only policy but then received approval from your manager to increase your budget and adjust your budgeted amount during the current period.

Creating an Amazon SNS topic for budget notifications

When you create a budget that sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, you need to either have a preexisting Amazon SNS topic or create one. Amazon SNS topics allow you to send notifications over SNS in addition to email. Your budget must have permissions to send a notification to your topic.

To create an Amazon SNS topic and grant permissions to your budget, use the Amazon SNS console.

> **Note**
>
> Amazon SNS topics must be in the same account as the Budgets you're configuring. Cross-account Amazon SNS isn't supported.

To create an Amazon SNS notification topic and grant permissions

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. On the navigation pane, choose **Topics**.
3. Choose **Create topic**.
4. For **Name**, enter the name for your notification topic.
5. (Optional) For **Display name**, enter the name that you want displayed when you receive a notification.
6. In **Access policy**, choose **Advanced**.
7. In the policy text field, after **"Statement": [**, add the following text:

```
{
  "Sid": "E.g., AWSBudgetsSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "budgets.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN",
   "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "<account-id>"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:budgets::<account-id>:*"
        }
      }
}
```

8. Replace **E.g., AWSBudgetsSNSPublishingPermissions** with a string. The `Sid` must be unique within the policy.
9. Choose **Create topic**.
10. Under **Details**, save your ARN.
11. Choose **Edit**.
12. Under **Access policy**, replace *your topic ARN* with the Amazon SNS topic ARN from step 10.
13. Choose **Save changes**.

    Your topic now appears in the list of topics on the **Topics** page.

Troubleshooting

You might encounter the following error messages when you're creating your Amazon SNS topic for budget notifications.

Please comply with SNS ARN format

There's a syntax error in the ARN you replaced (step 9). Confirm the ARN for proper syntax and formatting.

Invalid SNS topic

AWS Budgets doesn't have access to the SNS topic. Confirm that you've allowed budgets.amazonaws.com the ability to publish messages to this SNS topic, in the SNS topic's resource based policy.

The SNS topic is encrypted

You have **encryption** enabled on the SNS topic. The SNS topic won't work without additional permissions. Disable encryption on the topic, and refresh the **Budget edit** page.

Checking or resending notification confirmation emails

When you create a budget with notifications, you also create Amazon SNS notifications. For notifications to be sent, you must accept the subscription to the Amazon SNS notification topic.

To confirm that your notification subscriptions have been accepted or to resend a subscription confirmation email, use the Amazon SNS console.

To check your notification status or to resend a notification confirmation email

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. On the navigation pane, choose **Subscriptions**.
3. On the **Subscriptions** page, for **Filter**, enter `budget`. A list of your budget notifications appears.
4. Check the status of your notification. Under **Status**, `PendingConfirmation` appears if a subscription hasn't been accepted and confirmed.
5. (Optional) To resend a confirmation request, select the subscription with a pending confirmation and choose **Request confirmation**. Amazon SNS sends a confirmation request to the endpoints that are subscribed to the notification.

   When each owner of an endpoint receives the email, they must choose the **Confirm subscription** link to activate the notification.

Protecting your Amazon SNS budget alerts data with SSE and AWS KMS

You can use server-side encryption (SSE) to transfer sensitive data in encrypted topics. SSE protects Amazon SNS messages by using keys managed in AWS Key Management Service (AWS KMS).

To manage SSE using AWS Management Console or the AWS Service Development Kit (SDK), see Enabling Server-Side Encryption (SSE) for an Amazon SNS Topic in the *Amazon Simple Notification Service Getting Started Guide*.

To create encrypted topics using AWS CloudFormation, see the AWS CloudFormation User Guide.

SSE encrypts messages as soon as Amazon SNS receives them. The messages are stored encrypted and are decrypted using Amazon SNS only when they're sent.

Configuring AWS KMS permissions

You must configure your AWS KMS key policies before you can use SSE. The configuration enables you to encrypt topics, as well as encrypt and decrypt messages. For details about AWS KMS permissions, see AWS KMS API Permissions: Actions and Resources Reference in the *AWS Key Management Service Developer Guide*.

You can also use IAM policies to manage AWS KMS key permissions. For more information, see Using IAM Policies with AWS KMS.

> **Note**
>
> Although you can configure global permissions to send and receive message from Amazon SNS, AWS KMS requires you to name the full ARN of AWS KMS keys (KMS key) in the specific Regions. You can find this in the **Resource** section of an IAM policy.
> You must ensure that the key policies of the KMS keys allow the necessary permissions. To do this, name the principals that produce and consume encrypted messages in Amazon SNS as users in the KMS key policy.

To enable compatibility between AWS Budgets and encrypted Amazon SNS topics

1. Create a KMS key.
2. Add the following text to the KMS key policy.
3. Enable SSE for your SNS topic.

   > **Note**
   >
   > Be sure that you're using the same KMS key that grants AWS Budgets the permissions to publish to encrypted Amazon SNS topics.

4. Choose **Save Changes**.

Adding email recipients to a budget notification

To be notified about your budget's status, add email recipients to your budget notifications. When you add a new email address as a recipient, AWS Budgets sends a verification email to that address, and only verified addresses receive budget notifications. Email verification uses AWS User

Notifications and follows the same recipient-confirm pattern used by other AWS services that rely on User Notifications. Email recipients on budgets created before AWS Budgets added verification continue to receive notifications without change. This topic describes how to add email recipients to a budget notification, how verification works, and how to troubleshoot verification issues.

You can add up to 10 email recipients per budget notification.

> **Note**
>
> This topic covers email recipients added directly to a budget notification. If you send budget notifications through an Amazon SNS topic, see Creating an Amazon SNS topic for budget notifications, which describes the Amazon SNS subscription confirmation flow separately.

How verification works

When you add an email address as a recipient to a budget notification, AWS Budgets sends a verification email to that address. The verification email is sent from an `@aws.com` sender address. The recipient confirms the address by choosing the link in the verification email, which opens the AWS Management Console. The recipient must be signed in to the AWS account that added the email address to complete verification. Once verified, AWS Budgets begins sending budget notifications to the address. If the recipient does not verify the address, AWS Budgets does not send notifications to it.

If the recipient address is already verified for the same AWS account through another AWS service that uses User Notifications, adding it to a AWS Budgets recipient list activates it without a new verification email. The address appears with an Active status immediately.

Every email address is verified in an AWS account. If the same email address is a recipient on multiple budgets in the same account, one verification covers every budget. If the same email address is used across budgets in different AWS accounts (for example, a central FinOps address subscribed in linked accounts across an organization), each account requires its own verification, and the recipient must sign in to each account to complete verification. For scenarios where a single verification for many recipients is preferred, add an email distribution list as the recipient and manage list membership separately.

Verification status

Verification status appears in the AWS Budgets console on the budget detail page. Each recipient row shows one of the following statuses:

Active

The recipient confirmed the address, or the address was already verified for the AWS account through another AWS service that uses User Notifications. The address receives notifications.

Pending

AWS Budgets sent a verification email and is waiting for the recipient to confirm.

Active (legacy)

The address was added to a budget notification before AWS Budgets introduced verification, and continues to receive notifications without change. No action is required.

Inactive

The address is not yet registered to receive notifications. Choose **Send Notification** to register the address and send a verification email. The status moves to Pending until the recipient confirms.

Each recipient row with a Pending status includes a **Resend verification** button that sends a fresh verification email. Rows with an Inactive status include a **Send Notification** button that registers the address to receive notifications and sends a verification email.

Adding an email recipient to a budget notification

Follow these steps when creating a new budget or adding a recipient to an existing budget.

To add an email recipient

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management and Cost Management console at https://console.aws.amazon.com/cost-management/.
2. In the navigation pane, choose **Budgets**.
3. Create a new budget or open an existing budget, and add or edit an alert.
4. In the **Email recipients** field, enter one or more email addresses and save the alert.

5. AWS Budgets sends a verification email to each address that is not already verified in your account.
6. Each recipient must open the verification email, choose the link, and sign in to the AWS account that added the address. Verification completes in the AWS Management Console.
7. Refresh the budget detail page to see the updated verification status.

Verified recipients begin receiving budget notifications on the next scheduled evaluation.

Troubleshooting

The recipient did not receive the verification email

Ask the recipient to check the spam folder. Verification emails come from an `@aws.com` sender address. If your organization uses an email allow list, add the `@aws.com` domain. If the email is not there, verify the address is correct in the AWS Budgets console. Choose **Resend verification** to try again. Verification emails are subject to a short cooldown between sends to protect email deliverability.

The verification link has expired

Verification links expire 12 hours after send. Choose **Resend verification** to send a new link.

The recipient's status is Inactive

An Inactive status means the address is not yet registered to receive notifications. Verify the address in the AWS Budgets console and correct any typos, then choose **Send Notification** to register the address.

The recipient cannot complete verification

Verification requires the recipient to sign in to the AWS account that added the email address. If the recipient does not have access to that account, ask an administrator with access to that account to complete verification, or use a different recipient address. For scenarios where recipients cannot sign in to AWS, consider using an email distribution list as the recipient and managing list membership outside AWS.

A recipient address is verified in one AWS account but not another

Verification is per email address per account. Each account requires its own verification, even for the same email address, and the recipient must sign in to each account to complete verification.

Receiving budget alerts in chat applications

You can use Amazon Q Developer to receive and monitor your budget alerts in Amazon Chime, Microsoft Teams, and Slack.

Amazon Chime

To begin receiving your budget alerts in Amazon Chime

1. Go to AWS Budgets and either create a new budget or edit an existing one.
2. In the budget configuration, choose **Configure alerts**.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts.

   > **Note**
   >
   > To ensure AWS Budgets has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for budget notifications.

4. Complete and save your budget configuration.
5. Open Amazon Chime.
6. For **Amazon Chime**, choose the chat room that you want to set up to receive notifications through Amazon Q Developer.
7. Choose the Room settings icon on the top right and choose **Manage webhooks and bots**.

   Amazon Chime displays the webhooks associated with the chat room.
8. For the webhook, choose **Copy URL**, and then choose **Done**.

   If you need to create a new webhook for the chat room, choose **Add webhook**, enter a name for the webhook in the **Name** field, and then choose **Create**.
9. Open the Amazon Q Developer in chat applications console.
10. Choose **Configure new client**.
11. Choose **Amazon Chime**, and then choose **Configure**.
12. Under **Configuration details**, enter a name for your configuration. The name must be unique across your account and can't be edited later.
13. To configure Amazon Chime webhook, do the following:

    1. For **Webhook URL**, paste the webhook URL that you copied from Amazon Chime.

2. For **Webhook description**, use the following naming convention to describe the purpose of the webhook: **Chat_room_name/Webhook_name**. This helps you associate Amazon Chime webhooks with their Amazon Q Developer configurations.

14. If you want to enable logging for this configuration, choose **Publish logs to Amazon CloudWatch Logs**. For more information, see Amazon CloudWatch Logs for Amazon Q Developer.

> **Note**
>
> There is an additional charge for using Amazon CloudWatch Logs.

15. For **Permissions**, set the IAM permissions as follows:

    1. For **IAM role**, choose **Create an IAM role using a template**. If you want to use an existing role instead, choose it from the **IAM role** list. To use an existing IAM role, you might need to modify it for use with Amazon Q Developer. For more information, see Configuring an IAM Role for Amazon Q Developer.
    2. For **Role name**, enter a name. Valid characters: a-z, A-Z, 0-9.
    3. For **Policy templates**, choose **Notification permissions**. This is the IAM policy provided by Amazon Q Developer. It provides the necessary Read and List permissions for CloudWatch alarms, events, and logs, and for Amazon SNS topics.

16. Set up the SNS topics that will send notifications to the Amazon Chime webhook.

    1. For **SNS Region**, choose the AWS Region that hosts the SNS topics for this Amazon Q Developer subscription.
    2. For **SNS topics**, choose the SNS topic for the client subscription. This topic determines the content that's sent to the Amazon Chime webhook. If the region has additional SNS topics, you can choose them from the same dropdown list.

    > **Note**
    >
    > You can send budget alerts to multiple Amazon SNS topics and Regions.
    > At least one of the Amazon SNS topics must match the Amazon SNS topic or topics of your budget or budgets.

    3. If you want to add an SNS topic from another Region to the notification subscription, choose **Add another Region**.

17. Choose **Configure**.

For any additional details, see Tutorial: Get started with Amazon Chime in the *Amazon Q Developer in chat applications Administrator Guide*.

Microsoft Teams

To begin receiving your budget alerts in Microsoft Teams

1. Go to AWS Budgets and either create a new budget or edit an existing one.
2. In the budget configuration, choose **Configure alerts**.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts.

> **Note**
>
> To ensure AWS Budgets has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for budget notifications.

4. Complete and save your budget configuration.
5. Add Amazon Q Developer to your team.
6. Open the Amazon Q Developer in chat applications console.
7. Choose **Configure new client**.
8. Choose **Microsoft Teams**, and then choose **Configure**.
9. Copy and paste your Microsoft Teams channel URL.
10. Choose **Configure**.
11. On the Microsoft Teams authorization page, choose **Accept**.

For any additional details, see Tutorial: Get started with Microsoft Teams in the *Amazon Q Developer in chat applications Administrator Guide*.

Slack

To begin receiving your budget alerts in Slack

1. Go to AWS Budgets and either create a new budget or edit an existing one.
2. In the budget configuration, choose **Configure alerts**.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts.

> **Note**
>
> To ensure AWS Budgets has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for budget notifications.

4. Complete and save your budget configuration.
5. Add Amazon Q Developer to the Slack workspace.
6. Open the Amazon Q Developer in chat applications console.
7. Choose **Configure new client**.
8. Choose **Slack**, and then choose **Configure**.
9. From the dropdown list at the top right, choose the Slack workspace that you want to use with Amazon Q Developer.
10. Choose **Allow**.

For any additional details, see Tutorial: Get started with Slack in the *Amazon Q Developer in chat applications Administrator Guide*.

Reporting your metrics with AWS Budgets Reports

With AWS Budgets, you can configure a report to monitor the performance of your existing budgets on a daily, weekly, or monthly cadence and deliver that report to up to 50 email addresses.

You can create up to 50 reports for each standalone account or AWS Organizations management account. Each budget report costs $.01 USD for each report delivered. This is regardless of the number of recipients receiving the report. For example, a daily budget report costs $.01 a day, a weekly budget report costs $.01 a week, and a monthly budget report costs $.01 a month.

If you use consolidated billing in an organization and you own the management account, you can use IAM policies to control access to budgets by member accounts. By default, owners of member accounts can create their own budgets but can't create or edit budgets for other users. You can use IAM to allow users in a member account to create, edit, delete, or read the budget for your management account. Do this, for example, to allow another account to administer your budget. For more information, see Overview of managing access permissions. For more information about AWS Organizations, see the AWS Organizations User Guide.

Topics

- Creating an AWS Budgets report
- Editing an AWS Budgets report
- Copying an AWS Budgets report
- Deleting an AWS Budgets report

Creating an AWS Budgets report

Use the following procedure to create an AWS Budgets report.

To create an AWS Budgets report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets Reports**.
3. On the top right of the page, choose **Create budget report**.
4. Select the budgets that you want to include in your report. You can select up to 50 budgets.

   > **Note**
   >
   > If you select more, you can't proceed to the next step until you change your selection to 50 or fewer budgets.

5. For **Report frequency**, choose **Daily**, **Weekly**, or **Monthly**.

   - If you choose a **Weekly** report: For **Day of week**, choose the day of the week that you want the report delivered.
   - If you choose a **Monthly** report: For **Day of month**, choose the calendar day of the month that you want the report delivered. If you choose any day after the 28th day, and the next month doesn't have that calendar day, then your report is delivered on the last day of that month.

   Reports are delivered at approximately 0:00 UTC+0 on the specified day.
6. For **Email recipients**, enter the email addresses to deliver the report to. Separate multiple email addresses with commas. You can include up to 50 email recipients for each budget report.

7. For **Budget report name**, enter the name of your budget report. This name appears on the subject line of the budget report email. You can change the report name at any time.
8. Choose **Create budget report**.

Your report appears on the AWS Budgets Reports dashboard. On the dashboard, you can filter your reports by **Report name**. For each report, the dashboard also shows **Frequency**, **Budgets included**, and **Recipient(s)**.

Editing an AWS Budgets report

You can use this procedure to edit an AWS Budgets report.

To edit an AWS Budgets report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets Reports**.
3. Choose the name of the report that you want to edit.
4. On the **Edit budget report** page, change the parameters that you want to edit.
5. Choose **Save**.

Copying an AWS Budgets report

Use the following procedure to copy an AWS Budgets report.

To copy an AWS Budgets report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets Reports**.
3. From the list of reports, select the report that you want to copy.
4. At the top of the page, choose **Actions**, and then choose **Copy**.
5. Change the parameters that you want to update.
6. Choose **Create budget report**.

Deleting an AWS Budgets report

Use the following procedure to delete an AWS Budgets report.

To delete an AWS Budgets report

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets Reports**.
3. From the list of reports, select the report that you want to delete.
4. At the top of the page, choose **Actions**, and then choose **Delete**.
5. Choose **Confirm**.

Detecting unusual spend with AWS Cost Anomaly Detection

AWS Cost Anomaly Detection is a feature that uses machine learning models to detect and alert on anomalous spend patterns in your deployed AWS services.

Using AWS Cost Anomaly Detection includes the following benefits:

- You receive alerts individually in aggregated reports either in an email message or an Amazon SNS topic.

  For Amazon SNS topics, create an Amazon Q Developer in chat applications configuration that maps the Amazon SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving anomaly alerts in chat applications.
- You can evaluate your spend patterns using machine learning methods to minimize false positive alerts. For example, you can evaluate weekly or monthly seasonality and natural growth.
- You can investigate the root causes of the anomaly, ranked by their dollar impact and split across four dimensions: AWS service, AWS account, Region, or usage type.
- You can configure how to evaluate your costs. Choose whether you want to analyze all of your AWS services independently or analyze specific member accounts, cost allocation tags, or cost categories.

After your billing data is processed, AWS Cost Anomaly Detection runs approximately three times a day in order to monitor for anomalies in your net unblended cost data (that is, net costs after all

applicable discounts are calculated). You might experience a slight delay in receiving alerts. Cost Anomaly Detection uses data from Cost Explorer, which has a delay of up to 24 hours. As a result, it can take up to 24 hours to detect an anomaly after a usage occurs. If you create a new monitor, it can take 24 hours to begin detecting new anomalies. For a new service subscription, 10 days of historical service usage data is needed before anomalies can be detected for that service.

Note

You can opt out of Cost Anomaly Detection at any time. For more information, see Opting out of Cost Anomaly Detection.

Cost Anomaly Detection isn't available for bill source accounts that use billing transfer. Cost Anomaly Detection doesn't support billing transfer views.

Cost Anomaly Detection does not monitor third-party products and services available through AWS Marketplace, except for third-party foundation models on Amazon Bedrock. These models appear in Cost Explorer and on your bill under the AWS Marketplace billing entity. To get alerts for other AWS Marketplace charges, use AWS Budgets. A cost budget tracks your total AWS costs, including AWS Marketplace. You can use the **Billing entity** filter to track AWS Marketplace charges specifically. For more information, see Creating a budget.

Topics

- Setting up your anomaly detection
- Controlling access for Cost Anomaly Detection
- Getting started with AWS Cost Anomaly Detection
- Transitioning from customer to AWS managed monitors
- Editing your alert preferences
- Creating an Amazon SNS topic for anomaly notifications
- Receiving anomaly alerts in chat applications
- Using EventBridge with Cost Anomaly Detection
- Using AWS User Notifications with Cost Anomaly Detection
- Opting out of Cost Anomaly Detection
- Investigating anomaly root causes with Amazon Q Developer

Setting up your anomaly detection

The overviews in this section describe how to get started with AWS Cost Anomaly Detection in AWS Billing and Cost Management.

Topics

- Enabling Cost Explorer
- Controlling access using IAM
- Accessing the console
- Quotas

Enabling Cost Explorer

AWS Cost Anomaly Detection is a feature within Cost Explorer. To access AWS Cost Anomaly Detection, enable Cost Explorer. For instructions on how to enable Cost Explorer using the console, see Enabling Cost Explorer.

Controlling access using IAM

After you enable Cost Explorer at the management account level, you can use AWS Identity and Access Management (IAM) to manage access to your billing data for individual users. You can then grant or revoke access on an individual level for each user role, rather than granting access to all users.

A user must be granted explicit permission to view pages in the Billing and Cost Management console. With the appropriate permissions, the user can view costs for the AWS account that the user belongs to. For the policy that grants the necessary permissions to a user, see Billing and Cost Management actions policies.

For more information about using resource-level access and attribute-based access control (ABAC) for Cost Anomaly Detection, see Controlling access for Cost Anomaly Detection.

Accessing the console

When your setup is complete, access AWS Cost Anomaly Detection.

To access AWS Cost Anomaly Detection

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.

Quotas

For the default quotas, see AWS Cost Anomaly Detection.

Controlling access for Cost Anomaly Detection

You can use resource-level access controls and attribute-based access control (ABAC) tags for cost anomaly monitors and anomaly subscriptions. Each anomaly monitor and anomaly subscription resource has a unique Amazon Resource Name (ARN). You can also attach tags (key-value pairs) to each feature. Both resource ARNs and ABAC tags can be used to give granular access control to user roles or groups within your AWS accounts.

For more information about resource-level access controls and ABAC tags, see How AWS Cost Management works with IAM.

> **Note**
>
> Cost Anomaly Detection doesn't support resource-based policies. Resource-based policies are directly attached to AWS resources. For more information about the difference between policies and permissions, see Identity-based policies and resource-based policies in the *IAM User Guide*.

Controlling access using resource-level policies

You can use resource-level permissions to allow or deny access to one or more Cost Anomaly Detection resources in an IAM policy. Alternatively, use resource-level permissions to allow or deny access to all Cost Anomaly Detection resources.

When you create an IAM, use the following Amazon Resource Name (ARN) formats:

- `AnomalyMonitor` resource ARN

```
arn:${partition}:ce::${account-id}:anomalymonitor/${monitor-id}
```

- AnomalySubscription resource ARN

```
arn:${partition}:ce::${account-id}:anomalysubscription/${subscription-id}
```

To allow the IAM entity to get and create an anomaly monitor or anomaly subscription, use a policy similar to this example policy.

Note

- For `ce:GetAnomalyMonitor` and `ce:GetAnomalySubscription`, users have all or none of the resource-level access control. This requires the policy to use a generic ARN in the form of `arn:${partition}:ce::${account-id}:anomalymonitor/*`, `arn:${partition}:ce::${account-id}:anomalysubscription/*`, or `*`.
- For `ce:CreateAnomalyMonitor` and `ce:CreateAnomalySubscription`, we don't have a resource ARN for this resource. So, the policy always uses the generic ARN that was mentioned in the previous bullet.
- For `ce:GetAnomalies`, use the optional `monitorArn` parameter. When used with this parameter, we confirm if the user has access to the `monitorArn` passed.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ce:GetAnomalyMonitors",
                "ce:CreateAnomalyMonitor"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ce::999999999999:anomalymonitor/*"
        },
        {
            "Action": [
                "ce:GetAnomalySubscriptions",
                "ce:CreateAnomalySubscription"
            ],
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:ce::999999999999:anomalysubscription/*"
        }
    ]
}
```

To allow the IAM entity to update or delete anomaly monitors, use a policy similar to this example policy.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ce:UpdateAnomalyMonitor",
                "ce:DeleteAnomalyMonitor"
                ],
            "Resource": [
              "arn:aws:ce::999999999999:anomalymonitor/f558fa8a-
bd3c-462b-974a-000abc12a000",
              "arn:aws:ce::999999999999:anomalymonitor/f111fa8a-
bd3c-462b-974a-000abc12a001"
  ]
         }
    ]
}
```

Controlling access using tags (ABAC)

You can use tags (ABAC) to control access to Cost Anomaly Detection resources that support tagging. To control access using tags, provide the tag information in the `Condition` element of a policy. You can then create an IAM policy that allows or denies access to a resource based on the resource's tags. You can use tag condition keys to control access to resources, requests, or any part of the authorization process. For more information about IAM roles using tags, see Controlling access to and for users and roles using tags in the *IAM User Guide*.

Create an identity-based policy that allows updating anomaly monitors. If the monitor tag `Owner` has the value of the user name, use a policy that's similar to this example policy.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ce:UpdateAnomalyMonitor"
            ],
            "Resource": "arn:aws:ce::*:anomalymonitor/*",
            "Condition": {
                "StringEquals": {
   "aws:ResourceTag/Owner": "${aws:username}"
     }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ce:GetAnomalyMonitors",
            "Resource": "*"
        }
    ]
}
```

Getting started with AWS Cost Anomaly Detection

With AWS Cost Anomaly Detection in AWS Billing and Cost Management, you can configure your cost monitors and alert subscriptions to automatically adapt to your growing AWS environment.

AWS Cost Anomaly Detection offers AWS managed monitors that automatically track costs across all your accounts, teams, or business units without manual configuration. As your organization grows and changes, these monitors automatically include new accounts, tag values, or categories, maintaining comprehensive coverage without additional setup.

Topics

- Creating your cost monitors and alert subscriptions

- Detected anomalies overview
- Viewing your detected anomalies and potential root causes
- Monitor types

Creating your cost monitors and alert subscriptions

To start monitoring your spend, AWS Cost Anomaly Detection requires setting up at least one cost monitor to define what spending patterns to track. After creating your monitor, you can attach alert subscriptions to specify who receives notifications and through which channels. You can also create individual alerts using AWS User Notifications for more granular control over how alerts are delivered.

> **Note**
>
> You can only access cost monitors and alert subscriptions under the account that created them. Cost monitors for linked accounts, cost allocation tags, and cost categories can only be created in the management account

Cost monitors

To create a cost monitor

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Cost monitors** tab.
4. Choose **Create monitor**.
5. In **Step 1**, choose a monitor type and name your monitor.

   For **Monitor name**, enter a name for your anomaly monitor. We recommend that the name is a short description. That way, you know what the monitor represents when you view your monitors on the **Cost monitors** tab.

   For more information about each monitor type and best practices, see Monitor types.

   Choose your monitor method based on your needs:

- **For AWS managed monitors:**
  1. Under **Monitor method**, select **Managed by AWS**.
  2. Select the dimension you want to monitor:
     - AWS services - Tracks all AWS services automatically
     - Linked account - Tracks all member accounts automatically
     - Cost allocation tag - Tracks all values for a specified tag key
     - Cost category - Tracks all values in a specified category
  3. If you selected Cost allocation tag, specify the tag key from the dropdown (for example, "application-team" or "environment").
  4. If you selected Cost category, specify the category from the dropdown.
- **For customer managed monitors:**
  1. Select the dimension for your monitor.
  2. Under monitor method, select **Customer managed**.
  3. Choose the specific values you want to monitor (up to 10).

6. (Optional) Add a tag to your monitor. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

   a. Enter the key value for the tag.

   b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.

7. Choose **Next**.

8. In **Step 2**, configure your alert subscriptions.

   For **Alert subscription**, if you don't have an existing subscription, choose **Create a new subscription**. If you have existing subscriptions, select **Choose an existing subscription**.

   > **Note**
   >
   > An alert subscription notifies you when a cost monitor detects an anomaly. Depending on the alert frequency, you can notify designated individuals by email or Amazon SNS.
   > For Amazon SNS topics, configure to create an Amazon Q Developer in chat applications configuration. This configuration maps the Amazon SNS topic to a Slack channel or an Amazon Chime chat room. For example, create a subscription

for the Finance team in your organization. For more information, see Receiving anomaly alerts in chat applications.

For **Subscription name**, enter a name that describes your use case. For example, if the subscription is meant for leadership, the subscription name might be “Leadership report.”

Under **Alerting frequency**, choose your preferred notification frequency.

- **Individual alerts** - The alert notifies you as soon as an anomaly is detected. You might receive multiple alerts throughout a day. These notifications require an Amazon SNS topic.

  You can configure the Amazon SNS topic to create an Amazon Q Developer in chat applications configuration that maps the Amazon SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving anomaly alerts in chat applications.
- **Daily summaries** - An email notification with a daily summary of top 10 alerts from the previous day, sorted by cost impact. The system generates this summary at 00:00 UTC daily, though actual delivery time may vary. For example, an anomaly detected at 04:30 UTC on January 14 will be included in the daily summary sent at 00:00 UTC on January 15. At least one email recipient must be specified. For immediate alerts, we recommend using the individual alerts option.
- **Weekly summaries** - An email notification with a weekly summary of alerts. You receive one email per week containing information about multiple anomalies that occurred during that week. At least one email recipient must be specified.

Under **Alert recipients**, enter email addresses for this subscription.

For **Threshold**, enter a number to configure the anomalies that you want to generate alerts for.

There are two types of thresholds: absolute and percentage. Absolute thresholds trigger alerts when an anomaly's total cost impact exceeds your chosen threshold. Percentage thresholds trigger alerts when an anomaly's total impact percentage exceeds your chosen threshold. Total impact percentage is the percentage difference between the total expected spend and total actual spend.

(Optional) Choose **Add threshold** to configure a second threshold on the same subscription. Thresholds can be combined by choosing **AND** or **OR** from the dropdown list.

> **Note**
>
> AWS Cost Anomaly Detection sends you a notification when an anomaly reaches or exceeds the **Threshold**. If an anomaly continues over multiple days, then alert recipients will continue to get notifications while the threshold is met.
> Even if an anomaly is below the alert threshold, the machine learning model continues to detect spend anomalies on your account. All the anomalies that the machine learning model detected (with cost impacts that are greater or less than the threshold) are available in the **Detected anomalies** tab.

9. (Optional) Add a tag to your alert subscription. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

   a. Enter the key value for the tag.

   b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.

10. (Optional) Choose **Add alert subscriptions** to create another alert subscription. With this option, you can create a new subscription using the same monitor.

11. Choose **Create monitor**.

Important considerations for AWS managed monitors:

- Alert subscriptions attached to AWS managed monitors use the same threshold across all tracked values
- As new member accounts, tags, or categories are added to your AWS environment, they're automatically included
- You cannot convert existing customer managed monitors to AWS managed monitors
- For granular alert routing based on specific values, configure AWS User Notifications with JSON filtering patterns

> **Note**
>
> AWS managed monitors can track up to 5,000 values within a dimension. If your organization has more than 5,000 values (for example, more than 5,000 member accounts or tag values), the monitor will track the top 5,000 values based on their total spend.

Alert subscriptions

To create an alert subscription

You must create at least one alert subscription for each monitor. The "create cost monitor steps" that are described earlier already include the alert subscription creation process. If you want to create additional subscriptions, follow these steps.

1. Choose the **Alert subscriptions** tab.
2. Choose **Create a subscription**.
3. For **Subscription name**, enter a name that describes your use case. For example, if the subscription is meant for leadership, then the subscription name might be “Leadership report.”
4. Under **Alerting frequency**, choose your preferred notification frequency.

   - **Individual alerts** - The alert notifies you as soon as an anomaly is detected. You might receive multiple alerts throughout a day. These notifications require an Amazon SNS topic.

     You can configure the Amazon SNS topic to create an Amazon Q Developer in chat applications configuration that maps the Amazon SNS topic to a Slack channel or an Amazon Chime chat room. For more information, see Receiving anomaly alerts in chat applications.
   - **Daily summaries** - An email notification with a daily summary of top 10 alerts from the previous day, sorted by cost impact. The system generates this summary at 00:00 UTC daily, though actual delivery time may vary. For example, an anomaly detected at 04:30 UTC on January 14 will be included in the daily summary sent at 00:00 UTC on January 15. At least one email recipient must be specified. For immediate alerts, we recommend using the individual alerts option.

- **Weekly summaries** - An email notification with a weekly summary of alerts. You receive one email per week containing information about multiple anomalies that occurred during that week. At least one email recipient must be specified.

5. Under **Alert recipients**, enter email addresses for this subscription.
6. For **Threshold**, enter a number to configure the anomalies that you want to generate alerts for.

   There are two types of thresholds: absolute and percentage. Absolute thresholds trigger alerts when an anomaly's total cost impact exceeds your chosen threshold. Percentage thresholds trigger alerts when an anomaly's total impact percentage exceeds your chosen threshold. Total impact percentage is the percentage difference between the total expected spend and total actual spend.

   (Optional) Choose **Add threshold** to configure a second threshold on the same subscription. Thresholds can be combined by choosing **AND** or **OR** from the dropdown list.

   > **Note**
   >
   > AWS Cost Anomaly Detection sends you a notification when an anomaly reaches or exceeds the **Threshold**. If an anomaly continues over multiple days, then alert recipients will continue to get notifications while the threshold is met.
   > Even if an anomaly is below the alert threshold, the machine learning model continues to detect spend anomalies on your account. All the anomalies that the machine learning model detected (with cost impacts that are greater or less than the threshold) are available in the **Detected anomalies** tab.

7. In the **Cost monitors** section, select the monitors that you want to be associated with the alert subscription.
8. (Optional) Add a tag to your alert subscription. For more information about tags, see Tagging AWS resources in the *AWS General Reference guide*.

   a. Enter the key value for the tag.

   b. Choose **Add new tag** to add additional tags. The maximum number of tags that you can add is 50.

9. Choose **Create subscription**.

AWS User Notifications

For information about how to create individual alerts, see Using AWS User Notifications with Cost Anomaly Detection.

Detected anomalies overview

On the **Detected anomalies** tab, you can view a list of all the anomalies detected over a selected time frame. By default, you can see the anomalies that are detected in the last 90 days. You can search the anomalies by **Severity**, **Assessment**, **Services**, **Usage type**, **Region**, **Monitor type**, **Account**, or **Anomaly ID**. You can sort by **Start date**, **Last detected**, **Duration**, **Cost impact**, **Impact %**, **Monitor name**, and **Top root cause (Service)**.

The following default columns are included on the **Detected anomalies** tab:

Start date

The day that the anomaly started.

Last detected

The last time that the anomaly was detected.

Duration

The duration that the anomaly lasted. An anomaly can be ongoing.

Cost impact

The spend increase detected compared to the expected spend amount. It is calculated as **actual spend - expected spend**. For example, a total cost impact of $20 on a service monitor means that there was a $20 increase detected in a particular service with a total duration of the specified days.

Impact %

The percentage difference between the actual spend and expected spend. It is calculated as **(total cost impact / expected spend) * 100**. For example, if the total cost impact was $20 and the expected spend was $60, then the impact percentage would be 33.33%. This value cannot be calculated when expected spend is zero, so in those situations the value will show as “N/A”.

Monitor name

The name of the anomaly monitor.

Top root cause (Service)

The top service root cause for the anomaly. Choosing the service name in the Top root cause column displays the three other root cause dimensions—account, Region, and usage type—for the anomaly's top root cause.

View more

A link to the Anomaly details page with information on the root cause analysis and cost impact of the anomaly. The link also indicates the number of root causes detected for an anomaly.

The **Detected anomalies** tab can also be configured to display additional columns of information. Any changes you make will be saved at the account level for all subsequent visits to the **Detected anomalies** tab. The following **optional columns** are included on the **Detected anomalies** tab.

Account

The account ID and account name that caused the anomaly. If the account is empty, AWS has detected an anomaly, but the root cause is undetermined.

Region

The Region detected as the top root cause for the anomaly.

Usage type

The usage type detected as the top root cause for the anomaly.

Expected spend

The amount our machine learning models expected you to spend during the anomaly's duration, based on your historical spending pattern.

Actual spend

The total amount you actually spent during the anomaly's duration.

Assessment

For each detected anomaly, you can submit an assessment to help improve our anomaly detection systems. The possible values are **Not submitted**, **Not an issue**, or **Accurate anomaly**.

Severity

Represents how abnormal a certain anomaly is accounting for historical spending patterns. A low severity generally suggests a small spike compared to historical spend and a high severity

suggests a big spike. However, a small spike with historically consistent spend is categorized as high severity. And, similarly, a big spike with irregular historical spend is categorized as low severity.

Viewing your detected anomalies and potential root causes

After you create your monitors, AWS Cost Anomaly Detection evaluates your future spend. Based on your defined alert subscriptions, you might start receiving alerts within 24 hours.

To view your anomalies from an email alert

1. Choose the provided **View in Anomaly Detection** link.
2. On the **Anomaly details** page, you can view the root cause analysis and cost impact of the anomaly.
3. (Optional) Choose **View in Cost Explorer** to view a time series graph of the cost impact.
4. (Optional) Choose **View root cause** in the **Top ranked potential root causes** table for a root cause of interest to see a time series graph that's filtered by that root cause.
5. (Optional) Choose **Submit assessment** in the **Did you find this detected anomaly to be helpful?** information alert to provide feedback and help improve our detection accuracy.

To view your anomalies from the AWS Billing and Cost Management console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. (Optional) On the **Detected anomalies** tab, use the search area to narrow the list of detected anomalies for a particular category. The categories that you can choose are Severity, Assessment, Service, Account, Usage type, Region, and Monitor type.
4. (Optional) Choose the **Start date** for a particular anomaly to view the details.
5. On the **Anomaly details** page, you can view the root cause analysis and cost impact of the anomaly.
6. (Optional) Choose **View in Cost Explorer** to view a time series graph of the cost impact and, if necessary, dive deeper into the data.
7. (Optional) Choose **View root cause** in the **Top ranked potential root causes** table to see a time series graph that's filtered by the root cause.

8. (Optional) Choose **Submit assessment** in the **Did you find this detected anomaly to be helpful?** information alert to provide feedback and help improve our detection accuracy.

To view your anomalies from an Amazon SNS topic

1. Subscribe an endpoint to the Amazon SNS topic that you created for a cost monitor with individual alerts. For instructions, see Subscribing to an Amazon SNS topic in the *Amazon Simple Notification Service Developer Guide*.
2. After your endpoint receives messages from the Amazon SNS topic, open a message and then find the **anomalyDetailsLink** URL. The following example is a message from AWS Cost Anomaly Detection through Amazon SNS.

```
{
    "accountId": "123456789012",
    "anomalyDetailsLink": "https://console.aws.amazon.com/cost-management/home#/
anomaly-detection/monitors/abcdef12-1234-4ea0-84cc-918a97d736ef/anomalies/12345678-
abcd-ef12-3456-987654321a12",
    "anomalyEndDate": "2021-05-25T00:00:00Z",
    "anomalyId": "12345678-abcd-ef12-3456-987654321a12",
    "anomalyScore": {
        "currentScore": 0.47,
        "maxScore": 0.47
    },
    "anomalyStartDate": "2021-05-25T00:00:00Z",
    "dimensionKey": {
        "type": "DIMENSION",
        "key": "SERVICE"
    },
    "dimensionalValue": "ServiceName",
    "impact": {
        "maxImpact": 151,
        "totalActualSpend": 1301,
        "totalExpectedSpend": 300,
        "totalImpact": 1001,
        "totalImpactPercentage": 333.67
    },
    "monitorArn": "arn:aws:ce::123456789012:anomalymonitor/
abcdef12-1234-4ea0-84cc-918a97d736ef",
    "rootCauses": [
        {
            "linkedAccount": "AnomalousLinkedAccount",
```

```
            "linkedAccountName": "AnomalousLinkedAccountName",
            "region": "AnomalousRegionName",
            "service": "AnomalousServiceName",
            "usageType": "AnomalousUsageType",
            "impact": {
                "contribution": 601,
            }
        }
    ],
    "subscriptionId": "874c100c-59a6-4abb-a10a-4682cc3f2d69",
    "subscriptionName": "alertSubscription"
}
```


3. Open the **anomalyDetailsLink** URL in a web browser. The URL takes you to the associated **Anomaly details** page. This page shows the root cause analysis and cost impact of the anomaly.

Monitor types

You can choose the monitor type that fits your account structure. AWS Cost Anomaly Detection offers two approaches for creating monitors: AWS managed monitors that automatically track the top 5,000 values independently within a dimension, and customer managed monitors that let you select specific values that get monitored in aggregate.

Monitor Dimension	AWS Managed	Customer Managed
AWS services	Automatically evaluates all AWS services used by your account fo r anomalies. When you start using new AWS services, the monitor au tomatically begins evaluating them. Available in both management and member accounts.	Customer managed AWS services monitors are not supported.
Linked Accounts	Automatically tracks spending patterns across all member accounts in your organization. As new accounts are added, they're au	Track specific member accounts (up to 10) that you manually s elect. Spending is aggregated across selected accounts. Useful for

Monitor Dimension	AWS Managed	Customer Managed
	tomatically included in monitorin g coverage. Only available in management accounts.	monitoring specific project accounts or environments together.
Cost Allocation Tags	Automatically monitors all unique values for a specified tag key. For example, specifying "application-team" tracks every team value (tea m-a, team-b, team-c) independently. New tag values are automatically included as they're created.	Track specific tag values (up to 10) that you manually select for a given tag key. Useful when you need different thresholds for different tag values or want to monitor only high-priority teams.
Cost Categories	Automatically tracks all values within a specified cost category. If you have a "business-unit" category with values like "retail", "wholesal e", and "operations", the monitor analyzes spending patterns for each unit independently. New cost category values are automatically included as they're created.	Track one specific cost category value that you manually select. Us eful for monitoring specific business units or cost centers with unique threshold requirements.

The maximum number of member accounts or tag values you can select for each customer managed monitor is 10.

When to Use Each Monitor Type

Use **AWS managed monitors** when you need:

- Comprehensive coverage across all values in a dimension
- Automatic adaptation as your organization grows
- Minimal maintenance overhead
- Consistent monitoring across all teams/accounts

Use **customer managed monitors** when you need:

- Different alert thresholds for different groups
- To monitor specific subsets of accounts or teams
- To aggregate spending across specific values
- Special monitoring for high-priority or sensitive workloads

Best Practices:

- Use AWS managed monitors for comprehensive coverage across your primary cost organization dimension
- Maintain your AWS services monitor alongside other AWS managed monitors for aggregate service-level visibility
- Use customer managed monitors to supplement AWS managed monitors for specific use cases requiring different thresholds or groupings
- Avoid creating monitors that span multiple dimensions to prevent duplicate alerts

> **Note**
>
> Customer managed monitors were previously called custom monitors. The functionality remains the same, with the name change reflecting the distinction from monitors that AWS manages on your behalf.

For more information about creating your Amazon SNS topic, see Creating an Amazon SNS topic for anomaly notifications.

Transitioning from customer to AWS managed monitors

If you currently use multiple customer managed monitors to track individual accounts, teams, or categories, you can transition to AWS managed monitors for simplified management and automatic coverage.

Transition Process

1. **Create your AWS managed monitor alongside existing customer managed monitors**

- Choose the dimension that matches your primary cost organization method
- The AWS managed monitor will begin tracking all values automatically

2. **Verify detection coverage**
   - Allow the AWS managed monitor to run for at least 24-48 hours
   - Compare detected anomalies with your existing customer managed monitors
   - Ensure the AWS managed monitor is detecting anomalies as expected
3. **Configure alert subscriptions**
   - Set appropriate thresholds for your AWS managed monitor
   - Note that alert subscriptions attached to AWS managed monitors use the same threshold across all tracked values
   - For value-specific routing, configure AWS User Notifications with JSON patterns
4. **Remove redundant customer managed monitors**
   - After confirming complete coverage, delete individual customer managed monitors
   - Keep any customer managed monitors that serve specific purposes (such as grouping related accounts)

Example transition scenario: If you have 50 customer managed monitors tracking individual application teams via cost allocation tags:

1. Create one AWS managed cost allocation tag monitor using your team tag key
2. Verify it detects anomalies across all teams
3. Configure alert subscriptions with appropriate thresholds
4. Delete the 50 individual customer managed monitors

Important notes:

- Direct conversion from customer managed to AWS managed monitors is not supported
- AWS managed monitors may initially generate more anomaly detections due to comprehensive coverage
- Historical anomaly data from customer managed monitors is preserved when you delete them (available via API only; deleted monitors and their anomalies do not appear in the console)
- Consider keeping some customer managed monitors for specific use cases requiring different thresholds

Editing your alert preferences

You can adjust your cost monitors and alert subscriptions in AWS Billing and Cost Management to match your needs.

You can also edit your notification configurations in AWS User Notifications.

> **Note**
>
> When using AWS managed monitors, consider that a single threshold applies to all tracked values. If you need different alert thresholds for different teams or accounts, you can:
>
> - Create supplementary customer managed monitors with dedicated alert subscriptions with specific thresholds
> - Use AWS User Notifications to filter and route alerts based on anomaly attributes
> - Configure Amazon Amazon SNS topics with custom logic for alert routing

Cost monitors

To edit your cost monitors

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Cost monitors** tab.
4. Select the monitor that you want to edit.
5. Choose **Edit**.
   - (Alternative) Choose the individual monitor name.
   - Choose **Edit monitor**.
6. On the **Edit monitor** page, change any settings for **monitor name** and **attached alert subscriptions**.
7. Choose **Manage tags** to add, edit, or remove tags for the monitor.
8. Choose **Save**.

Alert subscriptions

To edit your alert subscriptions

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Alert subscriptions** tab.
4. Select the subscription that you want to edit.
5. Choose **Edit**.
   - (Alternative) Choose the individual monitor name.
   - Choose **Edit**.
6. On the **Edit alert subscription** page, change any settings for **subscription name**, **threshold**, **frequency**, **recipients**, or **cost monitors**.
7. Choose **Manage tags** to add, edit, or remove tags for the monitor.
8. Choose **Save**.

AWS User Notifications

For information about how to edit your notification configurations, see Editing notification configurations in AWS User Notifications in the *AWS User Notifications User Guide*.

Creating an Amazon SNS topic for anomaly notifications

To create an anomaly detection monitor that sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, you must already have Amazon SNS topic or create a new one. You can use Amazon SNS topics to send notifications over Amazon SNS in addition to email. AWS Cost Anomaly Detection must have permissions to send a notification to your topic.

To create an Amazon SNS notification topic and grant permissions

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation pane, choose **Topics**.
3. Choose **Create topic**.

4. For **Name**, enter the name for your notification topic.
5. (Optional) For **Display name**, enter the name that you want displayed when you receive a notification.
6. In **Access policy**, choose **Advanced**.
7. In the policy text field, after **"Statement": [**, enter one of the following statements:

   To allow the AWS Cost Anomaly Detection service to publish to the Amazon SNS topic, use the following statement.

```
{
  "Sid": "E.g., AWSAnomalyDetectionSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "costalerts.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN"
}
```

   To allow the AWS Cost Anomaly Detection service to publish to the Amazon SNS topic only on behalf of a certain account, use the following statement.

```
{
  "Sid": "E.g., AWSAnomalyDetectionSNSPublishingPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "costalerts.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "your topic ARN",
  "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "account-ID"
          ]
        }
  }
}
```

> **Note**
>
> In this topic policy, you enter the subscription's account ID as the value for the `aws:SourceAccount` condition. This condition has AWS Cost Anomaly Detection interact with the Amazon SNS topic only when performing operations for the account that owns the subscription.
> You can restrict AWS Cost Anomaly Detection to interact with the topic only when performing operations on behalf of a specific subscription. To do this, use the `aws:SourceArn` condition in the topic policy.
> For more information about these conditions, see `aws:SourceAccount` and `aws:SourceArn` in the *IAM User Guide*.

8. In the topic policy statement that you select, replace the following values:

   - Replace (for example, *`AWSAnomalyDetectionSNSPublishingPermissions`*) with a string. The `Sid` must be unique within the policy.
   - Replace *`your topic ARN`* with the Amazon SNS topic Amazon Resource Name (ARN).
   - If you're using the statement with the `aws:SourceAccount` condition, replace *`account-ID`* with the account ID that owns the subscription. If the Amazon SNS topic has multiple subscriptions from different accounts, add multiple account IDs to the `aws:SourceAccount` condition.

9. Choose **Create topic**.

   Your topic now appears in the list of topics on the **Topics** page.

Checking or resending notification confirmation email messages

When you create an anomaly detection monitor with notifications, you also create Amazon SNS notifications. For notifications to be sent, you must accept the subscription to the Amazon SNS notification topic.

To confirm that your notification subscriptions are accepted or to resend a subscription confirmation email, use the Amazon SNS console.

To check your notification status or to resend a notification confirmation email message

1. Sign in to the AWS Management Console and open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the navigation pane, choose **Subscriptions**.
3. Check the status of your notification. Under **Status**, `PendingConfirmation` appears if a subscription isn't accepted and confirmed.
4. (Optional) To resend a confirmation request, select the subscription with a pending confirmation and choose **Request confirmation**. Amazon SNS sends a confirmation request to the endpoints that are subscribed to the notification.

   When each owner of an endpoint receives the email, they must choose the **Confirm subscription** link to activate the notification.

Protecting your Amazon SNS anomaly detection alerts data with SSE and AWS KMS

You can use server-side encryption (SSE) to transfer sensitive data in encrypted topics. SSE protects Amazon SNS messages by using keys managed in AWS Key Management Service (AWS KMS).

To manage SSE using AWS Management Console or the AWS SDK, see Enabling Server-Side Encryption (SSE) for an Amazon SNS Topic in the *Amazon Simple Notification Service Getting Started Guide*.

To create encrypted topics using AWS CloudFormation, see the AWS CloudFormation User Guide.

SSE encrypts messages as soon as Amazon SNS receives them. The messages are stored encrypted and are decrypted using Amazon SNS only when they're sent.

Configuring AWS KMS permissions

You must configure your AWS KMS key policies before you can use server-side encryption (SSE). You can use this configuration to encrypt topics, in addition to encrypting and decrypting messages. For information about AWS KMS permissions, see AWS KMS API Permissions: Actions and Resources Reference in the *AWS Key Management Service Developer Guide*.

You can also use IAM policies to manage AWS KMS key permissions. For more information, see Using IAM Policies with AWS KMS.

> **Note**
>
> You can configure global permissions to send and receive message from Amazon SNS. However, AWS KMS requires that you name the full Amazon Resource Name (ARN) of the AWS KMS keys (KMS keys) in the specific AWS Regions. You can find this in the **Resource** section of an IAM policy.
> Ensure that the key policies of the KMS key allow the necessary permissions. To do this, name the principals that produce and consume encrypted messages in Amazon SNS as users in the KMS key policy.

To enable compatibility between AWS Cost Anomaly Detection and encrypted Amazon SNS topics

1. Create a KMS key.
2. Add one of the following policies as the KMS key policy:

   To grant the AWS Cost Anomaly Detection service access to the KMS key, use the following statement.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "costalerts.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

To grant the AWS Cost Anomaly Detection service access to the KMS key only when performing operations on behalf of a certain account, use the following statement.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "costalerts.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "account-ID"
                    ]
                }
            }
        }
    ]
}
```

Note

In this KMS key policy, you enter the subscription's account ID as the value for the `aws:SourceAccount` condition. This condition has AWS Cost Anomaly Detection interact with the KMS key only when performing operations for the account that owns the subscription.

To have AWS Cost Anomaly Detection interact with the KMS key only when performing operations on behalf of a specific subscription, use the `aws:SourceArn` condition in the KMS key policy.

For more information about these conditions, see `aws:SourceAccount` and `aws:SourceArn` in the *IAM User Guide*.

3. If you're using the KMS key policy with the `aws:SourceAccount` condition, replace *`account-ID`* with the account ID that owns the subscription. If the Amazon SNS topic has multiple subscriptions from different accounts, add multiple account IDs to the `aws:SourceAccount` condition.
4. Enable SSE for your Amazon SNS topic.

> **Note**
>
> Make sure that you're using the same KMS key that grants AWS Cost Anomaly Detection the permissions to publish to encrypted Amazon SNS topics.

5. Choose **Save Changes**.

Receiving anomaly alerts in chat applications

You can use Amazon Q Developer to receive your AWS Cost Anomaly Detection alerts in Amazon Chime and Slack.

Amazon Chime

To begin receiving your AWS Cost Anomaly Detection alerts in Amazon Chime

1. Follow Getting started with AWS Cost Anomaly Detection to create a monitor.
2. Create an alert subscription using the `Individual alerts` type. Amazon SNS topics can be configured for `individual alerts` only.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts. To ensure that Cost Anomaly Detection has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for anomaly notifications.
4. Attach the alert subscription to the monitor that you want to receive Amazon Chime alerts for.
5. Open Amazon Chime.
6. For **Amazon Chime**, choose the chat room that you want to set up to receive notifications through Amazon Q Developer.

7. Choose the Room settings icon on the top right and choose **Manage webhooks and bots**.

   Amazon Chime displays the webhooks associated with the chat room.

8. For the webhook, choose **Copy URL**, and then choose **Done**.

   If you need to create a new webhook for the chat room, choose **Add webhook**, enter a name for the webhook in the **Name** field, and then choose **Create**.

9. Open the Amazon Q Developer in chat applications console.
10. Choose **Configure new client**.
11. Choose **Amazon Chime**, and then choose **Configure**.
12. Under **Configuration details**, enter a name for your configuration. The name must be unique across your account and can't be edited later.
13. To configure Amazon Chime webhook, do the following:

    1. For **Webhook URL**, paste the webhook URL that you copied from Amazon Chime.
    2. For **Webhook description**, use the following naming convention to describe the purpose of the webhook: **Chat_room_name/Webhook_name**. This helps you associate Amazon Chime webhooks with their Amazon Q Developer configurations.

14. If you want to enable logging for this configuration, choose **Publish logs to Amazon CloudWatch Logs**. For more information, see Amazon CloudWatch Logs for Amazon Q Developer.

    > **Note**
    >
    > There is an additional charge for using Amazon CloudWatch Logs.

15. For **Permissions**, set the IAM permissions as follows:

    1. For **IAM role**, choose **Create an IAM role using a template**. If you want to use an existing role instead, choose it from the **IAM role** list. To use an existing IAM role, you might need to modify it for use with Amazon Q Developer. For more information, see Configuring an IAM Role for Amazon Q Developer.
    2. For **Role name**, enter a name. Valid characters: a-z, A-Z, 0-9.
    3. For **Policy templates**, choose **Notification permissions**. This is the IAM policy provided by Amazon Q Developer. It provides the necessary Read and List permissions for CloudWatch alarms, events, and logs, and for Amazon Amazon SNS topics.

16. Set up the Amazon SNS topics that will send notifications to the Amazon Chime webhook.

    1. For **Amazon SNS Region**, choose the AWS Region that hosts the Amazon SNS topics for this Amazon Q Developer subscription.
    2. For **Amazon SNS topics**, choose the Amazon SNS topic for the client subscription. This topic determines the content that's sent to the Amazon Chime webhook. If the region has additional Amazon SNS topics, you can choose them from the same dropdown list.
    3. If you want to add an Amazon SNS topic from another Region to the notification subscription, choose **Add another Region**.
17. Choose **Configure**.

For any additional details, see Tutorial: Get started with Amazon Chime in the *Amazon Q Developer in chat applications Administrator Guide*.

Slack

To begin receiving your AWS Cost Anomaly Detection alerts in Slack

1. Follow Getting started with AWS Cost Anomaly Detection to create a monitor.
2. Create an alert subscription using the `Individual alerts` type. Amazon SNS topics can be configured for `individual alerts` only.
3. Add an Amazon SNS topic as an alert recipient to a specific alert or alerts. To ensure that Cost Anomaly Detection has permissions to publish to your Amazon SNS topics, see Creating an Amazon SNS topic for anomaly notifications.
4. Attach the alert subscription to the monitor that you want to receive Slack alerts for.
5. Add Amazon Q Developer to the Slack workspace.
6. Open the Amazon Q Developer in chat applications console.
7. Choose **Configure new client**.
8. Choose **Slack**, and then choose **Configure**.
9. From the dropdown list at the top right, choose the Slack workspace that you want to use with Amazon Q Developer.
10. Choose **Allow**.

For any additional details, see Tutorial: Get started with Slack in the *Amazon Q Developer in chat applications Administrator Guide*.

Using EventBridge with Cost Anomaly Detection

AWS Cost Anomaly Detection is integrated with EventBridge, an event bus service that you can use to connect your applications with data from a variety of sources. For more information, see the Amazon EventBridge User Guide.

You can use EventBridge to detect and react to Cost Anomaly Detection events. Then, based on rules that you create, EventBridge invokes one or more target actions when an event matches the values that you specify in a rule. Depending on the type of event, you can capture event information, initiate additional events, send notifications, take corrective action, or perform other actions. To set up an EventBridge rule for Cost Anomaly Detection events, see Create a rule in Amazon EventBridge in the *Amazon EventBridge User Guide*.

Example: EventBridge event for Cost Anomaly Detection

When an immediate alert is detected, the subscriber receives an event with the `Anomaly Detected` detail type. The following example shows the event body for the detail type:

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "source": "aws.ce",
    "detail-type": "Anomaly Detected",
    "account": "<account ID>", // 12 digit account id.
    "region": "<region>", // Cost Anomaly Detection home region.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "resources": [
         "arn:aws:ce::123456789012:anomalymonitor/abcdef12-1234-4ea0-84cc-918a97d736ef"
    ],
    "detail": {
         "accountName": "<account name>",
         "anomalyEndDate": "2021-05-25T00:00:00Z",
         "anomalyId": "12345678-abcd-ef12-3456-987654321a12",
         "anomalyScore": {
            "currentScore": 0.47,
            "maxScore": 0.47
         },
         "anomalyStartDate": "2021-05-25T00:00:00Z",
         "dimensionValue": "<dimension value>", // service name for AWS Service Monitor
         "feedback": "string",
         "impact": {
```

```
            "maxImpact": 151,
            "totalActualSpend": 1301,
            "totalExpectedSpend": 300,
            "totalImpact": 1001,
            "totalImpactPercentage": 333.67
         },
         "rootCauses": [
            {
                "linkedAccount": "<linked account ID>", // 12 digit account id.
                "linkedAccountName": "<linked account name>",
                "region": "<region>",
                "service": "<service name>", // AWS service name
                "usageType": "<usage type>", // AWS service usage type
                "impact": {
                    "contribution": 601,
                }
            }
        ],
        "accountId": "<account ID>", // 12 digit account id.
        "monitorArn": "arn:aws:ce::123456789012:anomalymonitor/
abcdef12-1234-4ea0-84cc-918a97d736ef",
        "monitorName": "<your monitor name>",
        "anomalyDetailsLink": "https://console.aws.amazon.com/cost-management/home#/
anomaly-detection/monitors/abcdef12-1234-4ea0-84cc-918a97d736ef/anomalies/12345678-
abcd-ef12-3456-987654321a12"
    }
}
```

Using AWS User Notifications with Cost Anomaly Detection

You can use AWS User Notifications to set up delivery channels that notify you about Cost Anomaly Detection events. You will receive a notification when an event matches a specified rule. You can receive notifications for events through multiple channels, including email, Amazon Q Developer in chat applications such as Amazon Chime, Microsoft Teams, and Slack, or AWS Console Mobile Application push notifications. You can also see notifications using the Console Notifications Center in the AWS User Notifications console.

AWS User Notifications also supports aggregation, which can reduce the number of notifications you receive during specific events. For more information, see the AWS User Notifications User Guide.

To use AWS User Notifications, you must have the correct AWS Identity and Access Management (IAM) permissions. For more information about configuring your IAM permissions, see Creating a notification configuration in the *AWS User Notifications User Guide*.

Example: EventBridge event for `Anomaly Detected`

The following is a generalized example event for `Anomaly Detected`. You can subscribe to EventBridge events (such as this one) using AWS User Notifications.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "source": "aws.ce",
    "detail-type": "Anomaly Detected",
    "account": "<account ID>", // 12 digit account id.
    "region": "<region>", // Cost Anomaly Detection home region.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "resources": [
         "arn:aws:ce::123456789012:anomalymonitor/abcdef12-1234-4ea0-84cc-918a97d736ef"
    ],
    "detail": {
         "accountName": "<account name>",
         "anomalyEndDate": "2021-05-25T00:00:00Z",
         "anomalyId": "12345678-abcd-ef12-3456-987654321a12",
         "anomalyScore": {
            "currentScore": 0.47,
            "maxScore": 0.47
         },
         "anomalyStartDate": "2021-05-25T00:00:00Z",
         "dimensionValue": "<dimension value>", // service name for AWS Service Monitor
         "feedback": "string",
         "impact": {
            "maxImpact": 151,
            "totalActualSpend": 1301,
            "totalExpectedSpend": 300,
            "totalImpact": 1001,
            "totalImpactPercentage": 333.67
         },
         "rootCauses": [
            {
                "linkedAccount": "<linked account ID>", // 12 digit account id.
                "linkedAccountName": "<linked account name>",
                "region": "<region>",
```

```
                "service": "<service name>", // AWS service name
                "usageType": "<usage type>", // AWS service usage type
                "impact": {
                    "contribution": 601,
                }
            }
        ],
        "accountId": "<account ID>", // 12 digit account id.
        "monitorArn": "arn:aws:ce::123456789012:anomalymonitor/
abcdef12-1234-4ea0-84cc-918a97d736ef",
        "monitorName": "<your monitor name>",
        "anomalyDetailsLink": "https://console.aws.amazon.com/cost-management/home#/
anomaly-detection/monitors/abcdef12-1234-4ea0-84cc-918a97d736ef/anomalies/12345678-
abcd-ef12-3456-987654321a12"
    }
}
```

Filtering events

You can filter events either by service and name using the filters available in the AWS User Notifications console, or by specific properties if you create your own EventBridge filter from JSON code.

Topics

- Example: Filter by impact
- Example: Filter by service dimension
- Example: Filter by cost allocation tag
- Example: Filter by Region root cause
- Example: Filter by multiple criteria

Example: Filter by impact

The following filter captures any anomaly with a total impact greater than $100 and a percentage impact greater than 10%.

```
{
    "detail": {
        "impact": {
            "totalImpact": [{
                "numeric": [">", 100]
```

```
            }],
            "totalImpactPercentage": [{
                "numeric": [">", 10]
            }]
        }
    }
}
```

Example: Filter by service dimension

The following filter captures anomalies specific to the EC2 service, detected by the AWS services monitor.

```
{
    "detail": {
        "dimensionValue": ["Amazon Elastic Compute Cloud - Compute"],
        "monitorName": ["aws-services-monitor"]
    }
}
```

Example: Filter by cost allocation tag

The following filter captures anomalies for the Frontend application team, detected by a dimensional cost allocation tag monitor.

```
{
  "detail": {
    "dimensionValue": ["ApplicationTeam:Frontend"],
    "monitorName": ["dimensional-CAT-monitor"]
  }
}
```

Example: Filter by Region root cause

The following filter captures anomalies that have root causes in the US East (N. Virginia) Region.

```
{
  "detail": {
    "rootCauses": {
      "region": ["us-east-1"]
    }
```

```
  }
}
```

Example: Filter by multiple criteria

The following complex filter captures anomalies for the Frontend application team with a total impact greater than $100, a percentage impact greater than 10%, and root causes in the US East (N. Virginia) Region.

```
{
  "detail": {
    "dimensionValue": ["ApplicationTeam:Frontend"],
    "monitorName": ["dimensional-CAT-monitor"],
    "impact": {
        "totalImpact": [{ "numeric": [">", 100] }],
        "totalImpactPercentage": [{ "numeric": [">", 10] }]
    },
    "rootCauses": {
        "region": ["us-east-1"]
    }
  }
}
```

Opting out of Cost Anomaly Detection

You can opt out of Cost Anomaly Detection at any time. To opt out, you need to delete all cost monitors and alert subscriptions in your account. After you opt out, Cost Anomaly Detection no longer monitors your spend patterns for anomalies. You also won't receive any further notifications.

To opt out of Cost Anomaly Detection

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. To delete any existing cost monitors:
    a. Choose the **Cost monitors** tab.
    b. Select the cost monitor that you want to delete.
    c. Choose **Delete**.

d. In the **Delete cost monitor** dialog box, choose **Delete**.

e. Repeat the steps for any additional cost monitors.

4. To delete any existing alert subscriptions:

a. Choose the **Alert subscriptions** tab.

b. Select the alert subscription that you want to delete.

c. Choose **Delete**.

d. In the **Delete alert subscription** dialog box, choose **Delete**.

e. Repeat the steps for any additional alert subscriptions.

> **Note**
>
> You can also opt out of Cost Anomaly Detection by deleting your cost monitors and alert subscriptions in the Cost Explorer API. To do so, you need to use DeleteAnomalyMonitor and DeleteAnomalySubscription.

Investigating anomaly root causes with Amazon Q Developer

You can use Amazon Q Developer to investigate the root cause of a detected cost anomaly. When you investigate an anomaly, Amazon Q Developer analyzes your cost data and CloudTrail events to identify what changed, when, where, who triggered the change, and why it happened.

Cost investigation is available at no additional charge for customers using AWS Cost Anomaly Detection. Investigation might incur standard charges for the underlying services it uses on your behalf, such as CloudWatch Logs Insights queries on your CloudTrail data. For details, see CloudWatch Logs pricing.

Topics

- How cost investigation works
- Prerequisites
- Investigating an anomaly
- Understanding investigation results
- Continuing the investigation
- Cross-account investigation

- Limitations

How cost investigation works

When you investigate an anomaly, Amazon Q Developer performs the following analysis:

1. **Identifies what changed** in your cost data by breaking the anomaly down into its largest contributing dimensions (service, account, region, usage type).
2. **Determines whether the change is usage-driven or rate-driven.** A usage-driven change means more resources or activity at the same per-unit price (for example, a new deployment scaling up). A rate-driven change means similar usage at a different per-unit price (for example, a Savings Plans reallocation or a tiered pricing reset).
3. **For usage-driven changes, correlates with CloudTrail** to attribute the cost change to specific API calls and the IAM principals that made them.
4. **For rate-driven changes, attempts to explain the cost composition** by identifying what shifted in pricing or applied discounts.

The investigation output adapts to the anomaly. A simple anomaly with one root cause produces a concise narrative. A complex anomaly with multiple independent causes produces a per-cause breakdown with a synthesis.

Prerequisites

To use cost investigation, you need the following:

- **Amazon Q Developer access.** Users must have Amazon Q Developer permissions (`q:StartConversation`, `q:SendMessage`) and the `q:PassRequest` permission. The quickest way to grant access is to use the `AmazonQFullAccess` managed policy. For detailed permission configurations, see Security for cost management capabilities in Amazon Q Developer.
- **(Recommended) An organization-wide CloudTrail trail with management events logging enabled and CloudWatch Logs delivery.** For cross-account investigation, the capability discovers your organization trail automatically and queries CloudWatch Logs Insights to find events across all member accounts. If no organization trail is configured, the investigation completes with the cost data available and tells you what to enable for a fuller answer. For information about creating an organization trail, see Creating a trail for an organization in the *AWS CloudTrail User Guide*.

Investigating an anomaly

You can start an investigation from the following locations: the Cost Anomaly Detection console or an Amazon Q Developer conversation.

From the Cost Anomaly Detection console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Anomaly Detection**.
3. Choose the **Detected anomalies** tab.
4. Select an anomaly to view its details.
5. Choose **Investigate with Amazon Q Developer**.

Amazon Q Developer opens and begins the investigation automatically. Results typically appear within minutes.

From an Amazon Q Developer conversation

When you ask Amazon Q Developer a question about your AWS costs that is best answered by an investigation, Amazon Q Developer might invoke the investigation capability automatically as part of the conversation.

Understanding investigation results

Investigation results might include the following dimensions of a cost change, depending on the data available:

- **What changed.** The contributing service, account, region, and usage type. The investigation identifies the largest cost drivers, not just the top-level service total.
- **When.** The timeline of events leading up to the anomaly, anchored to the day the cost change started and the deployment or configuration events that preceded it.
- **Where.** The accounts and regions involved. For organizations with multiple linked accounts, the investigation identifies the specific account where the change originated.
- **Who.** The IAM principal that triggered the API call, whether that was a user, a role, or an automated process.

- **Why.** A plain-language explanation that ties the above together. For example: "An AWS Lambda function in account 111122223333 increased its invocation rate starting May 15 after a deployment by IAM role `deploy-prod`, driving a cost increase in us-east-1."

When a definitive root cause cannot be identified

Not every cost change maps to a single API call. Pricing-only changes (such as Savings Plans reallocations or tiered pricing resets) and demand-driven scaling can produce anomalies without a corresponding CloudTrail event. When the investigation cannot identify a definitive root cause, it surfaces what it did find and tells you what additional context would help. It does not fabricate an explanation.

Continuing the investigation

After the initial analysis, you can ask follow-up questions in the same Amazon Q Developer conversation to drill deeper or change direction. For example:

- "Break down the cost increase by service and region."
- "Is the cost concentrated in a single account or spread across the organization?"
- "How does this anomaly compare to recent cost changes in this account?"

Amazon Q Developer maintains the conversation context, so each follow-up builds on the prior analysis.

Cross-account investigation

Cost Anomaly Detection monitors that are created in the management (payer) account detect anomalies from spending across the organization. When you investigate an anomaly, the root cause often originates in a linked account within your organization. Cost Explorer aggregates billing data at the payer level, but CloudTrail event data is scoped to the account where the API call was made.

To bridge this gap, the investigation capability automatically discovers your organization-wide CloudTrail trail and queries the CloudWatch Logs location where the trail's events are stored. No configuration is required inside Cost Anomaly Detection or the investigation capability itself. Once the trail exists, the capability discovers and uses it automatically.

If your organization does not have an organization-wide trail with CloudWatch Logs delivery configured, the investigation completes with the data available in the payer account and tells you what to enable for cross-account attribution.

> **Note**
>
> When investigating anomalies using an organization trail delivered to CloudWatch Logs, the capability queries CloudWatch Logs Insights on your behalf, which incurs standard CloudWatch Logs Insights charges based on data scanned. For details, see Analyzing log data with CloudWatch Logs Insights.

Limitations

- The investigation can identify which user or role triggered cost changes that come from configuration changes (such as launching an EC2 instance, deploying a Lambda function, or creating an S3 bucket). It cannot identify which user or role triggered cost changes that come from data operations (such as Amazon S3 `GetObject` calls or Amazon DynamoDB `GetItem` calls) because CloudTrail does not capture those operations by default.
- CloudTrail event availability depends on your trail's retention configuration. Older anomalies might have limited or no CloudTrail attribution if events have aged out.
- Resource-level cost data from Cost Explorer is available only for the last 14 days. For older anomalies, the investigation uses service-level and account-level data.
- Anomaly data archives after 90 days. Investigations of archived anomalies might have limited data available.

Identifying opportunities with Cost Optimization Hub

Cost Optimization Hub is an AWS Billing and Cost Management feature that helps you consolidate and prioritize cost optimization recommendations across your AWS accounts and AWS Regions, so that you can get the most out of your AWS spend.

You can use Cost Optimization Hub to identify, filter, and aggregate AWS cost optimization recommendations across your AWS accounts and AWS Regions. It makes recommendations on resource rightsizing, idle resource deletion, Savings Plans, and Reserved Instances. With a single dashboard, you avoid having to go to multiple AWS products to identify cost optimization opportunities.

Cost Optimization Hub helps you quantify and aggregate estimated savings when you implement cost optimization recommendations. Cost Optimization Hub accounts for your specific commercial terms with AWS, such as Reserved Instances and Savings Plans, so you can easily compare and prioritize recommendations. It helps you measure cost efficiency to establish consistent cost savings benchmarks, set performance goals, and track progress to maximize your return on cloud investments.

After you enable Cost Optimization Hub, you can see estimated monthly savings in AWS Compute Optimizer, consistent with the savings estimates in Cost Optimization Hub.

Cost Optimization Hub provides the following main benefits:

- Automatically identify and consolidate your AWS cost optimization opportunities.
- Quantify estimated savings that incorporate your AWS pricing and discounts.
- Aggregate and deduplicate savings across related cost optimization opportunities.
- Prioritize your cost optimization recommendations with filtering, sorting, and grouping.
- Establish consistent cost savings benchmarks, set performance goals, and track progress to maximize your return on cloud investments.

Cost Optimization Hub provides you with a console experience and a set of API operations that you can use to measure and track cost efficiency and view the findings of the analysis and recommendations for your resources across multiple AWS Regions. You can also view findings and recommendations across multiple accounts within your organization when you opt in the management account of an organization. The findings from the feature are also reported in the consoles of the supported services, such as the Amazon EC2 console.

Topics

- Getting started with Cost Optimization Hub
- Customizing your Cost Optimization Hub preferences
- Viewing your cost optimization opportunities
- Understanding your cost efficiency metric
- Prioritizing your cost optimization opportunities
- Understanding cost optimization strategies
- Viewing your savings opportunities
- Estimating monthly savings

- Supported resources

Getting started with Cost Optimization Hub

The overviews in this section describe how to get started with Cost Optimization Hub in AWS Billing and Cost Management.

When you access Cost Optimization Hub for the first time, you're asked to opt in using the account that you're signed in with. Before you can use the feature, you must opt in. In addition, you can also opt in using the Cost Optimization Hub API, AWS Command Line Interface (AWS CLI), or SDKs.

By opting in, you authorize Cost Optimization Hub to import cost optimization recommendations generated by multiple AWS services in your account and all member accounts of your organization. These include rightsizing recommendations from AWS Compute Optimizer and Savings Plans recommendations from AWS Billing and Cost Management. These recommendations are saved in the US East (N. Virginia) Region.

In the future, AWS may expand the types of cost optimization recommendations that Cost Optimization Hub imports. AWS may also export recommendations from Cost Optimization Hub to other integrated AWS services.

Accounts supported by Cost Optimization Hub

The following AWS account types can opt in to Cost Optimization Hub:

- **Standalone AWS account**

  A standalone AWS account that doesn't have AWS Organizations enabled. For example, if you opt in to Cost Optimization Hub while signed in to a standalone account, Cost Optimization Hub identifies cost optimization opportunities and consolidates recommendations.
- **Member account of an organization**

  An AWS account that's a member of an organization. If you opt in to Cost Optimization Hub while signed in to a member account of an organization, Cost Optimization Hub identifies cost optimization opportunities and consolidates recommendations.
- **Management account of an organization**

  An AWS account that administers an organization. If you opt in to Cost Optimization Hub while signed in to a management account of an organization, Cost Optimization Hub gives you the

option to opt in the management account only, or the management account and all member accounts of the organization.

The management account can register a member account as a delegated administrator for Cost Optimization Hub. This enables the delegated administrator to see all recommendations on the management account's behalf. There can only be one delegated administrator per organization. For more information, see Delegate an administrator account.

Important

To opt in all member accounts for an organization, make sure that the organization has all features enabled. For more information, see Enabling All Features in Your Organization in the *AWS Organizations User Guide*.
When you opt in using your organization's management account and include all member accounts within the organization, trusted access for Cost Optimization Hub is enabled in your organization account. For more information, see Cost Optimization Hub and AWS Organizations trusted access.

Policy to opt in to Cost Optimization Hub

To opt in to Cost Optimization Hub, you need specific permissions. The required permissions differ depending on whether you're enabling it for a single account or for all accounts in your organization.

Both policies grant permission to create the necessary service-linked role and update the Cost Optimization Hub enrollment status. For more information on service-linked roles, see Service-linked roles for Cost Optimization Hub.

If enabling Cost Optimization Hub for all accounts, the management account also needs to set up AWS Organizations trusted access. For details, see Cost Optimization Hub and AWS Organizations trusted access.

The following are two policy statements. Choose the appropriate one based on your needs:

Policy for opting in all accounts in your organization

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-
optimization-hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
            "Condition": {"StringLike": {"iam:AWSServiceName": "cost-
optimization-hub.bcm.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-
optimization-hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "cost-optimization-hub.bcm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "cost-optimization-hub:UpdateEnrollmentStatus",
            "Resource": "*"
       }
    ]
}
```

Policy for opting in a single account

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
            "Condition": {"StringLike": {"iam:AWSServiceName": "cost-
optimization-hub.bcm.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
        },
        {
            "Effect": "Allow",
            "Action": "cost-optimization-hub:UpdateEnrollmentStatus",
            "Resource": "*"
       }
    ]
}
```

There are two AWS managed policies to help get you started with Cost Optimization Hub actions. One policy provides you with read-only access to Cost Optimization Hub, and the other policy provides you with admin access. For full details, see Managed policies.

Enabling Cost Optimization Hub

To access Cost Optimization Hub, you must first enable the feature.

To enable Cost Optimization Hub

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.

3. On the **Cost Optimization Hub** page, choose your relevant organization and member account settings:
   - **Enable Cost Optimization Hub for this account and all member accounts**: Recommendations in this account and all member accounts will be imported into Cost Optimization Hub.
   - **Enable Cost Optimization Hub for this account only**: Only recommendations in this account will be imported into Cost Optimization Hub.
4. Choose **Enable**.

You can also enable Cost Optimization Hub through the **Cost Management preferences** in the console, or you can use the AWS CLI or AWS SDK.

After you enable Cost Optimization Hub, AWS starts to import cost optimization recommendations from various AWS products, such as AWS Compute Optimizer. It can take as long as 24 hours for Cost Optimization Hub to import recommendations for all supported AWS resources.

Opting in to Compute Optimizer

For Cost Optimization Hub to import recommendations from AWS Compute Optimizer, you need to opt in to Compute Optimizer. Compute Optimizer supports standalone AWS accounts, member accounts of an organization, and the management account of an organization. For more information, see Getting started with AWS Compute Optimizer.

Accessing the console

When your setup is complete, access Cost Optimization Hub.

To access Cost Optimization Hub

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.

Opting out of Cost Optimization Hub

You can opt out of Cost Optimization Hub at any time. However, the organization account can't opt out for all member accounts. Each member needs to opt out at account level.

To opt out of Cost Optimization Hub

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management Preferences**.
3. In **Preferences**, choose **Cost Optimization Hub**.
4. On the **Cost Optimization Hub** tab, clear **Enable Cost Optimization Hub**.
5. Choose **Save preferences**.

Topics

- Cost Optimization Hub and AWS Organizations trusted access
- Delegating an administrator account

Cost Optimization Hub and AWS Organizations trusted access

When you opt in using your organization's management account and include all member accounts within the organization, trusted access for Cost Optimization Hub is automatically enabled in your organization account. Every time that you access recommendations for member accounts, Cost Optimization Hub verifies that trusted access is enabled in your organization account. If you disable Cost Optimization Hub trusted access after you opt in, Cost Optimization Hub denies access to recommendations for your organization's member accounts. Moreover, the member accounts within the organization aren't opted in to Cost Optimization Hub. To re-enable trusted access, opt in to Cost Optimization Hub again using your organization's management account and include all the member accounts within the organization. For more information, see Opting in your account. For more information about AWS Organizations trusted access, see Using AWS Organizations with other AWS services in the *AWS Organizations User Guide*.

Management account policy

This policy provides all the permissions necessary for a management account to opt in to Cost Optimization Hub and have full access to the service.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "cost-optimization-
hub.bcm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowAWSServiceAccessForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "cost-optimization-hub.bcm.amazonaws.com"
```

```
                    ]
                }
            }
        }
    ]
}
```

Member account policy

This policy provides the permissions necessary for a member account to have full access to Cost Optimization Hub.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries"
            ],
            "Resource": "*"
        }
    ]
}
```

Delegating an administrator account

You can delegate a member account in your organization as an administrator for Cost Optimization Hub. Delegating an administrator removes the need for you to use the management account to access and manage Cost Optimization Hub on behalf of the organization. This also enables you to

adopt an AWS security best-practice, which recommends that you delegate responsibilities outside of the management account where possible.

A delegated administrator can perform most Cost Optimization Hub actions, including getting recommendations and setting preferences, without the need to access the management account. However, the delegated administrator cannot change the opt-in status of the management account.

The management account controls the delegated administrator option for its organization. Each organization can only have one delegated administrator for Cost Optimization Hub at a time.

To register or update an account as a delegated administrator:

Console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. In the **Preferences** page, choose the **Cost Optimization Hub** tab.
4. Under **Organization and member account settings**, select **Delegated administrator**.
5. Choose the account ID that you want to add as the delegated administrator.
6. Choose **Save preferences**.

CLI

1. Log in as the management account of your organization.
2. Open a terminal or command prompt window.
3. Call the following API operation. Replace `123456789012` with your account ID.

```
aws organizations register-delegated-administrator \
                  --account-id 123456789012 \
                  --service-principal cost-optimization-hub.bcm.amazonaws.com
```

To remove a member account as a delegated administrator:

Console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. In the **Preferences** page, choose the **Cost Optimization Hub** tab.
4. Under **Organization and member account settings**, clear **Delegated administrator**.
5. Choose **Save preferences**.

CLI

1. Log in as the management account of your organization.
2. Open a terminal or command prompt window.
3. Call the following API operation. Replace `123456789012` with your account ID.

```
aws organizations deregister-delegated-administrator \
                  --account-id 123456789012 \
                  --service-principal cost-optimization-hub.bcm.amazonaws.com
```

Customizing your Cost Optimization Hub preferences

In **Cost Management preferences**, you can customize various Cost Optimization Hub settings, including how savings are estimated and your commitment preferences.

Savings estimation mode preferences

You can customize how your estimated monthly savings are calculated. Savings estimation mode supports the following two options:

- **After discounts**: Cost Optimization Hub estimates savings incorporating all discounts with AWS, such as Reserved Instances and Savings Plans.
- **Before discounts**: Cost Optimization Hub estimates savings by using AWS public (On-Demand) pricing, without incorporating any discounts.

> **Important**
>
> When you use billing transfer as a bill source account, the `after discounts` functionality is disabled and you can't enable it. Bill source accounts must validate rightsizing recommendations against their Reserved Instance and Savings Plans inventory to consider any unused commitment before making optimization decisions.

To customize how estimated monthly savings are calculated

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. On the **Preferences page**, choose the **Cost Optimization Hub** tab.
4. Under **Savings estimation mode**, choose **After discounts** or **Before discounts**.
5. Choose **Save preferences**.

Commitment preferences

You can customize your preferred term length and payment option for reservations and Savings Plans, which populates the overall estimated savings in the Cost Optimization Hub dashboard. For example, if you prefer 1-year no upfront commitments, configure these preferences and Cost Optimization Hub will reflect them in the dashboard within 24 hours. The resulting estimated monthly savings reflect the savings you can achieve with your preferred commitment term length and payment option.

To customize your preferred term length and payment option:

Console

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. On the **Preferences** page, choose the **Cost Optimization Hub** tab.
4. For **Term length**, choose between **Highest overall savings**, **1-year term**, or **3-year term**.

5. For **Payment option**, choose between **Highest overall savings**, **No upfront**, **Partial upfront**, or **All upfront**.
6. Choose **Save preferences**.

> **Note**
>
> If your preferred commitment type isn't available, such as for specific Regions or instance types, Cost Optimization Hub automatically recommends Savings Plans or reservations with the highest overall savings.

CLI

1. Log in to your account.
2. Open a terminal or command prompt window.
3. Use the `UpdatePreferences` API operation to update your preferred term and payment option:

```
aws cost-optimization-hub update-preferences
                  --preferred-commitment '{"term":"OneYear", "paymentOption":
 "NoUpfront"}'
```

You can change either the term or payment option, but both fields must be included in the request. For example, to change only the term to `ThreeYear` while maintaining your current payment option:

```
aws cost-optimization-hub update-preferences
                  --preferred-commitment '{"term":"ThreeYear", "paymentOption":
 "NoUpfront"}'
```

To use the default 3-year term (highest savings), either omit the term field or set it to null:

```
aws cost-optimization-hub update-preferences
                  --preferred-commitment '{"paymentOption": "NoUpfront"}'
```

To use the default for both fields (highest savings), use an empty object:

```
aws cost-optimization-hub update-preferences
                  --preferred-commitment '{}'
```

Viewing your cost optimization opportunities

Cost optimization findings for your resources are displayed on the Cost Optimization Hub dashboard. You can use this dashboard to filter cost optimization opportunities and aggregate estimated savings. You can compare your total savings opportunities against your previous month's AWS spend. These estimated savings reflect your preferred commitment preferences for reservations and Savings Plans. To customize these preferences, see Customizing your Cost Optimization Hub preferences.

Use the dashboard to group your savings opportunities by AWS account, Region, resource types, and tags. View the distribution of savings opportunities, explore recommended actions, and identify areas with the highest potential savings. The dashboard refreshes daily, reflecting your usage up to the previous day. For example, if today is December 2, the data includes your usage through December 1.

You can use the summary chart to filter recommendations.

Explore and narrow down the categories and recommended actions for cost optimization. To identify resources and specific actions per resource, choose **View opportunities** to go to the list of resources available for optimization. You can choose a particular recommendation, view its details, and deep link to the relevant pages in the AWS Billing and Cost Management console and AWS Compute Optimizer. For deeper analysis of any recommendation, select it and choose **Analyze with Amazon Q**.

At the bottom of the dashboard, you can see your total estimated savings as a percentage of your previous month's net amortized cost. This way, you can benchmark your cost efficiency.

Topics

- Viewing the dashboard

Viewing the dashboard

Use the following procedure to view the dashboard and your cost optimization opportunities.

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.

   By default, the dashboard displays an overview of cost optimization opportunities for AWS resources across all AWS Regions in the account that you're currently signed in to.
3. You can perform the following actions on the dashboard:

   - To view the cost optimization findings for a particular AWS Region in the account, choose the Region in the chart.
   - To view the cost optimization findings for resources in a particular account, under **Aggregate estimated savings by**, choose **AWS account**, and then choose an account ID in the chart.

     > **Note**
     >
     > Viewing cost optimization opportunities for resources in other accounts is available only if you're signed in to a management account of an organization, and you have opted in all member accounts of the organization.

   - To view cost optimization findings by resource type, under **Aggregate estimated savings by**, choose **Resource type**.
   - To view recommended actions, under **Aggregate estimated savings by**, choose **Recommended action**.
   - To filter findings on the dashboard, under **Filter**, choose from the filter options.
   - To go to the list of resources available for optimization, choose **View opportunities**.

Switching the dashboard view

The Cost Optimization Hub dashboard provides you two styles for viewing your cost optimization opportunities:

- Chart view
- Table view

You can set the style by choosing one of the views on the top right corner of the chart or table.

Understanding your cost efficiency metric

Cost efficiency is a metric that measures how effectively you're optimizing your AWS cloud resources. It is automatically generated everyday by considering resource optimization, resource utilization, and commitment savings and is applicable across multiple scopes—from individual regions to entire organizations.

It provides a simple, yet comprehensive measure of your cloud spend efficiency using the following formula:

Cost efficiency = 1 - (Potential Savings / Total Optimizable Spend) × 100%

For example, if your total monthly AWS spend that can be optimized is $100,000 and Cost Optimization Hub identifies $10,000 in potential savings, your cost efficiency is 90%.

You can track your cost efficiency over-time across your organization to understand and benchmark your cost efficiency. With daily refreshes, the metric provides insights into optimization progress, showing score improvements when you implement cost-saving recommendations, and score decreases when inefficient resources are provisioned.

The cost efficiency metric is based on a rolling 30-day spend and today's savings opportunity. For example, the metric on November 30 will use the optimizable spend from October 31st to November 29th and the potential savings on November 30th.

Potential Savings

Potential savings represent deduplicated, estimated total cost reductions you could achieve by implementing recommended actions across your AWS environment. These actions may include rightsizing resources, selecting optimal instance types, removing idle resources, and utilizing commitment-based pricing models such as Reserved Instances and Savings Plans.

Cost Optimization Hub prevents duplicate savings calculations by filtering and ranking overlapping opportunities to eliminate redundant savings and highlight those with the highest savings potential. For example, stopping an idle EC2 instance reduces the amount you can save through purchasing Savings Plans. Cost Optimization Hub proportionally reduces the estimated savings for Savings Plans recommendations based on the costs of idle EC2 instances that can be stopped.

Total Optimizable Spend

Total Optimizable Spend represents your AWS spending on services where Cost Optimization Hub provides recommendations such as Amazon EC2 instances, Amazon RDS databases, and Amazon

OpenSearch. It uses your **Net amortized costs** after removing any credits and refunds you might have. For more information, see Your net amortized costs.

> **Note**
>
> For supported services, the entire service spend is included in Total Optimizable Spend.

Supported Services

Optimizable spend in the cost efficiency metric is all spend under these included services:

- Amazon Elastic Compute Cloud (EC2) instances
- Amazon Elastic Container Service (ECS)
- Amazon Elastic Kubernetes Service (EKS)
- Amazon Elastic Block Store (EBS) volumes
- Amazon RDS databases
- Amazon SageMaker
- Amazon Redshift
- AWS Lambda functions
- OpenSearch
- MemoryDB
- DynamoDB
- ElastiCache

For a list of supported resources for these services, see Supported resources

Viewing your Cost Efficiency

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.
3. Your current Cost efficiency appears at the top of the page.
4. By default, you will see the **Overall** scores for your account on the Cost efficiency card on the right. You can perform the following actions on this card:

- To view the 5 most efficient accounts, under “View efficiency by”, choose **Most efficient accounts**
- To view the 5 least efficient accounts, under “View efficiency by”, choose **Least efficient accounts**
- To view the 5 most efficient regions, under “View efficiency by”, choose **Most efficient regions**

To view cost efficiency across all your accounts and regions, use the table view under **Optimization details** . You can search for specific accounts or Regions, and sort by cost efficiency by clicking the column header.

You can also sort the table by **Potential savings** or **Total optimizable spend** by clicking the column header. This helps you identify the accounts or Regions with the largest savings opportunity or the highest optimizable spend.

Frequently Asked Questions

1. **Why am I not able to view the cost efficiency?**

   Please check that you've enrolled into Compute Optimizer. For more information, see Getting started with AWS Compute Optimizer. If you are enrolled into Compute Optimizer but do not see the efficiency metric, it could be due to high variance in your AWS usage. We will generate the metric automatically once your usage becomes more stable.

2. **Why don't I see history in cost efficiency?**

   You will not see history if you are a new customer of Cost Optimization Hub and Compute Optimizer. If you are an existing customer but do not see the history, it could be because of lack of historical data. You should start seeing the history with continued usage.

Prioritizing your cost optimization opportunities

In Cost Optimization Hub, you can use custom filters, sorting, and grouping, so that you can prioritize your cost optimization effort by return-on-investments.

You can continue refining your cost optimization recommendations by using the additional filters under **Chart view** or **Table view**. You can include or exclude accounts, Regions, instance types, purchase options, rightsizing options, and tags.

For example, if you want to understand which AWS accounts have the most savings opportunities for EC2 instances, you can select all accounts and set the resource type filter to **EC2 Instance**.

Choose a slice of a summary view to filter recommendations. You can also choose a particular recommendation, view its details, and deep link to the relevant pages in the Billing and Cost Management console and AWS Compute Optimizer.

At the center of the summary chart, you can see aggregated savings across all sections.

You can change to **Table view**, displaying a table for account-level estimated monthly cost savings, ordered by savings in descending order.

Understanding cost optimization strategies

Cost Optimization Hub groups your recommendations into the following cost optimization strategies:

Purchase Savings Plans

Purchase Compute, EC2 instance, and SageMaker Savings Plans.

Purchase reservations

Purchase EC2, Amazon RDS, OpenSearch, Amazon Redshift, ElastiCache, MemoryDB, and DynamoDB reservations.

Stop

Stop idle or unused resources to save up to 100% of the resource cost.

Delete

Delete idle or unused resources to save up to 100% of the resource cost.

Scale in

Scale in idle or unused resources to save on resource costs.

Rightsize

Move to a smaller EC2 instance type of the same CPU architecture.

Upgrade

Move to a later generation product, such as moving from Amazon EBS io1 volume type to io2.

Migrate to Graviton

Move from x86 to Graviton to save costs.

The following table shows the full mapping of recommended actions and resource type.

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
Purchase Savings Plans	Compute Savings Plans	All	Very low	No	No
	EC2 Instance Savings Plans	All	Very low	No	No
	SageMaker Savings Plans	All	Very low	No	No
Purchase reservations	EC2 Reserved Instances	All	Very low	No	Yes
	Amazon RDS Reserved Instances	All	Very low	No	No
	Amazon Redshift reserved nodes	All	Very low	No	No
	OpenSearch Reserved Instances	All	Very low	No	No
	ElastiCache reserved nodes	All	Very low	No	No

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	MemoryDB reserved instances	All	Very low	No	No
	DynamoDB reserved capacity	All	Very low	No	No
Stop	EC2 instance	All	Low	No	Yes
	RDS DB instance	RDS MySQL and RDS PostgreSQL engines only	Low	Yes	Yes
Delete	EBS volume	All	Low	No	No
	Amazon ECS service	All	Low	No	No
	RDS DB instance	Aurora MySQL and Aurora PostgreSQL engines only	Low	No	Yes
Scale in	EC2 Auto Scaling group	All	Low	No	No
Rightsize	EC2 instance (standalone)	No hypervisor change	Medium	Yes	Yes

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	EC2 instance (standalone)	With hypervisor change	High	Yes	Yes
	EC2 Auto Scaling group	All	Medium	Yes	Yes
	EBS volume	All	Low	No	Yes
	Lambda function	All	Low	No	Yes
	Amazon ECS service	All	Low	Yes	Yes
	RDS DB instance	All	Medium	Yes	Yes
	RDS DB instance storage	All	Low	No	Yes
	Aurora DB cluster storage	All	Low	No	Yes
Upgrade	EC2 instance (standalone)	No hypervisor change	Medium	Yes	Yes
	EC2 instance (standalone)	With hypervisor change	High	Yes	Yes

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	EC2 Auto Scaling group	All	Medium	Yes	Yes
	EBS volume	All	Low	No	Yes
	RDS DB instance	All	Medium	Yes	Yes
	RDS DB instance storage	All	Low	No	Yes
Migrate to Graviton	EC2 instance (standalone)	With Graviton-compatible inferred workload type	High	Yes	Yes
	EC2 instance (standalone)	Without Graviton-compatible inferred workload type	Very high	Yes	Yes
	EC2 Auto Scaling group	With Graviton-compatible inferred workload type	High	Yes	Yes

Action	Resource type	Conditions	Implementation effort	Resource restart needed	Rollback possible
	EC2 Auto Scaling group	Without Graviton-compatible inferred workload type	Very high	Yes	Yes
	RDS DB instance	All	Medium	Yes	Yes

Viewing your savings opportunities

You can view details about your recommended actions on the **Savings opportunities** page. Use filters to refine the list of savings opportunities, and learn more about each recommendation by using a split-view panel. For deeper analysis of any recommendation, select it and choose **Analyze with Amazon Q**.

You can also group related recommendations. Cost Optimization Hub identifies recommended actions that interact with each other, and it reduces estimated aggregated savings based on the degree of overlap.

Cost Optimization Hub deduplicates amongst resource optimization strategies and proposes the recommendation with the highest savings. It also considers the reduction in usage by implementing the recommendations.

For example, an EC2 instance can either be deleted or rightsized, but not both. When Cost Optimization Hub estimates aggregated savings for the instance, it chooses the actions with the highest savings (in this case, delete), and ignores the savings from rightsizing.

Cost Optimization Hub also deduplicates amongst Savings Plans and Reserved Instances recommendations. It defaults to commitment options that offer the highest overall savings, prioritizing Compute Savings Plans for their flexibility and broader resource coverage. These recommendations typically favor three-year all upfront options. You can customize these in Cost Optimization Hub preferences. For more information, see Commitment preferences.

Note

When you use billing transfer as a bill source account, your estimated savings in Cost Optimization Hub might not match the effective savings data in your AWS Cost and Usage Report, Cost Explorer, and Bills page. This is because Cost Optimization Hub doesn't use custom data generated by Billing Conductor.

Topics

- Viewing recommended actions and estimated savings
- Grouping related recommendations
- Exporting your recommendations

Viewing recommended actions and estimated savings

Use the following procedure to view a recommended action and estimated savings for a specific resource ID.

1. On the **Savings opportunities** page, under **Resources with estimated savings**, choose a row in the table.

   This opens a split-view panel with a recommended action and estimated savings for your chosen resource.

   The recommended action includes the following information:

   - **Usage:** The usage based on a 14-day lookback period.
   - **Estimated cost (before discounts):** The savings estimate using AWS public (On-Demand) pricing without incorporating any discounts.
   - **Estimated other discounts:** Estimated other discounts include all discounts that are not itemized, which includes Free Tier. Itemized discounts include Savings Plans and Reserved Instances.
   - **Estimated cost (after discounts):** The savings estimate incorporating all discounts with AWS, such as Reserved Instances and Savings Plans.
   - **Estimated unused net amortized commitments:** The net amortized Savings Plans and Reserved Instances costs included in the cost of the current instance but can't be used for the recommended instance.

- **Estimated monthly savings:** The estimated monthly savings amount for the recommendation.
- **Estimated savings percentage:** The estimated savings percentage relative to the total cost.

2. Based on the recommended action, you can choose to view the recommendation in the AWS Billing and Cost Management console, or you can open it in AWS Compute Optimizer or the relevant console.

Grouping related recommendations

Use the following procedure to view related recommendations and their estimated savings.

1. On the **Savings opportunities** page, choose **Group related recommendations**.
2. Choose a row in the table.

   This opens a split-view panel with a choice of recommended actions for your chosen resource type.
3. Under **Recommended actions**, select one of the recommended actions.

   This updates the recommended action details on the left-hand side and the estimated savings on the right.
4. Based on the recommended action, you can choose to view the recommendation in the AWS Billing and Cost Management console, or you can open it in AWS Compute Optimizer or the relevant console.

Exporting your recommendations

Use the following procedure to export your recommendations and their estimated savings.

The exported CSV file reflects any filters that you applied on the **Savings opportunities** page.

> **Note**
>
> The CSV download supports a maximum file size of 350 MB. If your recommendations data exceeds this limit, use Data Exports to export your data. For more information, see Creating a standard data export.

1. On the **Savings opportunities** page, choose **Download as CSV**.
2. This opens a new browser tab and begins the download.
3. Keep the tab open until the download is complete.

Estimating monthly savings

Cost Optimization Hub analyzes specific pricing discounts to provide you with a measure of your cost efficiency. This is done by dividing the aggregated estimated monthly savings of your cost optimization opportunities by your amortized monthly AWS costs, exclusive of credits and refunds.

For recommendations associated with a resource, estimated monthly cost impact is an estimation of how much your AWS bill will change over a 730-hour period (365 * 24 /12). This estimate excludes the periods when the resources were not running and if you had implemented the recommended action 730 hours ago. If the recommendation has a different lookback period, the cost impact is normalized to a 730-hour period, which is the average number of hours per month.

Note that your estimated monthly savings is a quick approximation of future savings. The actual savings that you realize is dependent on your future AWS usage patterns.

Aggregating estimated savings

Cost Optimization Hub aggregates AWS cost optimization recommendations for you across your AWS accounts and AWS Regions. For example, it makes recommendations on resource rightsizing, idle resource deletion, Savings Plans, and Reserved Instances.

You can aggregate estimated savings by the following categories:

- AWS account
- AWS Region
- Resource type
- Recommended action
- Implementation effort
- Is resource restart needed
- Is rollback possible
- Tag key

To aggregate your cost optimization recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.
3. Choose to view your savings opportunities in **Chart view** or **Table view**.
4. Choose **Aggregate estimated savings by**, and then choose a category.

Supported resources

Cost Optimization Hub generates recommendations for the following resources:

- Amazon Elastic Compute Cloud (Amazon EC2) instances
- Amazon EC2 Auto Scaling groups
- Amazon Elastic Block Store (Amazon EBS) volumes
- AWS Lambda functions
- Amazon Elastic Container Service (Amazon ECS) tasks on AWS Fargate
- Compute Savings Plans
- EC2 Instance Savings Plans
- EC2 Reserved Instances
- Amazon RDS DB instances
- Amazon RDS DB instance storage
- Amazon RDS Reserved Instances
- Amazon Aurora DB cluster storage
- ElastiCache cluster
- ElastiCache reserved nodes
- MemoryDB cluster
- MemoryDB reserved instances
- DynamoDB table
- DynamoDB reserved capacity
- DocumentDB cluster

- OpenSearch Reserved Instances
- Amazon Redshift reserved nodes
- SageMaker endpoint
- SageMaker Savings Plans
- WorkSpaces
- NAT Gateway

Resource rightsizing and idle resource recommendations are provided by AWS Compute Optimizer. To see what type of recommendations are supported for each resource, see AWS resources supported by Compute Optimizer.

Optimizing your cost with rightsizing recommendations

The rightsizing recommendations feature in Cost Explorer helps you identify cost-saving opportunities by downsizing or terminating instances in Amazon Elastic Compute Cloud (Amazon EC2). Rightsizing recommendations analyze your Amazon EC2 resources and usage to show opportunities for how you can lower your spending. You can see all of your underutilized Amazon EC2 instances across member accounts in a single view to immediately identify how much you can save. After you identify your recommendations, you can take action on the Amazon EC2 console.

> **Note**
>
> We recommend that you use Cost Optimization Hub to identify cost optimization opportunities. For full details, see Cost Optimization Hub.
> Rightsizing recommendations doesn't support billing transfer.

Topics

- Getting started with rightsizing recommendations
- Using your rightsizing recommendations
- Sharing your rightsizing recommendations
- Understanding rightsizing recommendations calculations
- Understanding reservations in Cost Explorer

- Accessing reservation recommendations

Getting started with rightsizing recommendations

You can access your reservation recommendations and resource-based recommendations in the Billing and Cost Management console. After you enable the feature, it can take up to 24 hours to generate your recommendations.

To enable and access rightsizing recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Management preferences**.
3. On the **Preferences** page, under **Rightsizing - *legacy*** in the **General** tab, select **Enable Rightsizing recommendations**.
4. Choose **Save preferences**.

   > **Note**
   >
   > Only regular or a management account can enable rightsizing recommendations. After you enable the feature, both member and management account can access rightsizing recommendations unless the management account specifically prohibits member account access on the **settings** page.
   > To improve the recommendation quality, AWS might use your published utilization metrics, such as disk or memory utilization, to improve our recommendation models and algorithms. All metrics are anonymized and aggregated before AWS uses them for model training. If you want to opt out of this experience and request that your metrics not be stored and used for model improvement, contact AWS Support. For more information, see AWS Service Terms.

5. To access rightsizing recommendations, in the navigation pane, under **Legacy pages**, choose **Rightsizing**.

Using your rightsizing recommendations

You can see the following top-level key performance indicators (KPIs) in your rightsizing recommendations:

- **Optimization opportunities** – The number of recommendations available based on your resources and usage
- **Estimated monthly savings** – The sum of the projected monthly savings associated with each of the recommendations provided
- **Estimated savings (%)** – The available savings relative to the direct instance costs (On-Demand) associated with the instances in the recommendation list

To filter your rightsizing recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, under **Legacy pages**, choose **Rightsizing**.
3. On the **Rightsizing recommendations** page, under **Recommendation parameters**, filter your recommendations by selecting any or all of the following check boxes:
   - Idle instances
   - Underutilized instances
   - Include Savings Plans and Reserved Instances
4. Under **Findings**, use the search bar to filter by the following parameters:
   - Account ID (option available from the management account)
   - Region
   - Cost allocation tag

To view your rightsizing recommendations details

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, under **Legacy pages**, choose **Rightsizing**.
3. On the **Rightsizing recommendations** page, under **Findings**, choose a recommendation to view the details.

Enhancing your recommendations using CloudWatch metrics

We can examine your memory utilization if you enable your Amazon CloudWatch agent.

To enable memory utilization, see Installing the CloudWatch Agent.

> **Important**
>
> When you create a CloudWatch configuration file, use the default namespace and default names for the collected metrics.
> For **InstanceID**, choose `append_Dimension`. Do not add additional dimensions for individual memory or disk metrics. Disk utilization is currently not examined.
> For Linux instances, choose `mem_used_percent` as your metric for your CloudWatch agent to collect. For Windows instances, choose `"% Committed Bytes In Use"`.

For more information about the CloudWatch agent, see Collecting Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent in the *Amazon CloudWatch User Guide*.

Sharing your rightsizing recommendations

You can download a rightsizing recommendations report in CSV format.

To download your recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, under **Legacy pages**, choose **Rightsizing**.
3. Under **Findings**, choose **Download CSV**.

The following is a list of fields in the downloadable CSV file from the **Rightsizing recommendations** page. The fields are repeated if there are multiple rightsizing options available. The file also contains all of your relevant cost allocation tags.

- **Account ID** – The AWS account ID that owns the instance that the recommendation is based off of.
- **Account Name** – The name of the account that owns the instance that the recommendation is based off of.
- **Instance ID** – The unique instance identifier.
- **Instance Name** – The name you've given to the instance.

- **Instance Type** – The instance family and size of the original instance.
- **Instance Name** – The name you've given an instance. This field will show as blank if you haven't given the instance a name.
- **OS** – The operating system or platform of the current instance.
- **Region** – The AWS Region that the instance is running in.
- **Running Hours** – The total number of running hours of the instance over the last 14 days.
- **RI Hours** – The subset of the total running hours that are covered by an AWS reservation over the look-back period.
- **OD Hours** – The subset of the total running hours that are On-Demand over the look-back period.
- **SP Hours** – The subset of the total running hours that are covered by Savings Plans over the look-back period.
- **CPU Utilization** – The maximum CPU utilization of the instance over the look-back period.
- **Memory Utilization** – The maximum memory utilization of the instance over the look-back period (if available from the Amazon CloudWatch agent).
- **Disk Utilization** – The maximum disk utilization of the instance over the look-back period (if available from the CloudWatch agent - currently not supported).
- **Network Capacity** – The maximum network input/output operations per second capacity of the current instance. This isn't a measure of actual instance use or performance, only capacity. It's not considered in the recommendation.
- **EBS Read Throughput** – The maximum number of read operations per second.
- **EBS Write Throughput** – The maximum number of write operations per second.
- **EBS Read Bandwidth** – The maximum volume of read KiB per second.
- **EBS Write Bandwidth** – The maximum volume of write KiB per second.
- **Recommended Action** – The recommended action, either modify or terminate the instance.
- **Recommended Instance Type 1** – The instance family and size of the recommended instance type. For termination recommendations, this field is empty.
- **Recommended Instance Type 1 Estimated Saving** – The projected savings based on the recommended action, instance type, associated rates, and your current Reserved Instance (RI) portfolio.
- **Recommended Instance Type 1 Projected CPU** – The projected value of the CPU utilization based on utilization of current instance CPU and recommended instance specifications.

- **Recommended Instance Type 1 Projected Memory** – The projected value of the memory utilization based on utilization of current instance memory and recommended instance specifications.
- **Recommended Instance Type 1 Projected Disk** – The projected value of the disk utilization based on utilization of current instance disk and recommended instance specifications.
- **Recommended Instance Type 1 Network Capacity** – The maximum network input/output operations per second capacity of the recommended instance. This isn't a measure of actual instance use or performance, only capacity. It's not considered in the recommendation.

Understanding rightsizing recommendations calculations

This section provides an overview of the savings calculations that are used in your rightsizing recommendations algorithms.

Consolidated billing family

To identify all instances for all accounts in the consolidated billing family, rightsizing recommendations look at the usage for the last 14 days for each account. If the instance was stopped or terminated, we remove it from consideration. For all remaining instances, we call CloudWatch to get maximum CPU utilization data, memory utilization (if enabled), network in/out, local disk input/ output (I/O), and performance of attached EBS volumes for the last 14 days. This is to produce conservative recommendations, not to recommend instance modifications that could be detrimental to application performance or that could unexpectedly impact your performance.

Determining if an instance is idle, underutilized, or neither

We look at the maximum CPU utilization of the instance for the last 14 days to make one of the following assessments:

- **Idle** – If the maximum CPU utilization is at or below 1%. A termination recommendation is generated, and savings are calculated. For more information, see Savings calculation.
- **Underutilized** – If the maximum CPU utilization is above 1% and cost savings are available in modifying the instance type, a modification recommendation is generated.

If the instance isn't idle or underutilized, we don't generate any recommendations.

Generating modification recommendations

Recommendations use a machine learning engine to identify the optimal Amazon EC2 instance types for a particular workload. Instance types include those that are a part of AWS Auto Scaling groups.

The recommendations engine analyzes the configuration and resource usage of a workload to identify dozens of defining characteristics. For example, it can determine whether a workload is CPU-intensive or whether it exhibits a daily pattern. The recommendations engine analyzes these characteristics and identifies the hardware resources that the workload requires.

Finally, it concludes how the workload would perform on various Amazon EC2 instances to make recommendations for the optimal AWS compute resources that the specific workload.

Savings calculation

We first examine the instance running in the last 14 days to identify whether it was partially or fully covered by an RI or Savings Plans, or running On-Demand. Another factor is whether the RI is size-flexible. The cost to run the instance is calculated based on the On-Demand hours and the rate of the instance type.

For each recommendation, we calculate the cost to operate a new instance. We assume that a size-flexible RI covers the new instance in the same way as the previous instance if the new instance is within the same instance family. Estimated savings are calculated based on the number of On-Demand running hours and the difference in On-Demand rates. If the RI isn't size-flexible, or if the new instance is in a different instance family, the estimated savings calculation is based on whether the new instance had been running during the last 14 days as On-Demand.

Cost Explorer only provides recommendations with an estimated savings greater than or equal to $0. These recommendations are a subset of Compute Optimizer results. For more performance-based recommendations that might result in a cost increase, see Compute Optimizer.

You can choose to view saving with or without consideration for RI or Savings Plans discounts. Recommendations consider both discounts by default. Considering RI or Savings Plans discounts might result in some recommendations showing a savings value of $0. To change this option, see Using your rightsizing recommendations.

> **Note**
>
> Rightsizing recommendations doesn't capture second-order effects of rightsizing, such as the resulting RI hour's availability and how they will apply to other instances. Potential savings based on reallocation of the RI hours aren't included in the calculation.

Understanding reservations in Cost Explorer

Balancing your reservation usage and your On-Demand instance or provisioned capacity usage can help you achieve better efficiency. To help, Cost Explorer provides tools that help you understand where your greatest reservation costs are and how you can potentially lower your costs. Cost Explorer provides you with an overview of your current reservations, shows your utilization and coverage, and calculates reservation recommendations that could save you money if you purchase them.

Using your reservation reports

You can use the **Reservations Overview** page in the Billing and Cost Management console to see how many reservations you have, how much your reservations are saving you compared to similar usage of On-Demand Instances, and how many of your reservations are expiring this month.

Cost Explorer breaks down your reservations and savings by service and lists your potential savings; that is, the cost of On-Demand usage compared to what that usage could cost you with a reservation.

To use your potential savings, see Accessing reservation recommendations.

Managing your reservation expiration alerts

You can track your reservations and when those reservations expire in Cost Explorer. With reservation expiration alerts, you receive email alerts 7, 30, or 60 days in advance before your reservation expires. These alerts can be sent to up to 10 email recipients. You can also choose to be notified on the day that your reservation expires. Reservation expiration alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon OpenSearch Service reservations.

To turn on reservation expiration alerts

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Navigate to the **Overview** page under the **Reservations** section.
3. Choose **Manage alert subscriptions** in the upper right corner.
4. Select the check boxes for when you want to receive your alerts.
5. Enter email addresses for who you want to notify. You can have up to 10 email recipients.
6. Choose **Save**.

AWS starts monitoring your reservation portfolio and sends alerts based on the preferences that you specify.

Accessing reservation recommendations

If you enable Cost Explorer, you automatically get Amazon EC2, Amazon RDS, ElastiCache, OpenSearch Service, Amazon Redshift, Amazon MemoryDB, and Amazon DynamoDB purchase recommendations that could help reduce your costs. Reservations provide a discounted hourly rate (up to 75%) compared to On-Demand or provisioned capacity pricing. Cost Explorer generates your reservation recommendations using the following process:

- Identifies your On-Demand instance or provisioned capacity usage for a service during a specific time period
- Collects your usage into categories that are eligible for a reservation
- Simulates every combination of reservation in each category of usage
- Identifies the best number of each type of reservation to purchase to maximize your estimated savings

For example, Cost Explorer automatically aggregates your Amazon EC2 Linux, shared tenancy, and c4 family usage in the US West (Oregon) Region and recommends that you buy size-flexible regional RIs to apply to the c4 family usage. Cost Explorer recommends the smallest size instance in an instance family. This makes it easier to purchase a size-flexible RI. Cost Explorer also shows the equal number of normalized units so that you can purchase any instance size that you want. For this example, your RI recommendation would be for `c4.large` because that is the smallest size instance in the c4 instance family.

Cost Explorer recommendations are based on a single account or organization usage of the past seven, 30, or 60 days. Cost Explorer uses On-Demand instance usage during the selected look-back period to generate recommendations. All other usage in the look-back period that are covered by features such as RI, SPOT, and Savings Plans aren't included. Amazon EC2, ElastiCache, OpenSearch Service, Amazon Redshift, Amazon MemoryDB, and Amazon DynamoDB recommendations are for reservations scoped to Region, not Availability Zones, and your estimated savings reflects the application of those reservations to your usage. Amazon RDS recommendations are scoped to either Single-AZ or Multi-AZ RIs. Cost Explorer updates your recommendations at least once every 24 hours.

> **Note**
>
> Cost Explorer doesn't forecast your usage or take forecasts into account when recommending reservations. Instead, Cost Explorer assumes that your historical usage reflects your future usage when determining which reservations to recommend.

Linked accounts can only see recommendations if they have the relevant permissions. Linked accounts need permissions to view Cost Explorer and permissions to view recommendations. For more information, see Viewing reservation recommendations.

Topics

- RI recommendations for size-flexible RIs
- Viewing reservation recommendations
- Understanding reservation recommendations
- Modifying reservation recommendations
- Saving reservation recommendations
- Using reservation recommendations

RI recommendations for size-flexible RIs

Cost Explorer also considers the benefits of size-flexible regional RIs when generating your RI purchase recommendations. Size-flexible regional RIs help maximize your estimated savings across eligible instance families in your recommendations. AWS uses the concept of normalized units to compare the various sizes within an instance family. Cost Explorer uses the smallest normalization

factor to represent the instance type that it recommends. For more information, see Instance size flexibility in the *Amazon Elastic Compute Cloud User Guide*.

For example, let's say you own an EC2 RI for a `c4.8xlarge`. This RI applies to any usage of a `Linux/Unix c4` instance with shared tenancy in the same region as the RI, such as the following instances:

- One `c4.8xlarge` instance
- Two `c4.4xlarge` instances
- Four `c4.2xlarge` instances
- Sixteen `c4.large` instances

It also includes combinations of EC2 usage, such as one `c4.4xlarge` and eight `c4.large` instances.

If you own an RI that is smaller than the instance that you're running, you are charged the prorated, On-Demand price for the excess. This means that you could buy an RI for a `c4.4xlarge`, use a `c4.4xlarge` instance most of the time, but occasionally scale up to a `c4.8xlarge` instance. Some of your `c4.8xlarge` usage is covered by the purchased RI, and the rest is charged at On-Demand prices. For more information, see How Reserved Instance discounts are applied in the *Amazon Elastic Compute Cloud User Guide*.

Viewing reservation recommendations

Linked accounts need the following permissions to view recommendations:

- `ViewBilling`
- `ViewAccount`

For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

To view your reservation recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, under **Reservations**, choose **Recommendations**.

3. On the **Recommendations** page, under **Recommendation parameters**, choose the **Service** that you want recommendations for.

Understanding reservation recommendations

The **Reservations Recommendations** page shows you your estimated potential savings, your reservation purchase recommendations, and the parameters that Cost Explorer used to create your recommendations. You can change the parameters to get recommendations that might match your use case more closely.

The **Recommendations** page shows you the following three numbers:

- **Total purchase recommendations** – The number of different reservation purchase options Cost Explorer has found for you.
- **Estimated monthly savings** – How much Cost Explorer calculates you could save by purchasing the recommended reservations.
- **Estimated savings vs. On-Demand rates** – Your estimated savings as a percentage of your current costs.

These numbers provide you with a rough estimate of how much you could potentially save by buying more reservations. You can recalculate these numbers for a different use case using the following **Recommendation parameters**:

- **Term** – The duration for which you want recommendations.
- **Offering class** – Whether you want recommendations for a standard or convertible reservation.
- **Payment option** – Whether you want to pay for recommendations upfront.
- **Based on the past** – The number of days of previous usage that you want your recommendations to take into account.

At the bottom of the page are tabs with some of your savings estimates. The **All accounts** tab enables you to see the recommendations based on the combined usage across your entire organization, and the **Individual accounts** tab enables you to see recommendations that Cost Explorer generated on a per-linked-account basis. The table on each tab shows the different purchase recommendations and details about the recommendations. If you want to see the usage that Cost Explorer based a recommendation on, choose the **View associated usage** link in the recommendation details. This takes you to a report that shows the exact parameters that Cost

Explorer used to generate your recommendation. The report also shows your costs and associated usage grouped by **Purchase option**, so that you can view the On-Demand Instance usage that your recommendation is based on.

> **Note**
>
> Recommendations that Cost Explorer bases on an individual linked account consider all usage by that linked account, including any RIs used by that linked account. This includes RIs shared by another linked account. The recommendations don't assume that an RI will be shared with the linked account in the future.
> When you use billing transfer as a bill source account, your estimated savings in reservation recommendations might not match the effective savings data in your AWS Cost and Usage Report, Cost Explorer, and Bills page. This is because reservation recommendations don't use custom data generated by Billing Conductor.

You can sort your recommendations by **Monthly estimated savings**, **Upfront RI cost**, **Purchase recommendation**, or **Instance type**.

Modifying reservation recommendations

You can change the information that Cost Explorer uses when it creates your recommendations, and you can also change the types of recommendations that you want. This allows you to see recommendations for the reservations that work best for you, such as All upfront reservations with a one-year term, based on your last 30 days of usage.

> **Note**
>
> Instead of forecasting your future usage, Cost Explorer assumes that your future usage is the same as your previous usage. Cost Explorer also assumes that you are renewing any expiring reservations.

To modify your reservation recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, under **Reservations**, choose **Recommendations**.

3. On the **Recommendations** page, under **Recommendation parameters**, choose the **Service** that you want recommendations for.
4. Choose the relevant **Term**.
5. Choose the relevant **Offering class**.
6. Choose the relevant **Payment option**.
7. For **Based on the past**, select how many days of usage that you want your reservation recommendations to be based on.
8. Choose either **All accounts** or **Individual accounts** to see recommendations based either on your organization-wide usage or on all of your linked accounts based on their individual account usage.

Saving reservation recommendations

You can save reservation recommendations as a CSV file.

To save your reservation recommendations

1. On the **Reservations Recommendations** page, under **Recommendation parameters**, choose the **Service** that you want recommendations for and update any parameters you want to change.
2. Under **Recommended actions**, choose **Download CSV**.

The CSV file contains the following columns.

Reservation recommendations CSV columns

Column name	Service	Column explanation
Account ID	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The account associated with your recommendation.

Column name	Service	Column explanation
Availability zone	Amazon RDS	The availability zone of the instances used to generate a recommendation.
Average hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The average number of normalized units used per hour over the period chosen for generating recommendations.
Average hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The average number of instance hours used per hour over the period chosen for generating recommendations.
Average number of capacity units used per hour in the selected historical period	Amazon DynamoDB	The average number of provisioned capacity units used per hour over the period chosen for generating recommendations.
Break even months	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The estimated length of time before you recoup your upfront costs for this set of recommended reservations.
Cache engine	Amazon ElastiCache	The kind of engine that the recommended ElastiCache reserved node runs, such as Redis or Memcheched.

Column name	Service	Column explanation
Capacity unit type	Amazon DynamoDB	The type of capacity unit for the recommendation. Read capacity units are used for operations that retrieve data from a table. Write capacity units are used for operations that insert, update, or delete data in a table.
Database edition	Amazon RDS	The edition of the database engine that the recommended RDS reserved instance runs.
Database engine	Amazon RDS	The kind of engine that the recommended RDS reserved instance runs, such as Aurora MySQL or MariaDB.
Deployment model	Amazon RDS	Whether your recommended reserved instance is for RDS Custom. If the value is "Custom", you must to purchase the recommended reserved instances for RDS Custom to see potential savings.
Deployment option	Amazon RDS	Whether your reserved instance is for an RDS instance in a single Availability Zone or an RDS instance with a backup in another Availability Zone.

Column name	Service	Column explanation
Estimated savings	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The estimated savings of the recommended reservations.
Expected utilization	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	How much of the recommended reservations Cost Explorer estimates you will use.
Instance type	Amazon EC2, RDS, OpenSearch Service	The type of instance that the recommendation is generated for (for example, `m4.large` or `t2.nano`). For size-flexible recommendations, Cost Explorer aggregates all usage in a organization (for example, the m4 family) and shows a recommendation for the smallest reserved instance type that is available for purchase (for example, `m4.large`).
Max hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The maximum number of normalized units used in an hour over the period chosen for generating recommendations.

Column name	Service	Column explanation
Max hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The maximum number of instance hours used in an hour over the period chosen for generating recommendations.
Maximum number of capacity units used per hour in the selected historical period	Amazon DynamoDB	The maximum number of provisioned capacity units used in an hour over the period chosen for generating recommendations.
Min hourly normalized unit usage in historical period	Amazon EC2, RDS, MemoryDB	The minimum number of normalized units used in an hour over the period chosen for generating recommendations.
Min hourly usage in historical period	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	The minimum number of instance hours used in an hour over the period chosen for generating recommendations.
Minimum number of capacity units used per hour in the selected historical period	Amazon DynamoDB	The minimum number of provisioned capacity units used in an hour over the period chosen for generating recommendations.
Node type	Amazon ElastiCache, Redshift, MemoryDB	The type of node that the recommendation is generated for, such as `ds2.xlarge` .

Column name	Service	Column explanation
Normalized hours to purchase	Amazon EC2, RDS, MemoryDB	How many normalized units that Cost Explorer recommends that you buy.
Number of instances to purchase	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB	How many reservations Cost Explorer recommends that you buy.
Offering class	Amazon EC2	The offering class associated with the recommendation.
Payment option	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The recommended payment option for the recommendation.
Platform	Amazon EC2	The operating system and license model for the recommended reserved instance type.
Recommended number of capacity units to purchase	Amazon DynamoDB	How many reserved capacity units Cost Explorer recommends that you buy.

Column name	Service	Column explanation
Recommendation date	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The date that Cost Explorer generated your recommendation.
Recurring monthly cost	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The recurring monthly cost of the recommended reservations.
Region	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The Region used to generate a recommendation. You must purchase the recommended reservations in the recommended Region to see potential savings.
Size flexible	Amazon EC2, RDS, MemoryDB	Whether a recommended reservation is size-flexible.
Tenancy	Amazon EC2	The tenancy for the recommendation. Valid values are **shared** or **dedicated**.

Column name	Service	Column explanation
Term	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The recommended term length for the recommendation.
Upfront cost	Amazon EC2, RDS, Redshift, ElastiCache, OpenSearch Service, MemoryDB, DynamoDB	The upfront cost associated with the recommendation.

Using reservation recommendations

To purchase the recommended reservations, go to the purchase page in a service console. You can also save a CSV file of your recommendations and purchase the reservations at a later date.

To use Amazon Elastic Compute Cloud recommendations

1. On the **Reserved Instance Recommendations** page, choose Amazon EC2 RI Purchase Console.
2. Purchase your RIs by following the instructions at Buy Reserved Instances for Amazon EC2 in the *Amazon Elastic Compute Cloud User Guide*.

To use Amazon Relational Database Service recommendations

1. On the **Reserved instances** page in the Amazon RDS console, choose **Purchase Reserved DB Instance**.
2. Purchase your reservations by following the instructions at Purchasing reserved DB instances for Amazon RDS in the *Amazon RDS User Guide*.

To use Amazon Redshift recommendations

1. On the **Reserved nodes** page in the Amazon Redshift console, choose **Purchase reserved nodes**.
2. Purchase your reservations by following the instructions at Purchasing a reserved node in the *Amazon Redshift Management Guide*.

To use Amazon OpenSearch Service recommendations

1. On the **Reserved Instance Leases** page in the OpenSearch Service console, choose **Order Reserved Instance**.
2. Purchase your reservations by following the instructions at Reserved Instances in Amazon OpenSearch Service in the *Amazon OpenSearch Service Developer Guide*.

To use Amazon ElastiCache recommendations

1. On the **Reserved Nodes** page in the ElastiCache console, choose **Purchase reserved nodes**.
2. Purchase your reservations by following the instructions at Purchasing a reserved node in the *Amazon ElastiCache User Guide*.

To use Amazon MemoryDB recommendations

1. On the **Reserved nodes** page in the MemoryDB console, choose **Purchase reserved nodes**.
2. Purchase your reservations by following the instructions at Working with reserved nodes in the *Amazon MemoryDB Developer Guide*.

To use Amazon DynamoDB recommendations

1. On the **Reserved capacity** page in the DynamoDB console, choose **Purchase reserved capacity**.
2. Purchase your reserved capacity by following the instructions at Reserved capacity in the *Amazon DynamoDB Developer Guide*.

Generating estimates with Pricing Calculator

The in-console AWS Pricing Calculator is an AWS Billing and Cost Management feature that enables you to estimate your planned cloud costs using your discounts and purchase commitments. You can use Pricing Calculator to assess the cost impact and understand the return on investment for migrating workloads, planning new or growth of existing workloads, and plan for commitment purchases.

In-console AWS Pricing Calculator and the public Pricing Calculator

AWS provides two separate Pricing Calculator experiences: the in-console AWS Pricing Calculator and the public Pricing Calculator website. One of the main differences between the in-console version and the public version is that the public version doesn't require you to create an AWS account. The in-console Pricing Calculator is a feature of the AWS Billing and Cost Management service in the AWS console and has its own set of APIs, so it requires you to create an AWS account. For more information on how to create an AWS account, see Getting started with AWS Cost Management.

Both pricing calculators allow you to generate estimates for your specific workloads or applications. However, the in-console AWS Pricing Calculator has more advanced features that allow you to do the following:

- Model your future usage changes by importing your existing usage. This eliminates the need to manually input historical usage data.
- Model purchase commitment changes such as Savings Plans and Reserved Instances. Analyze the cost impact of changes to your existing commitments or adding new commitments.
- You can use both public On-Demand rates and after discount rates. This gives you a realistic estimate based on your existing usage tier.
- You can generate cost estimates for specific applications or workloads that you model. Alternatively, you can generate cost estimates for your consolidated billing family which takes into account your modeled usage and commitments. This automatically layers your existing usage and active commitments.

For more information about the public Pricing Calculator, see What is AWS Pricing Calculator?

Features of the in-console AWS Pricing Calculator

The in-console Pricing Calculator consists of two main estimate types:

Workload estimate

- Allows you to estimate the cost of specific workloads, applications, resources, and architectural changes.
- This type of estimate is available to all account types (standalone, management, and member accounts).
- Management accounts can configure the effective rate type that is available for use by their member accounts. The rate types available are Before discounts, After discounts, and After discounts and purchase commitments.
- Workload estimates are available immediately upon running the estimate.

For more information, see Workload estimates.

Bill estimate

- Allows you to estimate the cost of applying any modeled usage and commitment changes to your entire consolidated bill across your AWS organization.
- This type of estimate is only available to management or standalone account users.
- The bill estimate automatically includes your last month's consolidated billing usage. It also includes your existing commitments like Savings Plans and Reserved Instances.
- You can model new usage changes as well as modifications to your existing commitments without affecting your current commitments. For example, you can add new usage, make a change to existing usage, and remove an existing commitment to see how these configurations affect costs without affecting your bill.

For more information, see Bill estimates.

Pricing for AWS Pricing Calculator

AWS Pricing Calculator is available to all AWS customers. Workload estimates are provided free of charge. For bill estimates, you receive five free estimates per month. After your fifth estimate in a calendar month, the estimates cost $2 each.

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services.

> **Note**
>
> If an estimate fails to generate, this will not count as one of your five free estimates per month. You will also not be charged for any failed estimates.

Getting started with AWS Pricing Calculator

Before you can use AWS Pricing Calculator, you must make sure that you have properly set up your AWS account and user permissions. For instructions about how to set up your AWS account and permissions, see Getting started with AWS Cost Management.

Accounts supported by AWS Pricing Calculator

The following AWS account types are supported by Pricing Calculator:

- Standalone AWS account — A standalone AWS account that doesn't have AWS Organizations enabled.
- Member account of an organization — An AWS account that's a member of an AWS Organization.
- Management account of an organization — An AWS account that administers an AWS Organization.

For more information about AWS Organizations, see What is AWS Organizations?

> **Note**
>
> When you use billing transfer as a bill source account, AWS Pricing Calculator provides pricing estimates based on public pricing data, not the rates configured by your bill transfer account.

Accessing Pricing Calculator

You can access the Pricing Calculator within the AWS Billing and Cost Management Console and through a set of APIs. You can also access the calculator through the AWS SDK and CLI.

AWS Pricing Calculator provides service-specific resources, actions, and condition context keys for use in IAM permission policies. For more information, see Actions, resources, and condition keys for AWS Pricing Calculator.

For member accounts to create estimates using discounted rates, the management account of the organization must enable access to use discounts from the Pricing Calculator console preferences. If the management account hasn't enabled access, the estimates default to public pricing rates.

Important

- You must enable Cost Explorer to allow Pricing Calculator to import your historical AWS workload usage. For instructions on how to import your historical workload usage, see Adding historical usage to my workload estimate.
- Pricing Calculator will override any Cost Management preferences you have set, such as Linked account discounts. That means that if `After_discount` is selected, you will be able to see `netUnblendedRate` based cost, irrespective of your Linked account discount preference.
- For access to the Pricing Calculator console, you must migrate your policies from under `aws-portal` to fine-grained access controls. For information about how to do this, see Migrating access control for AWS Billing.
- Amazon Billing Conductor (ABC) proforma data views aren't available in Pricing Calculator. If your member accounts have access to Pricing Calculator, they will be able to view chargeable cost and usage depending on their rate type preference setting in Pricing Calculator.

Understanding AWS Pricing Calculator concepts

To help you get started, this page explains the key concepts of the in-console AWS Pricing Calculator and how they interact.

Key concepts

The in-console AWS Pricing Calculator enables you to estimate your planned cloud costs using your discount rates and purchase commitments. Here are the key concepts you'll work within the Pricing Calculator.

Before discount rates

The before discount rates refer to the public, On-Demand pricing for AWS services, without any discounts or commitments applied. These are the standard rates that are available to any AWS customer. For more information, see Before discount rates.

After discount rates

After discount rates refer to what you pay for AWS services, after applying any pricing discounts you have with AWS. For more information, see After discount rates.

Workload estimate

A workload estimate represents the incremental AWS usage you want to model. You can add and modify usage details in a workload estimate. However, workload estimates don't allow you to model changes to your AWS commitments. You can refer to a workload estimate resource using an Amazon Resource Name (ARN). For more information about workload estimates, see Workload estimates.

Usage

This represents your general AWS usage across all services, showing how much of each product is used.

Commitments

This represents your AWS commitments like Savings Plans or Reserved Instances, which provide discounted pricing in exchange for a term-based commitment. For more information, see Compute and EC2 Instance Savings Plans and Amazon EC2 Reserved Instances.

> **Note**
>
> You can't use a workload estimate to model your commitments.

Bill scenario

A bill scenario acts as a container that allows you to model anticipated usage and commitments for future needs. You can refer to a bill scenario resource using an ARN. For more information, see Bill estimates.

Bill estimate

A bill estimate incorporates all inputs from a bill scenario together with your usage and commitments from the most recent anniversary bill to calculate estimated costs. The pre-tax cost of the entire consolidated billing family will be displayed. You can refer to a bill estimate resource using an ARN. For more information, see Bill estimates.

> **Note**
>
> Bill estimates are only available to management and standalone accounts.

Groups

You can organize your estimates by defining groups. A group can reflect how your company is organized. A group can also reflect other organization methods, such as by product stack or product architecture. For example, if you want to price out different ways to build your AWS setup, you can use different groups for each variation of your setup and compare the estimates.

Anniversary bill

This is the line items for services that you used during the month. For more information about billing term definitions, see Billing details in the *AWS Data Exports User Guide*.

Understanding rates, discounts, and purchase commitments

This section outlines AWS rates, discounts, and commitments supported by Pricing Calculator and how they apply to both workload and bill estimate types. Before discount and after discount rates only apply to workload estimates. Bill estimate considers your own rates based on your existing usage and commitments, other discounts, and credits. Your choice of a rate type does not impact the bill estimate calculation.

Topics

- Before discount rates
- After discount rates
- Purchase commitments
- Setting your rates for member accounts

Before discount rates

The before discount rates refer to the public, On-Demand pricing for AWS services, without any discounts or commitments applied. These are the standard rates that are available to any AWS customer.

The before discount rates can be helpful in the following use cases:

- If you're a new AWS customer without any discounts or commitments, the before discount rates accurately represent the pricing you would pay for On-Demand usage.
- When estimating the cost of using a new AWS service or feature that you don't currently have discounts for, the before discount rates provide a baseline cost comparison.

Note

- Before discount rates don’t take into account any discounts or commitments that you may be eligible for as an existing AWS customer.
- If you are using before discount rates, tiered pricing is only accounted for if the modeled usage crosses a tier of usage. For example, if you want to model 100TB/month of S3 standard storage use, Pricing Calculator uses tiered S3 standard rates for the first 50 TB/Month and the next tiered rate for the remaining 50 TB/Month.

After discount rates

AWS Pricing Calculator offers two ways to estimate costs that account for your organization's discounts:

- After discounts
- After discounts and purchase commitments

These options help you understand how different types of discounts impact your estimated costs, whether from usage-based discounts alone or combined with commitment-based savings.

After discounts

After discount rates refer to what you pay for AWS services, after applying any usage-based discounts you have with AWS. These rates can help you estimate your actual AWS costs, taking the following into account:

- Your organization's volume or pricing discounts.
- Tiered pricing based on your usage volumes. Tiered pricing is only accounted for if the modeled usage crosses a tier of usage. For example, if you want to model 100TB/month of S3 standard storage use, Pricing Calculator uses tiered S3 standard rates for the first 50 TB/Month and the next tiered rate for the remaining 50 TB/Month.

> **Note**
>
> If you are using after discount rates, then a single rate is used based on your highest usage tier for that product SKU as of the last completed anniversary bill.

After discount rates are the increase in cost for using one additional unit of a SKU, considering all usage-based discounts at the consolidated billing family level. For SKUs that you used last month, the effective rate is the net unblended rate of the SKUs in the Cost and Usage Report. For SKUs that you have not yet used, we will construct mock workloads by adding one unit of usage for each of the SKUs on top of prior month's usage, and get the net unblended rate from the resulting anniversary bill output.

If you have any purchase commitments (Savings Plans or Reservations), the calculated after discount rate will not be affected by the commitment discount. This means that the after discount rate we use is based solely on your actual usage based on On-Demand usage rates and applicable discounts, such as tiering discounts, volume discounts, but not commitment discounts.

> **Note**
>
> AWS Pricing Calculator doesn’t take AWS Free Tier into account when calculating after discount rates. The calculator sets a minimum usage threshold that excludes Free Tier levels. For example, if the Free Tier covers up to 100 units, the calculator sets the usage to 101 units when calculating rates. This means that if you input usage amounts that would normally fall within the Free Tier, the calculator applies standard pricing rates to provide a cost estimate.

When you use After discount rates to generate a cost estimate, the estimate is tailored to your specific AWS usage-based pricing terms. This can help you to make informed decisions about how changes to your usage would impact your actual AWS spend.

Note

- After discount rates don't include the impact of active commitments, such as Savings Plans and Reserved Instances. The calculator assumes you don't have any unused commitments that may be applied to the estimate. The estimated cost might be larger than your actual spend if you have unused commitments that can be applied to your usage.
- For accounts opting in to Cost Explorer, after discount rates will become available for use within 72-90 hours of enabling Cost Explorer.
- Your most recent after discount rates are calculated based on the last completed anniversary bill month and are available by the 15th of the current month.
- After discounts aren't available to any product launched after the 15th of the current month. In this case, the after discount rates will become available on 15th of the following month.

After discounts and purchase commitments

The After discounts and purchase commitments rate calculates the effective pricing based on your usage patterns. For a specific AWS resource (SKU), the total cost combines various pricing models and commitment terms, including 1-year and 3-year Compute Savings Plans, Instance Savings Plans, Convertible RIs, and Standard RIs with no upfront payment options. For each commitment type, the calculation multiplies the coverage percentage by the corresponding commitment rate for that SKU. Any remaining On-Demand usage is calculated by multiplying the On-Demand coverage percentage by the SKU's After discount rate. For an example of how a purchase commitment applies to your usage, see Understanding how Savings Plans apply to your usage.

For EC2 instances, the calculation considers your previous month's usage patterns and determines coverage percentages based on whether the instance family was used in the same AWS Region, in different Regions, or not used at all. For example, if you used m5.2xlarge instances in a specific Region last month, the formula will calculate coverage based on that Region's specific usage patterns. If there was no usage of a particular instance family, the formula defaults to using

the overall EC2 usage patterns across all Regions to determine coverage percentages. All these coverage percentages (including On-Demand usage) must add up to 100%.

Similar approaches apply to other commitment-eligible services like Lambda, Fargate, SageMaker, and Amazon RDS, where we calculate service-specific coverage percentages based on your usage patterns.

Note

- For accounts opting in to Cost Explorer, After discount and purchase commitments rates will become available for use within 72-90 hours of enabling Cost Explorer.
- Your most recent After discount and purchase commitments rates are calculated based on the last completed anniversary bill month and are available by the 15th of the current month.
- After discount and purchase commitments aren't available to any product launched after the 15th of the current month. In this case, the rates will become available on 15th of the following month.

Purchase commitments

The purchase commitments supported by AWS Pricing Calculator are Amazon EC2 Reserved Instances (RIs) and Compute and EC2 Instance Savings Plans. For more information, see Compute and EC2 Instance Savings Plans and Amazon EC2 Reserved Instances.

You can use Pricing Calculator to model the impact of adding new Savings Plans or Reserved Instances, or removing existing commitments as part of a bill scenario. This allows you to see how these commitments would affect your overall estimated AWS costs.

Note

Any Savings Plans or Reserved Instances you have modeled in your public Pricing Calculator estimates won't be included when you're adding these estimates from the public Pricing Calculator to a workload estimate or bill scenario.

Setting your rates for member accounts

This section outlines how to set estimate rates for member accounts.

Procedure

To set estimate rates for member accounts

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Saved estimates** page, choose the settings icon.
4. In the prompt that appears, select the discount rates you want to apply to your member account(s).
5. Choose **Confirm**.

Workload estimates

Workload estimates allow you to estimate the cost of specific workloads, applications, resources, and architectural changes. This type of estimate is available to all account types: standalone AWS accounts, management accounts and member accounts. Management accounts can configure the effective rate type that is used for member accounts within their organization. The rate types are Before discounts, After discounts, and After discounts and purchase commitments. For more information about how a rate is applied to workload estimate, see After discount rates.

You only see cost estimates for usage that you specify. You can add new usage, import usage from your existing cost and usage data, or import public pricing calculator usage through its share URL. Workload estimates don't account for any usage that hasn't been specified in the estimate. For instructions on how to create a public Pricing Calculator estimate URL, see Sharing your estimate in the public Pricing Calculator user guide.

Topics

- Creating a workload estimate
- Adding new services to my workload estimate
- Configure new services in my workload estimate
- Adding historical usage to my workload estimate
- Adding previously saved estimates to my workload estimate

Creating a workload estimate

This section outlines how to generate a workload estimate.

Prerequisites

The following procedure assumes that you have already completed the Setting your rates for member accounts process.

Procedure

To create a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Workload estimate** tab, choose **Create workload estimate**.
4. In the **Create workload estimate** prompt, you can do the following:
   - Give your estimate a title.
   - Add key and value tag to your estimate.
   - Select the rate type for your estimate.

   > **Note**
   >
   > Once you create an estimate with a rate type, you will no longer be able to change the rate type selection later.
5. Choose **Submit**.

Adding new services to my workload estimate

This section outlines how to add new services to a workload estimate.

Prerequisites

The following procedure assumes that you have already completed the Creating a workload estimate process.

Procedure

To add new services to a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. Navigate to the workload estimate where you want to add new services.
4. From the **Add** dropdown, choose **New services**.
5. On the **Add new service** page, you can do the following:
   - Choose an account.
   - Choose a location type.
   - Choose a location.
   - Choose a service.
6. You can choose to add your usage to an existing group or a new group you create.
7. To add the new services to the workload estimate, choose **Next**.

Next steps

For instructions on how to configure the new services that you added to your workload estimate, see Configure new services in my workload estimate.

Configure new services in my workload estimate

This section outlines how to configure new services in a workload estimate.

Prerequisites

The following procedure assumes that you have already completed the Adding new services to my workload estimate process.

Procedure

To configure new services in a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. Navigate to the workload estimate where you added new services.

4. Select the dropdown arrow beside the name of the new service you added.
5. Choose **Configure**.
6. On the **Configure service** page, you can select **Guided configuration** or **Condensed configuration**.

   - In the **Guided configuration**, you can select a template for that specific service. For more information, see Guided configuration.
   - In the **Condensed configuration**, you can select the usage type and operation for that specific service. For more information, see Condensed configuration.
7. To complete the configuration process for the new services, choose **Save changes**.

Guided configuration

After you choose a Location type, Location, and Account, you will need to choose a Template. The templates provide products that typically go together so that you can build a realistic estimate. For example, if you choose the Amazon EC2 template, you are provided with EC2 Instance, EBS storage, EBS snapshots, CloudWatch monitoring, and several data transfer options. If you don't want to add a specific product to your estimate, you can remove that product by unselecting the checkbox on the product's container. All products are selected by default.

> **Note**
>
> The values in fields outside of Usage amount will not be saved and you will not be able to view those fields if you reopen a saved usage line.

Condensed configuration

You can use the condensed configuration if you are familiar with usage types and operations of products that you want to model usage for. Usage types are the units that each service uses to measure the usage of a specific type of resource. For example, the BoxUsage:t2.micro(Hrs) usage type filters by the running hours of Amazon EC2 t2.micro instances. Operation are requests made to a service and tasks performed by a service, such as write and get requests to Amazon S3.

Usage types and operation are available through the Price List API `GetProducts`. On Pricing Calculator console's Condensed configuration, you will be able to find the usage types and operations in their respective dropdown without needing to query Price List API.

Adding historical usage to my workload estimate

This section outlines how to add historical usage to a workload estimate.

Prerequisites

The following procedure assumes that you have already completed the Creating a workload estimate process.

Procedure

To add historical usage to a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. Navigate to the workload estimate where you want to add historical usage.
4. From the **Add** dropdown, choose **Historical workload from my accounts**.
5. Select the time range of historical usage that you want to import.

> **Note**
>
> A maximum of 2000 usage lines that can be added to a single workload estimate.

6. (Optional) Add up to five filters. Filters allow you to specify lines of your usage that you want to add. Filter example include cost category and services.

> **Note**
>
> For each filters, the values are based on the time period selected in the previous step.

7. You can choose to add your usage to an existing group or a new group you create.
8. Choose **Preview**.
9. Check that the preview shows the usage that you want to import to your workload estimate.

> **Note**
>
> The usage is aggregated based on the account, Region, service code, usage type, and operation. This means that if the time range is across multiple months and your

selection yields usage from the same account, Region, service code, usage type, and operation across multiple months, then all the usage amount and cost is added together into one line.

10. To add the historical usage to the workload estimate, choose **Import**.

> **Note**
>
> Once you import historical usage into your estimate, you will see that the estimated cost is calculated for all of the imported lines. Because you have explicitly added these lines in the import, these imported usage are considered part of the estimate. In a workload estimate, this is considered incremental usage.

Adding previously saved estimates to my workload estimate

This section outlines how to add previously saved estimates from the public Pricing Calculator to a workload estimate. For instructions on how to generate a public Pricing Calculator URL, see Sharing an estimate link in the public Pricing Calculator user guide.

> **Note**
>
> Any Savings Plans or Reserved Instances you have modeled in your public Pricing Calculator estimates won't be included when you're adding these estimates from the public Pricing Calculator to a workload estimate or bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a workload estimate process.

Procedure

To add previously saved estimates to a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.

3. Navigate to the workload estimate where you want to add previously saved estimates (URL).
4. From the **Add** dropdown, choose **Previously saved estimates**.
5. In the **Shared estimate URL** section, paste the URL of your previously saved estimate. For instruction on how to generate a public Pricing Calculator URL, see Sharing an estimate link in the public Pricing Calculator user guide.
6. Select an account
7. You can choose to add your usage to an existing group or a new group you create.
8. Choose **Import**.

Bill estimates

Bill estimates allow you to estimate pre-tax costs of your usage and commitments across your consolidated bill family. The bill estimate automatically includes your consolidated usage from the previous month. For example, if you add 100 instance-hours for a specific EC2 instance type in a given AWS Region, those hours will be added on top of your existing usage for that instance type in that Region with no extra input needed. It also includes your existing commitments like Savings Plans and Reserved Instances. Your benefit sharing preferences are applied, and any applicable discounts, credits, or refunds are included just as they were on your most recent anniversary bill. You can model new usage changes as well as add new commitments, modify your existing commitments, and add how you want your reserved instance and savings plans benefits to be shared.

To generate a bill estimate you must create a bill scenario. Bill scenario allows you to model commitments in addition to usage. After you complete modeling usage and commitments in a scenario, you can run a bill estimate.

Note

- Depending on the size of your workloads, generating a bill estimate can take between 20 minutes to 12 hours.
- Bill estimates are only available to management accounts and standalone AWS accounts.
- When you use billing transfer as a bill source account, AWS Pricing Calculator provides pricing estimates based on public pricing data, not the rates configured by your bill transfer account.

Topics

- Understanding the data entities used in bill estimates
- Creating a bill scenario
- Adding historical usage to your bill scenario
- Adding new services to my bill scenario
- Adding previously saved estimates to my bill scenario
- Adding benefit sharing preference to my bill scenario
- Adding Savings Plans to my bill scenario
- Adding Reserved Instances to my bill scenario
- Stale and expired bill scenarios
- Creating a bill estimate
- Viewing your Bill estimate

Understanding the data entities used in bill estimates

The bill estimates generation engine of AWS Pricing Calculator uses the following data entities from the specified timeframe.

Data entity	Description
Member accounts	The selection of member accounts are used to identify how usage was incurred by each member account during the last anniversary bill month and we layer your modeled usage on top of it.
Product and pricing attributes	The product and pricing attributes governs pricing. For example, a t4g.large EC2 shared tenancy instance running Linux in us-east-1 for 500 hrs for the month. A t4.large EC2 instance has 2 vCPUs, 8 GiB memory. Shared tenancy, number of vCPUs, allocated memory are the product attributes that determine the pricing for each unit of usage for this EC2 instance. We use the attributes and its pricing as of what was available during the last anniversary bill month.

Data entity	Description
Existing usage	Existing usage indicates the unchanged usage level from your last anniversary bill month upon which any of your modeled usage from a bill scenario is layered.
Savings Plans inventory	This inventory indicates active Savings Plans as of the last anniversary bill month. This inventory is automatically included in your bill estimates and any new Savings Plans you model is layered on this inventory that applies to Savings Plans eligible usage.
Reserved Instances inventory	This inventory indicates active Reserved Instances as of the last anniversary bill month. This inventory is automatically included in your bill estimates and any new Reserved Instances you model is layered on this inventory that applies to Reserved Instances eligible usage.
Benefits sharing preference	The accounts based on your **Reserved Instances and Savings Plans discount sharing preference** billing preference gets automatic Reserved Instances and Savings Plans discount benefits. We consider this benefit application setting as of the last anniversary bill to apply automatic benefit sharing when estimating your bill and allow you to layer discount sharing preference changes.

Creating a bill scenario

This section outlines how to generate a bill scenario.

Procedure

To create a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose **Create bill scenario**.

4. In the **Create bill scenario** prompt, you can do the following:
   - Give your bill scenario a name.
   - Add key and value tag to your scenario.
5. Choose **Submit**.

Adding historical usage to your bill scenario

This section outlines how to add historical usage to your bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add historical usage to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenario** of the **Bill estimate** tab, choose the scenario you want to add usage to.
4. From the **Add** dropdown in the **Usage** section, choose **Historical workload from my accounts**.
5. Select the time range of historical usage that you want to import.

> **Note**
>
> A maximum of 2000 usage lines that can be added to a single bill scenario.

6. (Optional) Add up to five filters. Filters allow you to specify lines of your usage that you want to add. Filter example include cost category and services.

> **Note**
>
> For each filters, the values are based on the time period selected in the previous step.

7. You can choose to add your usage to an existing group or a new group you create.
8. Choose **Preview**.

9. Check that the preview shows the usage that you want to import to your workload estimate.

> **Note**
>
> The usage is aggregated based on the account, Region, service code, usage type, and operation. This means that if the time range is across multiple months and your selection yields usage from the same account, Region, service code, usage type, and operation across multiple months, then all the usage amount and cost is added together into one line.

10. To add the historical usage to the workload estimate, choose **Import**.

Adding new services to my bill scenario

This section outlines how to add new services to a bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add new services to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose the scenario you want to add usage to.
4. From the **Add** dropdown in the **Usage** section, choose **New services**.
5. On the **Add new service** page, you can do the following:
   - Choose an account.
   - Choose a location type.
   - Choose a location.
   - Choose a service.
6. You can choose to add your usage to an existing group or a new group you create.
7. To add the new services to the workload estimate, choose **Configure**.

8. On the **Configure service** page, you can select **Guided configuration** or **Condensed configuration**.
   - In the **Guided configuration**, you can select a template for that specific service. For more information, see Guided configuration.
   - In the **Condensed configuration**, you can select the usage type and operation for that specific service. For more information, see Condensed configuration.
9. To complete the configuration process for the new services, choose **Save changes**.

Adding previously saved estimates to my bill scenario

This section outlines how to add previously saved estimates from the public Pricing Calculator to a bill scenario. For instructions on how to generate a public Pricing Calculator URL, see Sharing an estimate link in the public Pricing Calculator user guide.

> **Note**
>
> Any Savings Plans or Reserved Instances you have modeled in your public Pricing Calculator estimates won't be included when you're adding these estimates from the public Pricing Calculator to a workload estimate or bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add previously saved estimates to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose the scenario you want to add usage to.
4. From the **Add** dropdown in the **Usage** section, choose **Previously saved estimates**.
5. In the **Shared estimate URL** section, paste the URL of your previously saved estimate. For instruction on how to generate a public Pricing Calculator URL, see Sharing an estimate link in the public Pricing Calculator user guide.

6. Select an account
7. You can choose to add your usage to an existing group or a new group you create.
8. Choose **Import**.

Adding benefit sharing preference to my bill scenario

This section outlines how to add Reserved Instances and Savings Plans sharing group preference to a bill scenario. This allows you to model benefit sharing preference to evaluate the impact on your bill.

For information on sharing preferences, you can read details at Reserved Instances and Savings Plans discount sharing preferences..

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add Reserved Instances and Savings Plans sharing group preference to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose the scenario you want to add group sharing preference to.
4. In the **Reserved Instances and Savings Plans sharing group preferences** section, choose **Edit**.
5. Select the group preference you want and choose **Save changes**.
   - If you select Prioritized sharing group or Restricted sharing group, select a Cost Category from the drop down. For Open sharing, you do not need to choose a Cost Category.
6. Choose **Configure**.

Adding Savings Plans to my bill scenario

This section outlines how to add Savings Plans to a bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add Savings Plans to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose the scenario you want to add Savings Plans to.
4. In the **Savings Plans** section, choose **Add Savings Plans**.
5. Select the type of Savings Plans you want and choose **Add**.
6. Verify if you need to configure the Savings Plans you just added.
7. If you need to configure the Savings Plans, select the checkbox of the Savings Plans you need to configure.
8. Choose **Edit**.
9. On the Add new service page, do the following:
   - Choose a term.
   - Choose a Region.
   - Choose a instance family.
   - Choose a payment option.
   - Provide an hourly commitment.
10. Choose **Configure**.

Adding Reserved Instances to my bill scenario

This section outlines how to add Reserved Instances to a bill scenario.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To add Reserved Instances to a bill scenario

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** of the **Bill estimate** tab, choose the scenario you want to add Reserved Instances to.
4. In the **Reserved Instances** section, choose **Add Reserved Instances**.
5. Select the type of Reserved Instances you want and choose **Add**.
6. Verify if you need to configure the Reserved Instances you just added.
7. If you need to configure the Reserved Instances, select the checkbox of the Reserved Instances you need to configure.
8. Choose **Edit**.
9. On the Add new service page, do the following:
   - Choose a Region.
   - Choose a instance type.
   - Choose a platform.
   - Provide a tenancy.
   - Choose a offering class.
   - Choose a payment option.
   - Choose a term.
   - Provide a quantity.
10. Choose **Configure**.

Stale and expired bill scenarios

This section describes the stale and expired status of your bill scenario.

When a bill scenario displays a **Stale** status, you can no longer use it to create a Bill Estimate. A bill scenario will go stale after the final day of the month in which it was created. For example, if you created a bill scenario on the 15th of February, the scenario would go stale on March 1st. The stale scenario will be visible for 13 months. After 13 months the scenario will expire and

delete automatically. For example, a bill scenario created in February 2025 will expire and delete automatically on March 31, 2026.

Creating a bill estimate

This section outlines how to generate a bill estimate.

Prerequisites

The following procedure assumes that you have already completed the Creating a bill scenario process.

Procedure

To create a bill estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. In the **Bill scenarios** section of the **Bill estimate** tab, choose the scenario you want to generate a bill estimate from.
4. Choose **Create**.
5. In the **Create a bill estimate** prompt, you can do the following:
   - Give your bill estimate a name.
   - Add key and value tag to your estimate.
6. Choose **Save**.

While we are creating your bill estimate, the status shows **In progress**. When your bill estimate is ready, the status will show **Saved**. You will also receive an email notification when your bill estimate is ready.

> **Note**
>
> Depending on the size of your workloads, generating a bill estimate can take between 20 minutes to 12 hours.

Viewing your Bill estimate

This page describes the information displayed in the key sections of your Bill estimate. If you are part of an AWS Organization, this page displays pre-tax cost and usage for your consolidated bill family. If you are a standalone account, this page displays pre-tax cost and usage for your account. For information about how to generate a bill estimate, see Creating a bill estimate.

> **Note**
>
> If you run a bill estimate by specifying Reserved Instances and Savings Plans sharing group preference, you will see a section at the top of the bill estimate page that will tell you the benefit sharing preference and Cost category you used. It will allow you to go the Bill preferences page to make these changes directly.

Estimate section	Description
Estimate details	Displays when the estimate was created, expiration date, and the AWS account that created the estimate.
Bill impact	Displays the high-level estimate costs • **Total historical bill** If you're part of an AWS organization, this is the pre-tax cost from the anniversary bill charges of your consolidated billing family. If you're a standalone account, this is the the pre-tax cost from the anniversary bill charges of your account. • **Total estimated bill** If you're part of an AWS organization, this is the estimated cost for the consolidated billing family that includes your usage and commitment models. If you are a standalone account, this is the estimated cost that includes your usage and commitment models for your account. This cost is all charges net of all applicable discounts. This cost includes charges from all usage line items and commitments.

Estimate section	Description
Net change for top impacted services	This charts displays a net cost comparison between your anniversary bill charges and your estimated costs for your AWS services. If you have multiple services in your estimate, we will display the top seven services in the chart.

Estimate section	Description
Changed usage lines per service	Displays how costs and usage have changed for each affected service. This includes service usage lines that were directly and indirectly modeled in your bill scenario. Indirect modeling in your bill scenario is usage that was affected by increased or decreased commitment coverage. We identify these changes by comparing service details between your original anniversa ry bill and the new bill estimate. The following list provides an overview of each column in this section: • **Service > usage lines** — Displays the service code, usage type, and operation. • **Region** — An AWS Region, Wavelength zone, or Local zone where the usage line item is incurred. • **Account** — The AWS account in your consolidated bill family that incurred this usage and cost. • **Historical cost** — The cost of this line from your anniversa ry bill. If historical cost is empty, this means that the usage line didn't exist in your anniversary bill. This might happen when you model a product (SKU) usage that you've never used before. • **Modifications** — The cost arising from direct modeling of this usage line. In some cases this cost can reflect changes arising from commitment coverage. • **Commitments** — This shows all commitment coverage for the usage lines. For example, if a usage line is covered by Savings Plans, this shows the sum of all Savings Plans discounts that covers this line. • **Discounts** — The sum of any other discounts that has covered the usage line. • **Estimated cost** — The final pre-tax estimated cost of the usage line net of all commitments and discounts.

Estimate section	Description
Savings Plans	This displays all active and modeled Savings Plans for the account. The **State** column only displays a **New**, **Existing**, **Modified**, or **Configure** status. • **New** — Savings Plans you have modeled in the bill scenario from which the estimate is created. • **Existing** — The active and non-expired Savings Plans in your account. • **Excluded** — Savings Plans that you have chosen to exclude from the estimate. • **Configure** — This requires you to set the parameter you want for your Savings Plans.
Reserved Instances	This displays all active and modeled Reserved Instances for the account. The **State** column only displays a **New**, **Existing**, **Modified**, or **Configure** status. • **New** — Reserved Instances you have modeled in the bill scenario from which the estimate is created. • **Existing** — The active and non-expired Reserved Instances in your account. • **Excluded** — Reserved Instances that you have chosen to exclude from the estimate. • **Configure** — This requires you to set the parameter you want for your Reserved Instances.

Exporting your estimates

You can export your AWS Pricing Calculator workload estimates as a JSON or CSV file. You can only export your workload estimates through the AWS Cost Management console.

Procedure

To export a workload estimate

1. Open the Pricing Calculator console at https://console.aws.amazon.com/costmanagement/ .
2. In the navigation pane, choose **Pricing Calculator**.
3. On your **Saved estimates** page, choose the workload estimate you want to export.
4. In your workload estimate, choose **Export**.
5. From the dropdown, choose **CSV** or **JSON**. This will download the workload estimate to your local drive.

Using EventBridge with AWS Pricing Calculator

The in-console AWS Pricing Calculator can send events to Amazon EventBridge whenever certain events happen in your bill estimate. Unlike other destinations, you don't need to select which event types you want to deliver. After you have EventBridge set up, Pricing Calculator events can be sent to EventBridge. You can use EventBridge rules to route events to additional targets. For more information about setting up EventBridge, see Amazon EventBridge setup and prerequisites in the *Amazon EventBridge API Reference*.

The following lists the events AWS Pricing Calculator sends to EventBridge.

Event type	Description
BillEstimate Created	A bill estimate was created. The ARN, estimate name, and estimate ID of the bill estimate for which the event is sent to EventBridge will be emitted in the event.
BillEstimate Succeeded	A bill estimate completed. This means you will now be able to view the results of the bill estimate. The ARN, estimate name, and estimate ID of the bill estimate for which the event is sent to EventBridge will be emitted in the event.
BillEstimate Failed	A bill estimate generation failed.

Event type	Description
	The ARN, estimate name, and estimate ID of the bill estimate for which the event is sent to EventBridge will be emitted in the event.

You can also use AWS Pricing Calculator to send event notifications with EventBridge to write rules that take actions when an event occurs pertaining to your estimate. For example, you can have it send you a notification. For more information about rules in Amazon EventBridge, see Create a rule in Amazon EventBridge in the *Amazon EventBridge API Reference*.

For more information about the actions and data types you can interact with using the EventBridge API, see Amazon EventBridge API Reference in the *Amazon EventBridge API Reference*.

Amazon EventBridge permissions

AWS Pricing Calculator doesn't require any additional permissions to deliver events to Amazon EventBridge.

Event message structure examples

BillEstimate Created

```
{
    "version": "0",
    "id": "00000000-0000-0000-0000-000000000001",
    "detail-type": "BillEstimate Created",
    "source": "aws.bcm-pricing-calculator",
    "account": "111122223333",
    "time": "2024-09-12T13:47:34Z",
    "region": "us-east-1",
    "resources": ["arn:aws:bcm-pricing-calculator::111122223333:bill-
estimate/00000000-0000-0000-0000-000000000000"],
    "detail": {
        "id": "00000000-0000-0000-0000-000000000001",
        "name": "amzn-example-name"
     }
}
```

BillEstimate Succeeded

```
{
    "version": "0",
    "id": "00000000-0000-0000-0000-000000000002",
    "detail-type": "BillEstimate Succeeded",
    "source": "aws.bcm-pricing-calculator",
    "account": "111122223333",
    "time": "2024-09-12T13:47:34Z",
    "region": "us-east-1",
    "resources": ["arn:aws:bcm-pricing-calculator::111122223333:bill-
estimate/00000000-0000-0000-0000-000000000002"],
    "detail": {
        "id": "00000000-0000-0000-0000-000000000002",
        "name": "amzn-example-name"
     }
}
```

BillEstimate Failed

```
{
    "version": "0",
    "id": "00000000-0000-0000-0000-000000000003",
    "detail-type": "BillEstimate Failed",
    "source": "aws.bcm-pricing-calculator",
    "account": "111122223333",
    "time": "2024-09-12T13:47:34Z",
    "region": "us-east-1",
    "resources": ["arn:aws:bcm-pricing-calculator::111122223333:bill-
estimate/00000000-0000-0000-0000-000000000003"],
    "detail": {
        "id": "00000000-0000-0000-0000-000000000003",
        "name": "amzn-example-name",
        "failureReason": "We can't process this request right now because of an
 internal error. Try again later."
     }
}
```

Managing your costs using generative AI with Amazon Q Developer

Amazon Q Developer is a generative artificial intelligence (AI) powered conversational assistant that can help you understand, build, extend, and operate AWS applications. Amazon Q Developer provides powerful capabilities to help you manage your AWS costs through natural conversation. You can analyze your historical and forecasted costs from Cost Explorer, discover cost-saving recommendations from Cost Optimization Hub and AWS Compute Optimizer, understand Savings Plans and reservation opportunities, and get instant answers about AWS product attributes or service pricing. Amazon Q Developer can both answer specific questions (e.g., "What were net unblended costs for EC2 instances last month?") or perform complex or open-ended analysis (e.g., "What were the biggest drivers of last week's cost decrease?"). You can also visualize your cost data in charts and graphs using Amazon Q Developer with prompts like "Show me an area chart of costs by service over the last 6 months" or "Show me a bar chart of daily spending last week". Amazon Q Developer simplifies how you interact with AWS cost data by letting you ask questions in your own words instead of learning query syntax or navigating multiple console pages, while providing precise answers backed by real data from your AWS account, showing exactly which APIs were called, and showing you where to find the information in the console.

For more information about Amazon Q Developer, see What is Amazon Q Developer in the *Amazon Q Developer User Guide*.

Topics

- Overview of cost management capabilities in Amazon Q Developer
- How the cost management capabilities in Amazon Q Developer work
- Security for cost management capabilities in Amazon Q Developer

Overview of cost management capabilities in Amazon Q Developer

Amazon Q Developer is a generative artificial intelligence (AI) powered conversational assistant that can help you understand, analyze, and optimize your AWS costs. With Amazon Q Developer, you can ask complex, open-ended questions about your costs and let Q perform the analysis on your behalf. Q explores your cost data, forms and tests hypotheses, gathers information from multiple sources, performs calculations, and provides custom visualizations and actionable insights, all through a natural language conversation.

Amazon Q Developer helps you get deeper cost insights with less time and expertise. Instead of manually exploring data across multiple tools, adjusting filters, and performing offline calculations, you can delegate the analytical work to Q. This is particularly valuable for teams without dedicated FinOps expertise, as Q reduces the learning curve by handling the complexity of knowing which tools to use, which APIs to call, and how to structure queries.

For more information about Amazon Q Developer, see What is Amazon Q Developer in the *Amazon Q Developer User Guide*.

What you can do

Amazon Q Developer provides powerful capabilities across a wide range of cost management use cases:

Understand your costs

Analyze your historical spending patterns, view cost breakdowns by service or account, and track trends over time. For example, you can ask "What were my costs by service last month?" or "Show me my EC2 spending trends for the past six months."

Investigate cost changes

Perform root cause analysis to understand why your costs changed. Q can explore your data, identify the drivers of cost increases or decreases, and help you understand period-over-period changes. For example, you can ask "Why did my costs increase last week?" and Q will investigate the underlying causes.

Find savings opportunities

Identify cost optimization recommendations from Cost Optimization Hub, AWS Compute Optimizer, and Savings Plans and reservation recommendations. Q can help you find idle resources, rightsizing opportunities, and commitment-based discount opportunities. For example, you can ask "What are my top cost optimization opportunities?" or "Which EC2 instances are over-provisioned?". You can also ask detailed follow-up questions, such as "Tell me more about the second recommendation" or "Why was that EBS volume classified as idle?".

Monitor cost health

Check your budget status, identify cost anomalies, and monitor your free tier usage. Q can alert you to unusual spending patterns and help you stay within your budget targets. For example, you can ask "Have any teams exceeded their budgets?" or "Do I have any cost anomalies?"

Estimate future costs

Understand AWS service pricing and estimate the cost of new workloads you plan to build. Q can help you compare pricing across regions, calculate costs for specific configurations, and forecast future spending. For example, you can ask "How much would it cost to store 1 PB in S3 in Dublin?" or "What's my cost forecast for this month?"

Analyze commitment performance

Review your Savings Plans and Reserved Instances coverage and utilization to understand how effectively you're using commitment-based discounts. Q can identify underutilized commitments and opportunities to improve your discount coverage. For example, you can ask "Analyze our Savings Plans performance over the last month."

Check payment status

List previously-issued invoices, check whether you have an outstanding payment balance, and check which payment methods you have set up.

How to use it

Amazon Q Developer adapts to however you phrase your questions. You can ask specific, bounded questions when you know exactly what you want, or ask open-ended exploratory questions and let Q investigate on your behalf.

Example questions

Specific questions

When you know what data you need, you can ask targeted questions:

- "What were my net amortized S3 costs last month?"
- "Show me EC2 rightsizing recommendations."
- "How much does a c8g.2xlarge instance cost in us-east-1?"

Open-ended questions

When you want Q to explore and analyze your costs, you can ask broader questions:

- "Why did my costs increase last week?"
- "Analyze my cost data and give me insights."

- "What are some easy ways to lower my costs?"

Multi-step analytical questions

Q can handle complex questions that require gathering data from multiple sources and performing calculations:

- "What's my effective cost per EC2 instance hour after Savings Plans discounts?"
- "Which accounts had the biggest cost increases and what drove them?"
- "Analyze our Savings Plans performance and identify optimization opportunities."

Estimation questions

Q can help you estimate costs for new workloads or compare pricing across regions:

- "How much would it cost to store 1 PB in S3 in Dublin?"
- "What's the monthly cost of a t4g.xlarge RDS instance with Multi-AZ and 300 GB gp2 storage?"
- "What would be the price to build a basic three tier web app, with a small EC2 instance, API gateway, a ~5GB SQL database, and a basic JS front-end hosted in CloudFront?"

Visualizations

You can create charts and graphs to visualize your cost data:

- "Chart S3 costs by storage tier last week"
- "Graph my DynamoDB costs by region by day for the last 30 days"
- "Graph RDS costs by instance type for the last 6 months"
- "Show me an area chart of EC2-Other costs over the last 12 months"

Tips for getting the most value

Use follow-up questions to steer the analysis

Amazon Q Developer maintains context within a conversation, so you can ask follow-up questions to dive deeper or guide the analysis in a specific direction:

- Initial question: "Why did my costs increase last month?"

- Follow-up: "Next, check if any Savings Plans expired."
- Follow-up: "Focus on the EC2."

Be specific when you know what you want

While Q can handle open-ended questions, being more specific helps you get answers faster if you know exactly what you are looking for:

- Instead of: "Tell me about my costs"
- Try: "What were my net amortized EC2 instance costs in us-east-1 last month?"

Use key-value pairs for tags and cost categories

When filtering by cost allocation tags or cost categories, if you know the specific keys and values you want to use, you can specify them:

- Instead of: "How much did we spend in prod last month?"
- Try: "What was last month's spend for tag key='Environment', value='Production'?"

User experience

Transparency

With each response, Amazon Q Developer provides transparency into how it arrived at its answer:

- **API calls displayed**: Q shows you the details of each API call it makes, including the exact parameters used. This allows you to understand precisely what data Q retrieved.
- **Console deep-links**: Where available, Q provides links to matching views in the AWS Management Console, so you can verify the data or explore further.

This transparency helps you build trust in Q's responses and gives you the information you need to provide more specific instructions in follow-up questions.

Conversational and iterative

Amazon Q Developer maintains context throughout your conversation, enabling a natural, iterative dialogue:

- **Ask follow-up questions**: You can ask follow-up questions to dive deeper into specific aspects of the analysis. For example, after Q identifies that EC2 costs increased, you can ask "Which accounts had the highest EC2 cost increases?". You can also ask questions about generated visualizations, such as "What drove that increase on Wednesday?"
- **Steer the analysis**: You can guide Q's investigation by providing specific directions. For example, "Next, check if any Savings Plans expired" or "Focus on the production environment." For visualizations, you can request changes with follow-up prompts like "Let's switch from a bar chart to a line chart."
- **Refine your questions**: If a response isn't quite what you need, you can rephrase or add more details to get a more targeted answer.

Actionable insights

Amazon Q Developer goes beyond simple data retrieval to provide meaningful insights:

- **Interprets findings**: Q not only provides facts and data, it also identifies patterns, highlights anomalies, and explains what the data means.
- **Identifies opportunities**: Q proactively surfaces cost optimization opportunities and potential issues in your spending.
- **Provides guidance**: For optimization recommendations, Q can explain the steps needed to implement the changes.

Multi-account cost management

For customers logged into the management account of an AWS organization, Amazon Q Developer automatically aggregates cost data from all member accounts in the organization. You can filter or group costs by member account, just as you would in Cost Explorer.

You can also create custom billing views to define custom multi-account aggregations. Custom billing views allow you to aggregate data from multiple member accounts or even multiple organizations. Once you create a custom billing view, the aggregations are available in both Cost Explorer and Amazon Q Developer. For more information, see Getting started with custom billing views. To use a custom billing view in Amazon Q Developer, specify the name of the billing view you'd like to use for your conversation with a prompt like "I'd like you to use the cross-org-rollup billing view for the rest of this conversation." Custom billing views are supported for historical and forecasted cost data and budgets data.

Getting started

Prerequisites

To use the cost management capabilities in Amazon Q Developer, you need:

- **Appropriate IAM permissions**: You need permissions to use Amazon Q Developer and to access the underlying Billing and Cost Management services. For details, see the section called "Security and privacy".
- **Cost Explorer opt-in**: To analyze your historical and forecasted costs, you must first opt in to Cost Explorer. To opt in, open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/. After you opt in, it can take up to 24 hours for AWS to process your cost and usage data.

To take advantage of the full range of cost management capabilities, you can also:

- **Opt in to Cost Optimization Hub**: To receive personalized cost optimization recommendations, opt in to Cost Optimization Hub, and then choose **Enroll**. After you opt in, it can take up to 24 hours for recommendations to be calculated.
- **Opt in to Compute Optimizer**: To receive resource optimization recommendations, such as rightsizing EC2 instances or terminating idle EBS volumes, opt in to Compute Optimizer.
- **Create budgets**: To monitor your spending against budget targets, create budgets in AWS Budgets.
- **Create a cost anomaly detection monitor**: To identify unusual spending patterns, create a cost anomaly detection monitor in AWS Cost Anomaly Detection.
- **Enable resource-level data, hourly data, and extended history**: To access resource-level cost data, hourly granularity, and up to 38 months of cost history, configure these settings on the Cost Management Preferences page.

Start a conversation with Amazon Q Developer

1. Sign in to the AWS Management Console at https://console.aws.amazon.com.
2. Choose the Amazon Q icon on the right side of the console navigation bar.
3. Ask a question about your costs, such as:
    - "What were my costs last month?"

- "What are my top cost optimization opportunities?"
- "How much does a c8g.2xlarge instance running Linux cost in us-east-1?"
- "Show me a pie chart of my costs by region last week"

Use Amazon Q Developer in chat applications

You can also chat about your AWS costs in Microsoft Teams and Slack. Amazon Q Developer in chat applications allows you to ask cost questions directly from your team's chat channels, making it easy to collaborate on cost analysis and optimization without switching contexts. For example, you can ask "@Amazon Q what were my EC2 costs last month?" or "@Amazon Q what are my top cost optimization opportunities?" directly in your Slack or Teams channel.

To get started with Amazon Q Developer in chat applications, see Chatting with Amazon Q Developer in chat applications in the *Amazon Q Developer User Guide*.

Next steps

After you start using Amazon Q Developer for cost management, you can:

- Learn more about the section called “How it works” to understand the agentic architecture and data sources
- Review the section called “Security and privacy” to ensure your team has appropriate access
- Explore the full range of capabilities by asking open-ended questions like "Analyze my costs and give me insights"
- Set up additional services like Cost Optimization Hub and Budgets to unlock more capabilities

Pricing

The cost management capabilities in Amazon Q Developer are included with Amazon Q Developer. Under the Amazon Q Developer Free Tier, you can ask up to 25 questions per account per month that require account or resource context to answer (including cost management questions). Beyond this free tier limit, an Amazon Q Developer Pro subscription is required.

For more information, see Amazon Q Developer pricing.

How the cost management capabilities in Amazon Q Developer work

Agentic architecture

Amazon Q Developer uses an agentic architecture to analyze your AWS costs. When you ask a question, Q creates a plan for how to answer it, gathers data from multiple sources, performs calculations, and dynamically updates its plan based on what it learns at each step. This approach allows Q to handle complex, open-ended questions that do not have predefined workflows.

To answer your question, Amazon Q Developer can perform the following steps.

1. **Forms a plan**: When you ask a question, Q analyzes your request and creates an initial plan for how to gather the necessary information.
2. **Gathers data**: Q retrieves data from the appropriate Billing and Cost Management APIs based on your question. For complex questions, Q may call multiple APIs in series or in parallel.
3. **Performs calculations**: Q can perform calculations ranging from simple period-over-period changes to complex unit economic metrics like cost per vCPU-hour or cost per GB-month of storage.
4. **Updates the plan**: As Q reviews the results from each API call or calculation, it updates its plan based on what it learns. For example, if Q discovers that EC2 costs increased significantly, it might decide to investigate whether any Savings Plans expired.
5. **Continues until complete**: Q continues gathering data and refining its analysis until it has enough information to provide a comprehensive answer to your question.

Throughout this process, Q displays the details of each API call it makes and each calculation it performs, so you can see exactly how it arrived at its answer.

If you request it, Q can create a chart of your Billing and Cost Management data. To create a chart, Q gathers data from the relevant APIs, performs any necessary calculations, formats the data to populate the chart, then renders the chart. Charts generated in Amazon Q Developer reflect a snapshot of your billing data at the time you requested the chart, and do not update as additional charges are incurred.

Data sources and API integrations

Amazon Q Developer retrieves cost data from 38 APIs across seven Billing and Cost Management services. This broad integration allows Q to answer questions that span multiple data sources without requiring you to switch between different tools or console pages.

Cost Explorer

Amazon Q Developer uses Cost Explorer APIs to retrieve your historical and forecasted cost and usage data:

- **GetCostAndUsage**: Retrieves cost and usage data aggregated by time period and dimension
- **GetCostAndUsageWithResources**: Retrieves resource-level cost data with hourly granularity
- **GetCostForecast**: Retrieves forecasted costs for a specified time period
- **GetUsageForecast**: Retrieves forecasted usage for a specified time period
- **GetDimensionValues**: Retrieves available values for cost dimensions (such as service names or account IDs)
- **GetTags**: Retrieves available cost allocation tag keys and values
- **GetCostCategories**: Retrieves available cost category keys and values
- **GetAnomalies**: Retrieves detected cost anomalies
- **GetReservationCoverage**: Retrieves the percentage eligible spend covered by reservations
- **GetReservationUtilization**: Retrieves the utilization of purchased reservations
- **GetReservationPurchaseRecommendation**: Retrieves recommendations for purchasing reservations
- **GetSavingsPlansCoverage**: Retrieves the percentage of eligible spend covered by Savings Plans
- **GetSavingsPlansUtilization**: Retrieves the utilization of purchased Savings Plans
- **GetSavingsPlansUtilizationDetails**: Retrieves detailed utilization data for Savings Plans
- **GetSavingsPlansPurchaseRecommendation**: Retrieves recommendations for purchasing Savings Plans
- **GetRightsizingRecommendation**: Retrieves rightsizing recommendations for EC2 instances
- **GetCostAndUsageComparisons**: Retrieves cost comparisons between time periods
- **GetCostComparisonDrivers**: Retrieves the drivers of cost changes between time periods

Cost Optimization Hub

Amazon Q Developer uses Cost Optimization Hub APIs to retrieve personalized cost optimization recommendations:

- **GetRecommendation**: Retrieves details for a specific recommendation

- **ListRecommendations**: Retrieves a list of recommendations with filtering options
- **ListRecommendationSummaries**: Retrieves summary information about recommendations

AWS Compute Optimizer

Amazon Q Developer uses Compute Optimizer APIs to retrieve resource optimization recommendations:

- **GetAutoScalingGroupRecommendations**: Retrieves rightsizing recommendations for Auto Scaling groups
- **GetEBSVolumeRecommendations**: Retrieves recommendations for EBS volumes
- **GetEC2InstanceRecommendations**: Retrieves rightsizing recommendations for EC2 instances
- **GetECSServiceRecommendations**: Retrieves recommendations for ECS services
- **GetRDSDatabaseRecommendations**: Retrieves recommendations for RDS databases
- **GetLambdaFunctionRecommendations**: Retrieves recommendations for Lambda functions
- **GetIdleRecommendations**: Retrieves recommendations for idle resources
- **GetLicenseRecommendations**: Retrieves recommendations for license optimization
- **GetEffectiveRecommendationPreferences**: Retrieves the effective recommendation preferences

AWS Budgets

Amazon Q Developer uses the Budgets API to retrieve information about your budget configurations and status:

- **DescribeBudgets**: Retrieves budget details including thresholds and actual spending

Free Tier

Amazon Q Developer uses Free Tier APIs to retrieve information about your free tier usage:

- **GetFreeTierUsage**: Retrieves your current free tier usage
- **GetAccountPlanState**: Retrieves information about your current account type and free tier eligibility
- **ListAccountActivities**: Retrieves a list of account activities you can take to earn additional free tier credits

- **GetAccountActivity**: Retrieves details of a specific account activity you can take to earn additional free tier credits

AWS Price List

Amazon Q Developer uses Price List APIs to retrieve public pricing information for AWS services:

- **DescribeServices**: Retrieves a list of available AWS services
- **GetAttributeValues**: Retrieves valid values for product attributes
- **GetProducts**: Retrieves pricing information for specific products

Calculation engine

Amazon Q Developer includes a flexible calculation engine that allows it to perform a wide range of calculations on your cost data. This capability enables it to provide deeper insights than simple data retrieval alone.

Types of calculations

Q can perform calculations including:

- **Period-over-period changes**: Calculate the difference in costs between two time periods, both in absolute terms and as a percentage change.
- **Unit economics**: Calculate metrics like cost per vCPU-hour, cost per GB-month of storage, or cost per API request.
- **Effective rates**: Calculate the effective cost per unit after applying discounts from Savings Plans or Reserved Instances.
- **Aggregations**: Sum, average, or find the minimum or maximum values across multiple dimensions.
- **Custom metrics**: Combine multiple data points to create custom metrics tailored to your question.

API transparency

With each response, Amazon Q Developer provides full transparency into how it retrieved and processed your data. This transparency helps you understand exactly what Q did to answer your

question and allows you to verify the results or provide more specific instructions in follow-up questions.

What Amazon Q Developer displays

For each response, Q shows you:

- **API calls made**: Q displays the name of each API it called to retrieve data.
- **Parameters used**: Q shows the exact parameters it used for each API call, including time ranges, filters, grouping dimensions, and any other relevant parameters.
- **Console deep-links**: Where applicable, Q provides links to matching views in the AWS Management Console. These links allow you to verify the data Q retrieved or explore the data further using the console's visualization and filtering capabilities.

Using transparency to refine your questions

The transparency that Q provides allows you to guide its behavior more effectively. For example:

- If Q retrieved data for the wrong time period, you can specify the exact dates you want in a follow-up question.
- If Q grouped costs by one tag key but you wanted them grouped by another, you can ask Q to regroup the data.

Limitations

Amazon Q Developer has the following limitations:

- **Pricing data**: The pricing and cost estimation capabilities only provide public pricing data from the AWS Price List APIs. Customer-specific discounts are not reflected in pricing estimates. Amazon Q Developer does not integrate with the AWS Pricing Calculator, so it cannot create or save workload estimates that reflect customer-specific discounts or pricing.
- **Savings Plans analysis**: Amazon Q Developer can provide Savings Plans recommendations and analyze your historical Savings Plans coverage and utilization. Q does not integrate with Savings Plans Purchase Analyzer, so it cannot model the impact of a specific Savings Plans purchase on savings, coverage, or utilization.
- **Mutating actions**: Amazon Q Developer can retrieve and analyze cost data, but cannot take mutating actions on your behalf, such as creating or modifying budgets, purchasing Savings Plans or Reserved Instances, or modifying Cost Management preferences.

Security for cost management capabilities in Amazon Q Developer

The following provides an overview of permissions and data protection for the cost management capabilities in Amazon Q Developer.

Permissions overview

To use the cost management capabilities in Amazon Q Developer, you need three sets of Identity and Access Management (IAM) permissions:

1. **Amazon Q permissions**: Permissions to chat with Amazon Q in the console (such as `q:StartConversation` and q:SendMessage)
2. **Service permissions**: Permissions to access the underlying Billing and Cost Management services that provide cost data
3. **PassRequest permission**: The `q:PassRequest` permission that allows Amazon Q to call AWS APIs on your behalf

The quickest way for an administrator to grant users access to Amazon Q Developer is to use the `AmazonQFullAccess` managed policy.

Permissions for cost management capabilities

The following IAM policy statement grants users access to all cost management capabilities in Amazon Q Developer:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAmazonQChatAndPassRequest",
            "Effect": "Allow",
            "Action": [
                "q:StartConversation",
                "q:SendMessage",
                "q:GetConversation",
                "q:ListConversations",
                "q:UpdateConversation",
                "q:DeleteConversation",
                "q:PassRequest"
            ],
```

```
            "Resource": "*"
        },
         {
            "Sid": "AllowCostExplorerAccess",
            "Effect": "Allow",
            "Action": [
                "ce:GetCostAndUsage",
                "ce:GetCostAndUsageWithResources",
                "ce:GetCostForecast",
                "ce:GetUsageForecast",
                "ce:GetTags",
                "ce:GetCostCategories",
                "ce:GetDimensionValues",
                "ce:GetSavingsPlansUtilization",
                "ce:GetSavingsPlansCoverage",
                "ce:GetSavingsPlansUtilizationDetails",
                "ce:GetReservationUtilization",
                "ce:GetReservationCoverage",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetRightsizingRecommendation",
                "ce:GetAnomalies",
               "ce:GetCostAndUsageComparisons",
               "ce:GetCostComparisonDrivers"
            ],
            "Resource": "*"
        },
         {
            "Sid": "AllowCostOptimizationHubAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries"
            ],
            "Resource": "*"
        },
         {
            "Sid": "AllowComputeOptimizerAccess",
            "Effect": "Allow",
            "Action": [
                "compute-optimizer:GetAutoScalingGroupRecommendations",
                "compute-optimizer:GetEBSVolumeRecommendations",
                "compute-optimizer:GetEC2InstanceRecommendations",
```

```
                "compute-optimizer:GetECSServiceRecommendations",
                "compute-optimizer:GetRDSDatabaseRecommendations",
                "compute-optimizer:GetLambdaFunctionRecommendations",
                "compute-optimizer:GetIdleRecommendations",
                "compute-optimizer:GetLicenseRecommendations",
                "compute-optimizer:GetEffectiveRecommendationPreferences"
            ],
            "Resource": "*"
        },
         {
            "Sid": "AllowBudgetsAccess",
            "Effect": "Allow",
            "Action": [
                "budgets:ViewBudget"
            ],
            "Resource": "*"
        },
         {
            "Sid": "AllowFreeTierAccess",
            "Effect": "Allow",
            "Action": [
                "freetier:GetFreeTierUsage",
                "freetier:GetAccountPlanState",
                "freetier:ListAccountActivities",
               "freetier:GetAccountActivity"
            ],
            "Resource": "*"
        },
         {
            "Sid": "AllowPricingAccess",
            "Effect": "Allow",
            "Action": [
                "pricing:GetProducts",
                "pricing:GetAttributeValues",
                "pricing:DescribeServices"
            ],
            "Resource": "*"
        }
    ]
}
```

You can scope down this policy to grant access to only specific cost management capabilities. For example, if you don't want users to access resource-level cost data, you can remove the `ce:GetCostAndUsageWithResources` action, or add an explicit deny statement.

q:PassRequest permission

`q:PassRequest` is an Amazon Q Developer permission that allows Amazon Q Developer to call AWS APIs on your behalf. When you add the `q:PassRequest` permission to an IAM identity, Amazon Q Developer gains permission to call any API that the IAM identity has permission to call. For example, if an IAM role has the `ce:GetCostAndUsage` permission and the `q:PassRequest` permission, Amazon Q Developer can call the GetCostAndUsage API when a user assuming that IAM role asks Amazon Q Developer to retrieve cost and usage data from Cost Explorer.

You can also allow IAM principals to access Cost Explorer and to use Amazon Q Developer, but restrict them from using the cost analysis or cost optimization capabilities in Amazon Q Developer, by using the `aws:CalledVia` global condition key. The following IAM policy provides an example of using this condition key:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "AllowQDeveloperAccess",
            "Effect": "Allow",
            "Action": [
                "q:StartConversation",
                "q:SendMessage",
                "q:GetConversation",
                "q:ListConversations",
                "q:PassRequest"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCostExplorerAccess",
            "Effect": "Allow",
            "Action": [
                "ce:*"
            ],
            "Resource": "*"
       },
        {
```

```
            "Sid": "DenyCostExplorerAccessViaAmazonQ",
             "Effect": "Deny",
             "Action": [
                 "ce:*"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "aws:CalledVia": [
                         "q.amazonaws.com"
                     ]
                 }
             }
         }
    ]
}
```

Multi-account access

For users of AWS Organizations, management account administrators can restrict member account users' access to Cost Explorer and Cost Optimization Hub data (including access to discounts, credits, and refunds) using the Cost Management preferences in the AWS Billing and Cost Management console. These preferences apply to Amazon Q Developer in the same way that they apply to the management console, SDK, and CLI. Amazon Q Developer respects the existing preferences of customers.

Cross-region calls

Data from the Cost Optimization Hub and Cost Explorer services is hosted in the US East (N. Virginia) Region. Data from AWS Compute Optimizer is hosted in the AWS Region where the underlying resources, such as EC2 instances, are located. Data served from the AWS Price List APIs is hosted in us-east-1, eu-central-1, and ap-south-1 (note that AWS Price List APIs do not serve any customer-specific data). Cost management requests in Amazon Q Developer may require cross-region calls. For more information, see Cross-region processing in Amazon Q Developer in the *Amazon Q Developer User Guide*.

Data protection

We may use certain content from Amazon Q Developer Free Tier for service improvement. Amazon Q Developer may use this content, for example, to provide better responses to common questions, fix Amazon Q Developer operational issues, for debugging, or for model training. Content that

AWS may use for service improvement includes, for example, your questions to Amazon Q Developer and the responses and code that Amazon Q Developer generates. We do not use content from Amazon Q Developer Pro or Amazon Q Business for service improvement.

The way you opt out of Amazon Q Developer Free Tier using content for service improvement depends on the environment where you use Amazon Q. For the AWS Management Console, AWS Console Mobile Application, AWS websites, and AWS Chatbot, configure an AI services opt-out policy in AWS Organizations. For more information, see AI services opt-out policies in the *AWS Organizations User Guide*.

Managing your costs with Savings Plans

Savings Plans offers a flexible pricing model that provides savings on AWS usage. Savings Plans provide savings beyond On-Demand rates in exchange for a commitment of using a specified amount of compute power (measured every hour) for a one or three year period. You can manage your plans by using recommendations, performance reporting, and budget alerts in AWS Cost Explorer.

For more information, see What is Savings Plans in the *Savings Plans User Guide*.

Using AWS Billing and Cost Management console with our new AWS experience

Warning

We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

When you sign up for AWS using Sign up for AWS (new), you use AWS Settings to set up your billing, create spend limits to control your costs, and retrieve and pay invoices. You use AWS Billing and Cost Management to create budgets, analyze, and optimize your costs.

Sign up for AWS (advanced) supports many features for billing and cost management, but some of them aren't required for customers who have an AWS environment with preconfigured defaults. The following table shows what you can do in the AWS Billing and Cost Management console, in the AWS Settings console, and what's not available for this experience. If you want to use any of the features that are not available, you need to Sign up for AWS (advanced), or activate advanced features for your account.

Included in the AWS Billing and Cost Management console	Included in AWS Settings	Not available in this experience
• Budgets • Cost Explorer • Cost Optimization Hub • Free Tier	• Invoices • Payment methods • Tax settings • Credits • Spend limits	• Savings Plans • Reserved Instances • Cost Anomaly Detection • Cost Categories • Data Exports / CUR • Billing and Cost Management Dashboards • Billing Views • Billing Conductor • Console Pricing Calculator

Included in the AWS Billing and Cost Management console	Included in AWS Settings	Not available in this experience
		• Carbon Footprint Tool • Budget Reports

Note

If you have active sessions for a project and for an IAM user, you might get redirected to the AWS Billing and Cost Management console. To use the AWS Billing and Cost Management console, sign out of any AWS account that you access as an IAM user.

Use a budget in the AWS Billing and Cost Management console

Warning

We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

The following information is about creating a budget in the AWS Billing and Cost Management console when you're using our new AWS experience. If you created your account using Sign up for AWS (advanced) or activated advanced features, see Managing your costs with AWS Budgets.

You can use AWS Budgets to enable cost and usage tracking. Some examples include:

- Setting a monthly cost budget with a fixed target amount to track all costs associated with your account.
- Setting a monthly cost budget with a variable target amount, assuming that each month, your budget should grow by 5 percent.
- Setting a custom period budget that aligns with your project duration or grant period.

You can create the following types of budgets:

- **Cost budgets**: Set limits for services and receive alerts when costs approach or exceed your defined threshold.
- **Usage budgets**: Establish usage limits for one or more services and get notified when usage approaches or exceeds your set threshold.
- **Spend limits**: Create a total monthly limit for each project you own. AWS will take cost-saving actions such as pausing unused resources to make sure your monthly costs never exceed your monthly limit. You can't create a spend limit in the AWS Billing and Cost Management console, but you can create one in AWS Settings. For more information, see Create a spend limit in AWS Settings.

Budget considerations

When creating a budget, consider the following:

- AWS Budgets information is updated up to three times a day. Updates typically occur 8–12 hours after the previous update.
- There can be a delay between when you incur a charge and when you receive a notification from AWS Budgets for the charge. This is due to a delay between when an AWS resource is used and when that resource usage is billed. You might incur additional costs or usage that exceed your budget notification threshold before AWS Budgets can notify you, and your actual costs or usage may continue to increase or decrease after you receive the notification.
- Budgets can track your blended, unblended, net unblended, amortized, and net amortized costs.
- Budgets can include or exclude charges such as discounts, refunds, support fees, and taxes.
- You can set up optional notifications that warn you if you exceed, or are forecasted to exceed, your budgeted amount for cost or usage budgets. You can have notifications sent to an Amazon SNS topic, to an email address, or to both. For more information, see Creating an Amazon SNS topic for budget notifications.
- Project team members can create budgets, but cannot create spend limits.
- A budget is visible to project team members.

Budget actions

Budget actions are actions run by AWS Budgets on your behalf. This could include sending a message, stopping the creation of a new resource, or performing a cost-saving action associated with a usage plan. You cannot create any new service control policies for your budget.

For more information about AWS Budgets actions, see Configuring budget actions.

Best practices

Use the following best practices when you're working with budgets.

Set budgets on a recurring basis

You can set budgets on a recurring basis or for a specific time frame. This gives you insight into your costs. This also makes sure you don't unexpectedly stop receiving budget alerts.

Use custom period budgets

You can set a start and end date for your budgeting cycle. Use a custom period budget for your project duration or grant period and combine them with other budget types. When you use a custom budget, consider the following:

- The end date of your budgeting cycle must be within three years of the start date.
- For amount calculations, only the date (00:00 UTC) is used. The end date is excluded from calculations.
- Custom period budgets don't auto-renew and expire on the end date.

Use advanced options when you need them

Cost budgets can be aggregated by blended, unblended, net unblended, amortized, or net amortized costs. Cost budgets can also include or exclude refunds, credits, taxes, and support charges. Create a budget that uses the financial information you care about.

Set budget alerts

Send budget alerts to places you regularly access to stay on top of your costs.

When you set budget alerts, consider the following:

- You can send budget alerts to up to 10 email addresses and one Amazon SNS topic.
- You can create alerts for actual values or forecasted values.
- Actual alerts are only sent once per budget, per budget period.

- Forecasted-based alerts can be sent out more than once per budget, per budget period. This is because forecasted values can change.
- AWS requires 5 weeks of usage data to generate budget forecasts. Any forecasted-based alerts won't be sent out until AWS has enough historical information.

Send your budget alerts to an Amazon SNS topic

You can send your budget alert to an Amazon SNS topic to deliver the alert message to multiple subscribers, including Lambda functions, SMS text messages, and service providers like Datadog or Splunk.

For budget notifications to be sent successfully, your budget must have permissions to send a notification to your topic, and you must accept the subscription to the Amazon SNS notification topic. For more information, see Creating an Amazon SNS topic for budget notifications.

Tag your budgets

You can use tags to help organize your AWS Budgets resources. You can add, update, or remove tags from your AWS Budgets resources at any time. If you create a tag, you won't see it in any cost or usage data.

Create a spend limit in AWS Settings

You can create a spend limit to set the most you'll ever pay per month for each project. This feature is only available using the AWS Settings console, but you can view your spend limit and service-related costs in the AWS Billing and Cost Management console. Anyone with access to a project can view a spend limit, but only project owners can modify them. Your account must be on the Paid Plan to access a spend limit. For more information, see Upgrade your account in AWS Settings.

Create a budget in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can create budgets for each project to track and take action on your costs and usage. In the AWS Billing and Cost Management console, you can create cost budgets and usage budgets, but

you cannot create spend limits. For more information about budgets, see Use a budget in the AWS Billing and Cost Management console.

When you create a budget, AWS Budgets creates a graph to help you see your costs. It can take up to 24 hours for this graph to appear.

To create a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets**.
3. For **Budget monitoring**, choose **Create budget**.
4. For **Budget setup**, choose a setup type. We recommend that you use a template budget.
   - If you choose **Use a template (simplified)**, do the following:
     a. Choose a template.
     b. For **Budget name**, enter a name for your budget.
     c. For **Email recipients**, enter up to 10 email recipients you want to notify when this project exceeds your budget.
     d. Choose **Create**.

     You can change the default configuration, like which services are included in the budget after your budget is created.
   - If you choose **Customize (advanced)**, follow the instructions for Creating a cost budget or Creating a usage budget based on your budget type.

Update a budget in the AWS Billing and Cost Management console

> **Warning**
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can update a budget at any time. When you update a budget, your changes are saved immediately, but budget calculations refresh up to three times a day. If you created a budget using a template, you'll need to update the budget to change the default configuration.

The following procedure shows how to update a zero spend budget to only create alerts for costs associated with S3.

To update a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Budgets**.
3. Choose your budget and then choose **Edit**.
4. For **Budget scope**, choose **Filter specific AWS cost dimensions**.
5. For **Filters**, choose **Add filter**.
6. For **Dimension**, select **Service**.
7. For **Values**, select **S3 (Simple Storage Service)**.
8. Choose **Apply Filter**.
9. Choose **Next**.
10. (Optional) Modify the alerts if necessary.
11. Choose **Next** and then choose **Next**.
12. Choose **Save**.

Budget methods in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

The following information is about budget methods in the AWS Billing and Cost Management console for our new AWS experience. A budget method is how you set your budget. Your budget doesn't need to be USD 30 per month but can reflect the flexibility in your growth and development.

Fixed

A fixed budget lets you monitor the same amount every budget period.

Planned

A planned budget lets you set a different amount to monitor each month or quarter.

With a planned budget, you can set the budget amount for up to 12 months or 4 quarters. After 12 months or 4 quarters, your budget amount is fixed at the last budget amount.

Auto-adjusting

An auto-adjusting budget dynamically sets your budget amount based on your spending or usage over a time range that you specify.

The historical or forecast time range that you select is the auto-adjustment baseline for your budget.

At the beginning of each new period, AWS Budgets calculates your budget amount from your cost or usage data within the baseline time range. If AWS Budgets updates your budget, all budget alert notification subscribers get a notification that the budget amount changed.

When using auto-adjusting budgets, consider the following:

- AWS Budgets doesn't include periods at the beginning of your baseline time range that don't have cost or usage data. This might impact your budget amount.
- You see a temporary forecast while you're creating or editing a budget. After you save your budget, your auto-adjusted budget is set for the first time.

Budget filters in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

The following information is about budget filters in the AWS Billing and Cost Management console for our new AWS experience. You can use the following budget filters.

API operation

Choose an action, such as `CreateBucket`.

Availability zone

Choose the Availability Zone in which the resource that you want to create a budget for is running.

Billing entity

Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services.

Charge type

Different types of charges or fees.

- **Credit**: Any AWS credits that are applied to your account.
- **Other out-of-cycle charges**: Any subscription charges that aren't upfront reservation charges or support charges.
- **Refund**: Any refunds that you received. Refunds are listed as a separate line item in the data table. They don't appear as an item in the chart because they represent a negative value in the calculation of your costs. The chart displays only positive values.
- **Reservation applied usage**: Usage that AWS applied reservation discounts to.
- **Support fee**:
- **Tax**: Any taxes that are associated with the charges or fees in your cost chart.
- **Usage**: Usage that AWS didn't apply reservation discounts to.

Instance family

Choose the family of instances to track using this budget.

Instance type

Choose the type of instance that you want to track with this budget.

Invoicing entity

The AWS entity that issues the invoice. Possible values include:

- **Amazon Web Services, Inc.** – The entity that issues invoices to customer globally, where applicable.
- **Amazon Web Services India Private Limited** – The entity that issues invoices to customers based in India.
- **Amazon Web Services South Africa Proprietary Limited** – The entity that issues invoices to customers in South Africa.

Legal entity

The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. The values might differ for third-party AWS Marketplace transactions. Possible values include:

- **Amazon Web Services, Inc.** – The entity that sells AWS services.
- **Amazon Web Services India Private Limited** – The local Indian entity that acts as a reseller for AWS services in India.

> **Note**
>
> Amazon Web Services EMEA SARL is the marketplace operator for your purchases if your account is located in EMEA (excluding Turkey and South Africa), and the seller is eligible in EMEA. Purchases include subscriptions. Amazon Web Services, Inc. is the marketplace operator for purchases if the seller isn't eligible for EMEA. For more information, see AWS Europe.

Purchase option

Choose `On Demand Instances`, `Standard Reserved Instances`, or `Savings Plans`.

Service

Choose an AWS service. This is only supported for cost budgets.

Tag

If you activated any tags, choose a resource tag. A tag is a label that you can use to organize your resource costs and track them on a detailed level.

Usage type

Usage types are the units each service uses to measure the usage for specific types of resources. If you choose a filter such as S3 and then choose a usage type value, such as DataTransfer-Out-Bytes (GB), your costs are limited to S3 DataTransfer-Out-Bytes (GB).

You can create a usage budget only for a specific unit of measure. If you choose Usage type but not Usage type group, the budget monitors all of the available units of measure for the usage type.

Usage type group

A usage type group is a collection of usage types that have the same unit of measure. If you choose both the Usage type group and the Usage type filters, Cost Explorer shows you usage types that are automatically constrained to the group unit of measure. For example, assume you choose the group EC2: Running Hours (Hrs), and then choose the EC2-Instances filter for Usage type. Cost Explorer shows you only the usage types that are measured in hours.

View your budget in the AWS Billing and Cost Management console

Warning

We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can view all your budgets, including spend limits in the AWS Billing and Cost Management console. AWS Budgets information is updated up to three times a day. There can be a delay between when you incur a charge and when you receive a notification from AWS Budgets for the charge. This is due to a delay between when an AWS resource is used and when that resource usage is billed. You might incur additional costs or usage that exceed your budget notification threshold before AWS Budgets can notify you, and your actual costs or usage may continue to increase or decrease after you receive the notification.

Both project owners and project team members can view budgets.

View your budget

You can view your budget in two ways. First, you can choose the checkbox next to your budget to open the split-view panel. Second, you can choose the budget name to open the budget details page.

View your budget using the split-view panel

To view your budget using the split-view panel, choose the checkbox next to your budget. You'll have access to the following:

- **Budget preview.** Your budget preview shows a filterable table with the following:

- Current costs and usage for a budget during the budget period.
- Budgeted costs or usage for the budget period.
- Forecasted usage or costs for the budget period.
- Indicators of when your alerts will be triggered.

- **Alerts.** Your alerts are listed with any notifications or information about the state of your budget.

View your budget in the budget details page

To view your budget using the budget details page, choose your budget name to open the budget details page. You'll have access to the following:

- **Budget health**: This is the overall state of your budget. This includes two key values:
  - **Current vs. budgeted** – Your current incurred costs compared to your budgeted costs.
  - **Forecasted vs. budgeted** – Your current forecasted costs compared to your budgeted costs.
- **Alerts**: Your alerts are listed with any notifications or budget actions that AWS Budgets might take on your resources. You can choose **View all alerts** to open the Alerts tab to edit or delete alerts.
- **Details**: This shows the budget type, amount, and additional parameters for your budget.
- **Budget history**: This chart and table show the history of your budget. This history is only supported for quarterly budgets which show the last four quarters of history and monthly budgets which show the last 12 months of budget history.

  If you have a custom time period for your budget, if you have multi-year data disabled, you can view up to 14 months of historical data.
- **Tags**: You can view or add tags associated with your budget.

Download your data in a CSV file

You can download your budgets as a CSV file. The file includes all of the data for all of your budgets, such as Budget Name, Current Value and Forecasted Value, Budgeted Value, and more.

To download a budget

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/cost-management/.

2. On the navigation pane, choose **Budgets**.
3. Choose **Download CSV**.
4. Open or save your file.

Use Cost Explorer in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

The following information is about using Cost Explorer in the AWS Billing and Cost Management console when you're using our new AWS experience. If you created your account using Sign up for AWS (advanced) or activated advanced features, see Analyzing your costs and usage with Cost Explorer.

You can view and analyze your costs and usage with Cost Explorer. You can view your costs in three unique cost and usage graphs, and you can compare usage across a variety of dimensions and forecast your future spending. Cost Explorer is also available programmatically. For more information about the AWS Cost Explorer API, see the AWS Billing and Cost Management API Reference.

Forecasting your data for Cost Explorer with our new AWS experience

A forecast is a prediction of how much you will use AWS services over the forecast time period that you selected. This forecast is based on your past usage. You can use a forecast to estimate your AWS bill and set alarms and budgets for based on predictions. Because forecasts are predictions, the forecasted billing amounts are estimated and might differ from your actual charges for each statement period.

Like weather forecasts, billing forecasts can vary in accuracy. Different ranges of accuracy have different prediction intervals. The higher the prediction interval, the more likely the forecast has a wider range. For example, suppose that you have a budget set to 100 dollars for a given month. An 80% prediction interval might forecast your spend between 90 and 100, with a mean of 95. The range in the prediction band is dependent on your historical spend volatility, or fluctuations. The

more consistent and predictable the historical spend, the narrower the prediction range in forecast spend.

Cost Explorer forecasts have a prediction interval of 80%. If AWS doesn't have enough data to forecast an 80% prediction interval, Cost Explorer doesn't provide a forecast. This is common for accounts that have less than one full billing cycle.

Considerations

When using Cost Explorer when you're using our new AWS experience, consider the following:

- You can access your cost data using the Cost Explorer API. Each paginated API request results in a charge of $0.01. Because you're charged per paginated request, identify the exact dataset you want to access before submitting queries. If you're using an AI agent to access the Cost Explorer API, make sure it is aware of the $0.01 charge.
- AWS prepares data for the current month, previous 13 months, and forecasts cost data for the next 12 months.
- It takes AWS about 24 hours to prepare your current month's data. It takes AWS a few more days to complete the preparation for your previous and forecasted data.
- You can only view Cost Explorer data for one project at a time.
- All costs reflect your usage up to the previous day.
- In the current billing period, the data depends on your upstream data from your billing applications, and some data might be updated later than 24 hours.
- Data transfer costs are included in the services that they're associated with, such as Amazon EC2 or Amazon S3. They aren't represented as either a separate line item in the data table or a bar in the chart.
- If you choose any forecasted dates, your current date's cost and usage data shows as Forecast and won't include historical data.

Because you're using our new AWS experience, we provide a streamlined version of the Cost Explorer console that helps you understand your costs and usage. Features that aren't covered in the following documentation are not available for our new AWS experience customers.

Topics

- Access your cost data in the AWS Billing and Cost Management console
- Explore your data in the AWS Billing and Cost Management console

- Filter your data in the AWS Billing and Cost Management console
- Download the cost data CSV file in the AWS Billing and Cost Management console
- Ask questions about your costs using Amazon Q Developer in the AWS Billing and Cost Management console
- Cost comparisons in the AWS Billing and Cost Management console
- Troubleshoot Cost Explorer in the AWS Billing and Cost Management console

Access your cost data in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can access your cost data using the AWS Console or using AWS Settings. When you use AWS Settings, you can see the total monthly spend of all projects you have access to. When you use the AWS Console, you can only see the project you're currently in. To switch between projects, use the menu at the top right of the page.

The data you see in AWS Settings and in Cost Explorer are refreshed at least once per day. The cadence when they're refreshed might differ. This can result in differences for your month-to-date estimated charges in AWS Settings and the Cost Management Console.

To access your cost data using AWS Settings

1. Open AWS Settings at https://settings.aws.com.
2. In the main navigation pane, choose **Billing**.

   You'll see the monthly spend of all your projects.
3. For cost per project, under **Inspect costs**, choose **View**.

To access your cost data using AWS Billing and Cost Management console

- Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.

You'll be directed to the Cost Explorer page.

Explore your data in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can use Cost Explorer to explore your cost data for a project. The Cost dashboard gives you insights into your cost and usage overview, lets you explore your costs with AI, and provides you with two visual tools to understand your cost. The following documentation explains how to use these two visual tools.

Use the cost and usage graph to explore your data

The first visual tool is the cost and usage graph (). This chart has three views to understand your cost data:

- Bar charts
- Stacked bar charts
- Line graphs

You can set the style by choosing one of the views in the top corner of the chart.

You can also choose to view your cost data in time frequencies, or levels of granularity. The following levels of granularity are supported in Universal Coordinated Time (UTC):

- **Monthly** – these are defined as calendar months.
- **Daily** – these are defined as 12:00:00 to 11:59:59 PM.

You can use preconfigured time ranges or set custom time frames.

We also provide some relative auto-selected time ranges that are useful to understand your cost. If you choose any future times, your data will be forecasted. For more information, see the section called “Forecasting your data for Cost Explorer with our new AWS experience”.

The cost and usage graph lets you filter your data to gain additional insights. For more information about supported filters and how to filter your data, see Filter your data in the AWS Billing and Cost Management console.

Group your data to find cost patterns

To gain further insight into your data, you can group it in various dimensions. For instance, if you group your data by tags, you might see all resources tagged Prod have a higher cost compared to the rest of your resources. It might make sense for those resources to have a greater cost, and Cost Explorer can help you understand your costs. If you group your data, forecasting is not available.

Use the Cost Explorer data table to explore your data

The second visual tool is the cost and usage breakdown. This breakdown represents whatever view you've created for the cost and usage graph. This lets you directly read the costs figures without having to navigate on the chart. Data transfer costs are included in the services that they're associated with, such as Amazon EC2 or Amazon S3. They aren't represented as a separate line item on this table.

You can download the .csv file that contains the complete data set for your chart. For more information, see Download the cost data CSV file in the AWS Billing and Cost Management console.

Filter your data in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

With Cost Explorer, you can filter how you view your AWS costs by one or more of the following values:

- API operation
- Availability Zone
- Billing entity
- Charge type
- Include all

- Instance type
- Legal entity
- Linked account
- Platform
- Purchase option
- Region
- Resources
- Service
- Tag
- Tenancy
- Usage type
- Usage type group

You can use Cost Explorer to see which service you use the most or apply multiple filters to look at intersecting datasets.

The following procedure shows you how to filter your cost and usage graph based on DynamoDB usage only.

To filter your data

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. For **Filters**, choose a **Service**, and then select **DynamoDB**.

   You can filter by entering DynamoDB in the search box.
3. Choose **Apply**.

To save this view, use your browser's bookmark feature to save your settings. If your view has a forecast, it won't be saved, and instead Cost Explorer displays the most recent forecast when you revisit your saved chart.

Use multiple filters to show data in common

You can combine filters to show data in common. You can use up to 1024 filters in Cost Explorer.

When you select multiple filters, Cost Explorer uses AND. This means if you filter for service of Amazon EC2 and tag of Prod, only data about Amazon EC2 resources tagged with the Prod tag is shown. When you select multiple values within a filter, Cost Explorer uses OR.

Filter and group options

In Cost Explorer, you can filter by the following groups. Note that these are not the same filters as filtering the data that you want to view.

API operation

Requests made to and tasks performed by a service, such as write and get requests to Amazon S3.

Availability Zone

Distinct locations within a Region that are insulated from failures in other Availability Zones. They provide inexpensive, low-latency network connectivity to other Availability Zones in the same Region.

Billing entity

Helps you identify whether your invoices or transactions are for AWS Marketplace or for purchases of other AWS services.

Charge type

Different types of charges or fees.

- **Credit**: Any AWS credits that are applied to your account.
- **Other out-of-cycle charges**: Any subscription charges that aren't upfront reservation charges or support charges.
- **Refund**: Any refunds that you received. Refunds are listed as a separate line item in the data table. They don't appear as an item in the chart because they represent a negative value in the calculation of your costs. The chart displays only positive values.
- **Reservation applied usage**: Usage that AWS applied reservation discounts to.
- **Tax**: Any taxes that are associated with the charges or fees in your cost chart. Cost Explorer adds all taxes together as a single component of your costs. If you select five or fewer filters, Cost Explorer displays your tax expenses as a single bar. If you select six or more filters, Cost Explorer displays five bars, stacks, or lines, and then aggregates all remaining items, including taxes, into a sixth bar, stack slice, or plot line that's labeled Other.

Cost Explorer displays your tax costs in the chart only when you choose Monthly drop down.

- **Usage**: Usage that AWS didn't apply reservation discounts to.

Instance type

The type of RI that you specified when you launched an Amazon EC2 host, Amazon RDS instance class, Amazon Redshift node, or Amazon ElastiCache node. The instance type determines the hardware of the computer used to host your instance.

Legal entity

The Seller of Record of a specific product or service. In most cases, the invoicing entity and legal entity are the same. Possible values include:

- **Amazon Web Services, Inc.** – The entity that sells AWS services.
- **Amazon Web Services India Private Limited** – The local Indian entity that acts as a reseller for AWS services in India.

Linked account

The member accounts in an organization.

Platform

The operating system that your RI runs on. Platform is either Linux or Windows.

Purchase option

The method you choose to pay for your Amazon EC2 instances. This includes Reserved Instances, Spot Instances, Scheduled Reserved Instances, and On-Demand Instances.

Region

The geographic areas where AWS hosts your resources.

Resources

The unique identifier for your resources.

Service

AWS products. To learn what's available, see AWS Products and Services.

Tag

A label that you can use to track the costs associated with specific areas or entities within your business.

Tenancy

Specifies if the Amazon EC2 instance is hosted on shared or single-tenant hardware. Some tenancy values include Shared (Default), Dedicated, and Host.

Usage type

Usage types are the units that each service uses to measure the usage of a specific type of resource. For example, the `BoxUsage:t2.micro(Hrs)` usage type filters by the running hours of Amazon EC2 t2.micro instances.

Usage type group

Usage type groups are filters that collect a specific category of usage type filters into one filter. For example, `BoxUsage:c1.medium(Hrs)`, `BoxUsage:m3.xlarge(Hrs)`, and `BoxUsage:t1.micro(Hrs)` are all filters for Amazon EC2 instance running hours, so they are collected into the EC2: Running Hours filter.

Usage type groups are available for DynamoDB, Amazon EC2, ElastiCache, Amazon RDS, Amazon Redshift, and Amazon S3. The specific groups available to your account depend on what services you've used. The list of groups that might be available includes but isn't limited to the following:

DDB: Data Transfer - Internet (In)

Filters by the costs associated with how many GB are transferred to your DynamoDB databases.

DDB: Data Transfer - Internet (Out)

Filters by the costs associated with how many GB are transferred from your DynamoDB databases.

DDB: Indexed Data Storage

Filters by the costs associated with how many GB that you have stored in DynamoDB.

DDB: Provisioned Throughput Capacity - Read

Filters by the costs associated with how many units of read capacity that your DynamoDB databases used.

DDB: Provisioned Throughput Capacity - Write

Filters by the costs associated with how many units of write capacity that your DynamoDB databases used.

EC2: CloudWatch - Alarms

Filters by the costs associated with how many CloudWatch alarms that you have.

EC2: CloudWatch - Metrics

Filters by the costs associated with how many CloudWatch metrics that you have.

EC2: CloudWatch - Requests

Filters by the costs associated with how many CloudWatch requests that you make.

EC2: Data Transfer - CloudFront (Out)

Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a CloudFront distribution.

EC2: Data Transfer - CloudFront (In)

Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a CloudFront distribution.

EC2: Data Transfer - Inter AZ

Filters by the costs associated with how many GB are transferred into, out of, or between your Amazon EC2 instances in different AZs.

EC2: Data Transfer - Internet (In)

Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from outside the AWS network.

EC2: Data Transfer - Internet (Out)

Filters by the costs associated with how many GB are transferred from an Amazon EC2 instance to a host outside the AWS network.

EC2: Data Transfer - Region to Region (In)

Filters by the costs associated with how many GB are transferred to your Amazon EC2 instances from a different AWS Region.

EC2: Data Transfer - Region to Region (Out)

Filters by the costs associated with how many GB are transferred from your Amazon EC2 instances to a different AWS Region.

EC2: EBS - I/O Requests

Filters by the costs associated with how many I/O requests that you make to your Amazon EBS volumes.

EC2: EBS - Magnetic

Filters by the costs associated with how many GB that you have stored on Amazon EBS Magnetic volumes.

EC2: EBS - Provisioned IOPS

Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon EBS.

EC2: EBS - SSD(gp2)

Filters by the costs associated with how many GB per month of General Purpose storage that your Amazon EBS volumes use.

EC2: EBS - SSD(io1)

Filters by the costs associated with how many GB per month of Provisioned IOPS SSD storage that your Amazon EBS volumes use.

EC2: EBS - Snapshots

Filters by the costs associated with how many GB per month that your Amazon EBS snapshots store.

EC2: EBS - Optimized

Filters by the costs associated with how many MB per instance hour that your Amazon EBS-optimized instances use.

EC2: ELB - Running Hours

Filters by the costs associated with how many hours that your Elastic Load Balancing load balancers ran.

EC2: Elastic IP - Additional Address

Filters by the costs associated with how many Elastic IP addresses that you attached to running Amazon EC2 instances.

EC2: Elastic IP - Idle Address

Filters by the costs associated with Elastic IP addresses that you have that aren't attached to running Amazon EC2 instances.

EC2: NAT Gateway - Data Processed

Filters by the costs associated with how many GB that your network address translation gateways (NAT gateways) processed.

EC2: NAT Gateway - Running Hours

Filters by the costs associated with how many hours that your NAT gateways ran.

EC2: Running Hours

Filters by the costs associated with how many hours that your Amazon EC2 instances ran.

This Usage Type Group contains only the following Usage Types:

- BoxUsage
- DedicatedUsage
- HostBoxUsage
- HostUsage
- ReservedHostUsage
- SchedUsage
- SpotUsage
- UnusedBox

ElastiCache: Running Hours

Filters by the costs associated with how many hours that your Amazon ElastiCache nodes ran.

ElastiCache: Storage

Filters by the costs associated with how many GB that you stored in Amazon ElastiCache.

RDS: Running Hours

Filters by the costs associated with how many hours that your Amazon RDS databases ran.

This Usage Type Group contains only the following Usage Types:

- AlwaysOnUsage
- BoxUsage
- DedicatedUsage
- HighUsage
- InstanceUsage
- MirrorUsage
- Multi-AZUsage
- SpotUsage

RDS: Data Transfer – CloudFront – In

Filters by the costs associated with how many GB are transferred into Amazon RDS from a CloudFront distribution.

RDS: Data Transfer – CloudFront – Out

Filters by the costs associated with how many GB are transferred from a CloudFront distribution to Amazon RDS data transfers.

RDS: Data Transfer – Direct Connect Locations – In

Filters by the costs associated with how many GB are transferred into Amazon RDS through a Direct Connect network connection.

RDS: Data Transfer – Direct Connect Locations – Out

Filters by the costs associated with how many GB are transferred from Amazon RDS through a Direct Connect network connection.

RDS: Data Transfer – InterAZ

Filters by the costs associated with how many GB are transferred into, out of, or between Amazon RDS buckets in different Availability Zones.

RDS: Data Transfer – Internet – In

Filters by the costs associated with how many GB are transferred to your Amazon RDS databases.

RDS: Data Transfer – Internet – Out

Filters by the costs associated with how many GB are transferred from your Amazon RDS databases.

RDS: Data Transfer – Region to Region – In

Filters by the costs associated with how many GB are transferred to your Amazon RDS instances from a different AWS Region.

RDS: Data Transfer – Region to Region – Out

Filters by the costs associated with how many GB are transferred from your Amazon RDS instances to a different AWS Region.

RDS: I/O Requests

Filters by the costs associated with how many I/O requests that you make to your Amazon RDS instance.

RDS: Provisioned IOPS

Filters by the costs associated with how many IOPS-months that you have provisioned for Amazon RDS.

RDS: Storage

Filters by the costs associated with how many GB that you have stored in Amazon RDS.

Redshift: DataScanned

Filters by the costs associated with how many GB that your Amazon Redshift nodes scanned.

Redshift: Running Hours

Filters by the costs associated with how many hours that your Amazon Redshift nodes ran.

S3: API Requests - Standard

Filters by the costs associated with GET and all other standard storage Amazon S3 requests.

S3: Data Transfer - CloudFront (In)

Filters by the costs associated with how many GB are transferred into Amazon S3 from a CloudFront distribution.

S3: Data Transfer - CloudFront (Out)

Filters by costs associated with how many GB are transferred from a CloudFront distribution to Amazon S3 data transfers, such as how much data was uploaded from your Amazon S3 bucket to your CloudFront distribution.

S3: Data Transfer - Inter AZ

Filters by the costs associated with how many GB are transferred into, out of, or between Amazon S3 buckets in different Availability Zones.

S3: Data Transfer - Internet (In)

Filters by the costs associated with how many GB are transferred to an Amazon S3 bucket from outside the AWS network.

S3: Data Transfer - Internet (Out)

Filters by the costs associated with how many GB are transferred from an Amazon S3 bucket to a host outside the AWS network.

S3: Data Transfer - Region to Region (In)

Filters by the costs associated with how many GB are transferred to Amazon S3 from a different AWS Region.

S3: Data Transfer - Region to Region (Out)

Filters by the costs associated with how many GB are transferred from Amazon S3 to a different AWS Region.

S3: Storage - Standard

Filters by the costs associated with how many GB that you have stored in Amazon S3.

Download the cost data CSV file in the AWS Billing and Cost Management console

Warning

We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

To review your entire cost data in comprehensive detail, or to analyze it using other formats, you can download a comma-separated values (CSV) file of your cost data.

When you download a .csv file, the file's columns represent cost and the rows represent time. The file data shows up to 15 decimal places of precision, and dates are represented in YYYY-MM-DD format.

To download a .csv file

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Create a Cost Explorer view that you want to download to a CSV file.
3. Choose **Download as CSV**.

Ask questions about your costs using Amazon Q Developer in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

Cost Explorer lets you ask questions about your AWS costs. You can use suggested prompts or ask in your own words. When you ask a question, Amazon Q Developer opens a new chat panel in the console, and Cost Explorer can automatically update charts and report parameters.

Amazon Q Developer draws from extensive knowledge beyond what is visible in your current Cost Explorer view, including pricing data and budget information, to provide richer context and more comprehensive answers. If a follow-up question produces a visualization that Cost Explorer can display, it updates automatically. Otherwise, the visualization appears in Amazon Q Developer's artifacts panel while insights continue in the chat.

Use suggested prompts

Cost Explorer displays suggested prompts above your Cost & Usage Overview data. These prompts surface the most commonly asked cost questions.

When you choose a suggested prompt, the following occurs:

- The Amazon Q Developer chat panel opens automatically.

- The prompt is submitted to Amazon Q Developer without requiring additional input.
- Amazon Q Developer generates detailed insights in the chat panel.
- Cost Explorer refreshes with the corresponding visualization, and all report parameters including filters, groupings, and date ranges are automatically configured in the Report Parameters panel.

Use the Ask question button

If you have a question that goes beyond our suggested prompts, choose **Ask question** to open a chat panel. You can ask a question in this panel.

Cost comparisons in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can create cost comparisons using Cost Explorer to understand changes in your AWS spending. Use Cost Comparisons to analyze cost variations between months and get cost comparison drivers. Cost comparison drivers explain the reason behind these variations. For instance, a cost comparison driver might be that there was a 5% increase in cost for DynamoDB due to an increase in ReadCapacity from 50,000 to 70,000. This means you read from your DynamoDB table more frequently that month. This might indicate an increase in customers for your service, or an issue in your service architecture. As a developer, it's your job to understand why these cost drivers occur.

Use cost comparison

Use Cost Comparison to compare two months, a baseline and comparison month, in the following two ways:

Query for any two months across any Cost Explorer dimension and cost metric. Cost Comparison analyzes your costs by:

- Calculating the total cost for each selected dimension in the baseline month.
- Comparing these with costs in the comparison month.
- Ranking the dimension values by the absolute cost difference.

- Returning the top 10 increases or decreases for each dimension.

The following procedure shows you how to create a cost comparison for Lambda, Amazon EC2, and DynamoDB over two months.

To create a cost comparison

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the right pane, under **Report parameters**, choose **Compare**.
3. For **Date Range**, keep **Month over month**.
4. For **Group by**, choose **Service**.
5. For **Filters**, choose **Service**, and then choose **DynamoDB** and **Lambda**.
6. Choose **Apply**.

Request detailed cost drivers for the cost change associated with a specific dimension value. Cost Comparison gathers these cost drivers by:

- Identifying the specific usage type driving the largest change.
- Calculating the total cost for each charge type in the baseline and comparison months.
- Ranking the results by absolute cost difference.
- Returning a breakdown of cost changes for each charge type.

Troubleshoot Cost Explorer in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

The following troubleshooting content can help you resolve issues with Cost Explorer.

If you receive a data threshold error

Cost Explorer supports up to 500 million usage records for resource-level data at daily granularity. If you receive this error, your filtering has used too many usage records. Reduce the number of services you want to use for resource-level filtering.

If AWS does not forecast your future cost or usage

AWS requires enough data to construct an 80% prediction interval. If you do not see a forecast, your project does not have enough data. This often happens for projects that have not been open for a full billing cycle.

There is an inconsistency between my billing data and what is shown on Cost Explorer

In the current billing period, the data depends on your upstream data from your billing applications. Some data might be updated later than 24 hours. Slight inconsistencies between billing data and Cost Explorer can be expected.

View your savings opportunities in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

Cost Optimization Hub is not supported for the Free Tier of our new AWS experience. When you upgrade to the Paid Plan, Cost Optimization Hub is automatically turned on for your account. For more information, see Upgrade your account in AWS Settings.

Cost Optimization Hub shows idle resources that you can delete for savings opportunities. You can choose individual resources to find more information or export your savings opportunities.

Cost Optimization Hub provides information about the savings opportunity:

- **Estimated cost (before discounts)**: The savings estimate using AWS public (On-Demand) pricing without incorporating any discounts.

- **Estimated other discounts**: Estimated other discounts include all discounts that are not itemized, which includes Free Tier.
- **Estimated cost (after discounts)**: The savings estimate incorporating all discounts with AWS.
- **Estimated monthly savings**: The estimated monthly savings amount for the recommendation. This is calculated by dividing the aggregated estimated monthly savings of your cost optimization opportunities by your amortized monthly AWS costs, exclusive of credits and refunds. The estimated monthly savings is a quick approximation of your future savings. Any actual savings are dependent on your future AWS usage.
- **Estimated savings percentage**: The estimated savings percentage relative to the total cost.

We also provide information such as the resource ID, usage, and any tags associated with the resource.

Supported resources

The following resources are supported:

- Amazon Elastic Compute Cloud (Amazon EC2) instances
- Amazon EC2 Auto Scaling groups
- Amazon Elastic Block Store (Amazon EBS) volumes
- Amazon Elastic Container Service (Amazon ECS) tasks on AWS Fargate
- Amazon Relational Database Service DB instances
- NAT Gateway
- Amazon DynamoDB table
- ElastiCache cluster
- SageMaker endpoint
- MemoryDB cluster
- DocumentDB cluster

When you group related recommendations, Cost Optimization Hub identifies recommended actions that interact with each other, and it reduces estimated aggregated savings based on the degree of overlap. Cost Optimization Hub deduplicates amongst resource optimization strategies and proposes the recommendation with the highest savings. It also considers the reduction in usage by implementing the recommendations.

To find and delete an idle resource

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.

   The cost optimization hub will show your savings opportunities.
3. Choose a resource.

   The cost optimization hub will open a panel that provides more information about your resource.
4. Under **Estimated savings**, choose **Open in Service Console**.

   You'll be directed to the service console where you can delete the resource.

Download your recommendations in the AWS Billing and Cost Management console

> **Warning**
>
> We're currently releasing our new experience to a limited number of customers. You might not be able to access this experience yet.

You can download your recommendations. The maximum file size for a download is 350 MB. If you have more than 350 MB of recommendation data, you can't download your information.

To download your recommendations

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. In the navigation pane, choose **Cost Optimization Hub**.
3. At the bottom of the **Savings opportunities** page, choose **Download as CSV**.

Security in AWS Cost Management

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Cost Management, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Billing and Cost Management. The following topics show you how to configure Billing and Cost Management to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Billing and Cost Management resources.

Topics

- Data protection in AWS Cost Management
- Identity and Access Management for AWS Cost Management
- Logging and monitoring in AWS Cost Management
- Compliance validation for AWS Cost Management
- Resilience in AWS Cost Management
- Infrastructure security in AWS Cost Management

Data protection in AWS Cost Management

The AWS shared responsibility model applies to data protection in AWS Cost Management. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see Data Privacy FAQ. For information about data protection in Europe, see the General Data Protection Regulation (GDPR) Center.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with AWS Cost Management or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Identity and Access Management for AWS Cost Management

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS Cost Management resources. IAM is an AWS service that you can use with no additional charge.

Topics

- User types and billing permissions
- Audience
- Authenticating with identities
- Managing access using policies
- Overview of managing access permissions
- How AWS Cost Management works with IAM
- Identity-based policy examples for AWS Cost Management
- Using identity-based policies (IAM policies) for AWS Cost Management
- AWS Cost Management policy examples
- Migrating access control for AWS Cost Management
- Cross-service confused deputy prevention
- Troubleshooting AWS Cost Management identity and access
- Service-linked roles for AWS Cost Management
- Using service-linked roles
- AWS managed policies for AWS Billing and Cost Management

User types and billing permissions

This table summarizes the default actions that are permitted in AWS Cost Management for each type of billing user.

User types and billing permissions

User type	Description	Billing permissions
Account owner	The person or entity in whose name your account is set up as.	• Has full control of all Billing and Cost Management resources. • Receives a monthly invoice of AWS charges.
User	A person or application defined as a user in an account by an account owner or administrative user. Accounts can contain multiple users.	• Has permissions explicitly granted to the user or a group that includes the user. • Can be granted permission to view Billing and Cost Management console pages. For more information, see Overview of managing access permissions. • Can't close accounts.
Organization management account owner	The person or entity associated with an AWS Organizations management account. The management account pays for AWS usage that is incurred by a member account in an organization.	• Has full control of all Billing and Cost Management resources for the management account only. • Receives a monthly invoice of AWS charges for the management account and member accounts. • Views the activity of member accounts in the billing reports for the management account.

User type	Description	Billing permissions
Organization member account owner	The person or entity associated with an AWS Organizations member account. The management account pays for AWS usage that is incurred by a member account in an organization.	• Doesn't have permission to review any usage reports or account activity except for its own. Doesn't have access to usage reports or account activity for other member accounts in the organization or for the management account. • Doesn't have permission to view billing reports. • Has permission to update account information only for its own account. Can't access other member accounts or the management account.

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting AWS Cost Management identity and access)
- **Service administrator** - determine user access and submit permission requests (see How AWS Cost Management works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for AWS Cost Management)

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-

based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

Overview of managing access permissions

Granting access to your billing information and tools

The AWS account owner can access billing information and tools by signing in to the AWS Management Console using the account credentials. We recommend that you don't use the account credentials for everyday access to the account, and especially that you don't share account credentials with others to give them access to your account.

For your daily administrative tasks, create an administrative user to securely control access to AWS resources. By default, users don't have access to the AWS Cost Management console. As an administrator, you can create roles under your AWS account that your users can assume. After you create roles, you can attach your IAM policy to them, based on the access needed. For example, you can grant some users limited access to some of your billing information and tools, and grant others complete access to all of the information and tools.

> **Note**
>
> IAM is a feature of your AWS account. If you are already signed up for a product that is integrated with IAM, you don't need to do anything else to sign up for IAM, nor will you be charged for using it.
>
> Permissions for Cost Explorer apply to all accounts and member accounts, regardless of IAM policies. For more information about Cost Explorer access, see Controlling access to Cost Explorer.

Activating access to the Billing and Cost Management console

IAM roles within an AWS account can't access the Billing and Cost Management console pages by default. This is true even if the role has IAM policies that grant access to certain Billing and Cost Management features. The AWS account administrator can allow roles access to Billing and Cost Management console pages by using the **Activate IAM Access** setting.

On the AWS Cost Management console, the **Activate IAM Access** setting controls access to the following pages:

- Home
- Cost Explorer
- Reports
- Rightsizing recommendations
- Savings Plans recommendations
- Savings Plans utilization report
- Savings Plans coverage report
- Reservations overview

- Reservations recommendations
- Reservations utilization report
- Reservations coverage report
- Preferences

For a list of pages the **Activate IAM Access** setting controls for the Billing console, see Activating access to the Billing console in the *Billing User Guide*.

> **Important**
>
> Activating IAM access alone doesn't grant roles the necessary permissions for these Billing and Cost Management console pages. In addition to activating IAM access, you must also attach the required IAM policies to those roles. For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

The **Activate IAM Access** setting doesn't control access to the following pages and resources:

- The console pages for AWS Cost Anomaly Detection, Savings Plans overview, Savings Plans inventory, Purchase Savings Plans, and Savings Plans cart
- The Cost Management view in the AWS Console Mobile Application
- The Billing and Cost Management SDK APIs (AWS Cost Explorer, AWS Budgets, and AWS Cost and Usage Reports APIs)
- AWS Systems Manager Application Manager
- The in-console AWS Pricing Calculator
- The cost analysis capability in Amazon Q
- The AWS Activate Console

By default, the **Activate IAM Access** setting is deactivated. To activate this setting, you must log in to your AWS account using the root user credentials, and then select the setting in the **Account** page. Activate this setting in each account where you want to allow IAM role access to the Billing and Cost Management console pages. If you use AWS Organizations, then activate this setting in each management or member account where you want to allow IAM role access to the console pages.

> **Note**
>
> The **Activate IAM Access** setting isn't available to users with administrator access. This setting is available only to the root user of the account.

If the **Activate IAM Access** setting is deactivated, then IAM roles in the account can't access the Billing and Cost Management console pages. This is true even if they have administrator access or the required IAM policies.

To activate IAM user and role access to the Billing and Cost Management console

1. Sign in to the AWS Management Console with your root account credentials (specifically, the email address and password that you used to create your AWS account).
2. On the navigation bar, choose your account name, and then choose Account.
3. Next to **IAM User and Role Access to Billing Information**, choose **Edit**.
4. Select the **Activate IAM Access** check box to activate access to the Billing and Cost Management console pages.
5. Choose **Update**.

After you activate IAM access, you must also attach the required IAM policies to the IAM roles. The IAM policies can grant or deny access to specific Billing and Cost Management features. For more information, see Using identity-based policies (IAM policies) for AWS Cost Management.

How AWS Cost Management works with IAM

AWS Cost Management integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization has access to specific pages on the AWS Cost Management console. You can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits.

For more information about how to activate access to the Billing and Cost Management Console, see Tutorial: Delegate Access to the Billing Console in the *IAM User Guide*.

Before you use IAM to manage access to AWS Cost Management, learn what IAM features are available to use with AWS Cost Management.

IAM features you can use with AWS Cost Management

IAM feature	AWS Cost Management support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Partial
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Forward access sessions (FAS)	Yes
Service roles	Yes
Service-linked roles	No

To get a high-level view of how AWS Cost Management and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for AWS Cost Management

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for AWS Cost Management

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Resource-based policies within AWS Cost Management

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for AWS Cost Management

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of AWS Cost Management actions, see Actions defined by AWS Cost Management in the *Service Authorization Reference*.

Policy actions in AWS Cost Management use the following prefix before the action:

```
ce
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "ce:action1",
      "ce:action2"
         ]
```

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Policy resources for AWS Cost Management

Supports policy resources: Partial

Policy resources are only supported for monitors, subscriptions, and cost categories.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of AWS Cost Explorer resource types, see Actions, resources, and condition keys for AWS Cost Explorer in the *Service Authorization Reference*.

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Policy condition keys for AWS Cost Management

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match

the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of AWS Cost Management condition keys, actions, and resources, see Condition keys for AWS Cost Management in the *Service Authorization Reference*.

To view examples of AWS Cost Management identity-based policies, see Identity-based policy examples for AWS Cost Management.

Access control lists (ACLs) in AWS Cost Management

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Attribute-based access control (ABAC) with AWS Cost Management

Supports ABAC (tags in policies): Partial

ABAC (tags in policies) are only supported for monitors, subscriptions, and cost categories.

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using Temporary credentials with AWS Cost Management

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Forward access sessions for AWS Cost Management

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for AWS Cost Management

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break AWS Cost Management functionality. Edit service roles only when AWS Cost Management provides guidance to do so.

Identity-based policy examples for AWS Cost Management

By default, users and roles don't have permission to create or modify AWS Cost Management resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by AWS Cost Management, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for AWS Cost Management in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the AWS Cost Management console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete AWS Cost Management resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API

operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the AWS Cost Management console

To access the AWS Cost Management console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS Cost Management resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the AWS Cost Management console, also attach the AWS Cost Management `ConsoleAccess` or `ReadOnly` AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Using identity-based policies (IAM policies) for AWS Cost Management

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.

If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic provides examples of identity-based policies that demonstrate how an account administrator can attach permissions policies to IAM identities (roles and groups) and thereby grant permissions to perform operations on Billing and Cost Management resources.

For a full discussion of AWS accounts and users, see What Is IAM? in the *IAM User Guide*.

For information on how you can update customer managed policies, see Editing customer managed policies (console) in the *IAM User Guide*.

Topics

- Billing and Cost Management actions policies
- Billing and Cost Management recommended actions policies
- Managed policies
- AWS Cost Management updates to AWS managed policies

Billing and Cost Management actions policies

This table summarizes the permissions that allow or deny users access to your billing information and tools. For examples of policies that use these permissions, see AWS Cost Management policy examples.

For a list of actions policies for the Billing console, see Billing actions policies in the *Billing user guide*.

Permission name	Description
`aws-portal:ViewBilling`	Allow or deny users permission to view the Billing and Cost Management console pages. For an example policy, see Allow IAM users to view your billing information in the *Billing User Guide*.

Permission name	Description
`aws-portal:ViewUsage`	Allow or deny users permission to view AWS usage Reports. To allow users to view usage reports, you must allow both `ViewUsage` and `ViewBilling`. For an example policy, see Allow IAM users to access the reports console page in the *Billing User Guide*.
`aws-portal:ModifyBilling`	Allow or deny users permission to modify the following Billing and Cost Management console pages: • Budgets • Consolidated Billing • Billing preferences • Credits • Tax settings • Payment methods • Purchase orders • Cost Allocation Tags To allow users to modify these console pages, you must allow both `ModifyBilling` and `ViewBilling`. For an example policy, see Allow users to modify billing information.
`aws-portal:ViewAccount`	Allow or deny users permission to view the following Billing and Cost Management console pages: • Billing Dashboard • Account Settings

Permission name	Description
`aws-portal:ModifyAccount`	Allow or deny users permission to modify Account Settings. To allow users to modify account settings, you must allow both `ModifyAccount` and `ViewAccount` . For an example of a policy that explicitly denies a user access to the **Account Settings** console page, see Deny access to account settings, but allow full access to all other billing and usage information.
`budgets:ViewBudget`	Allow or deny users permission to view Budgets. To allow users to view budgets, you must also allow `ViewBilling` .
`budgets:ModifyBudget`	Allow or deny users permission to modify Budgets. To allow users to view and modify budgets, you must also allow `ViewBilling` .
`ce:GetPreferences`	Allow or deny users permissions to view the Cost Explorer preferences page. For an example policy, see View and update the Cost Explorer preferences page.
`ce:UpdatePreferences`	Allow or deny users permissions to update the Cost Explorer preferences page. For an example policy, see View and update the Cost Explorer preferences page.

Permission name	Description
ce:DescribeReport	Allow or deny users permissions to view the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
ce:CreateReport	Allow or deny users permissions to create reports using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
ce:UpdateReport	Allow or deny users permissions to update using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
ce:DeleteReport	Allow or deny users permissions to delete reports using the Cost Explorer reports page. For an example policy, see View, create, update, and delete using the Cost Explorer reports page.
ce:DescribeNotificationSubscription	Allow or deny users permissions to view Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.

Permission name	Description
ce:CreateNotificationSubscription	Allow or deny users permissions to create Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
ce:UpdateNotificationSubscription	Allow or deny users permissions to update Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
ce:DeleteNotificationSubscription	Allow or deny users permissions to delete Cost Explorer reservation expiration alerts in the reservation overview page. For an example policy, see View, create, update, and delete reservation and Savings Plans alerts.
ce:CreateCostCategoryDefinition	Allow or deny users permissions to create cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*. You can add resource tags to monitors during Create. In order to create monitors with resource tags, you need the ce:TagResource permission.

Permission name	Description
ce:DeleteCostCategoryDefinition	Allow or deny users permissions to delete cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
ce:DescribeCostCategoryDefinition	Allow or deny users permissions to view cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
ce:ListCostCategoryDefinitions	Allow or deny users permissions to list cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
ce:ListTagsForResource	Allow or deny users permissions to list all resource tags for a given resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.
ce:UpdateCostCategoryDefinition	Allow or deny users permissions to update cost categories. For an example policy, see View and manage cost categories in the *Billing User Guide*.
ce:CreateAnomalyMonitor	Allow or deny users permissions to create a single AWS Cost Anomaly Detection monitor. You can add resource tags to monitors during Create. In order to create monitors with resource tags, you need the ce:TagResource permission.

Permission name	Description
ce:GetAnomalyMonitors	Allow or deny users permissions to view all AWS Cost Anomaly Detection monitors.
ce:UpdateAnomalyMonitor	Allow or deny users permissions to update AWS Cost Anomaly Detection monitors.
ce:DeleteAnomalyMonitor	Allow or deny users permissions to delete AWS Cost Anomaly Detection monitors.
ce:CreateAnomalySubscription	Allow or deny users permissions to create a single subscription for AWS Cost Anomaly Detection. You can add resource tags to subscriptions during Create. In order to create subscriptions with resource tags, you need the ce:TagResource permission.
ce:GetAnomalySubscriptions	Allow or deny users permissions to view all subscriptions for AWS Cost Anomaly Detection .
ce:UpdateAnomalySubscription	Allow or deny users permissions to update AWS Cost Anomaly Detection subscriptions.
ce:DeleteAnomalySubscription	Allow or deny users permissions to delete AWS Cost Anomaly Detection subscriptions.
ce:GetAnomalies	Allow or deny users permissions to view all anomalies in AWS Cost Anomaly Detection.
ce:ProvideAnomalyFeedback	Allow or deny users permissions to provide feedback on a detected AWS Cost Anomaly Detection.

Permission name	Description
ce:TagResource	Allow or deny users permissions to add resource tag key-value pairs to a resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.
ce:UntagResource	Allow or deny users permissions to delete resource tags from a resource. For a list of supported resources, see ResourceTag in the *AWS Billing and Cost Management API Reference*.
ce:GetCostAndUsageComparisons	Allow or deny users permissions to retrieve cost and usage comparisons.
ce:GetCostComparisonDrivers	Allow or deny users permissions to retrieve cost drivers.

Billing and Cost Management recommended actions policies

To get started with recommended actions, you need to have the following core permission:

- bcm-recommended-actions:ListRecommendedActions

Additional permissions are then required based on recommended action type. The following table summarizes the different recommended action types and the corresponding IAM policy permissions needed in order to see the recommended actions.

> **Note**
>
> Even with a granted IAM policy permission, the corresponding recommended action type is only seen if the recommended action actually applies.

Recommended action type	Required permission name	Description
Expired payment method	`"bcm-recommended-actions:ListRecommendedActions", "payments:ListPaymentPreferences", "payments:GetPaymentInstrument"`	For payment-related recommended actions.
Invalid payment method	`"bcm-recommended-actions:ListRecommendedActions", "payments:ListPaymentPreferences", "payments:GetPaymentInstrument"`	For payment-related recommended actions.
Payments past due	`"bcm-recommended-actions:ListRecommendedActions", "payments:GetPaymentStatus"`	For payment-related recommended actions.
Payments due	`"bcm-recommended-actions:ListRecommendedActions", "payments:GetPaymentStatus"`	For payment-related recommended actions.
Fix tax registration information	`"bcm-recommended-actions:ListRecommendedActions",`	For recommended actions related to tax settings.

Recommended action type	Required permission name	Description
	`"tax:GetTaxRegistration"`	
Update tax exemption certificate	`"bcm-recommended-actions:ListRecommendedActions", "tax:GetExemptions"`	For recommended actions related to tax settings.
Migrate to granular permissions	`"bcm-recommended-actions:ListRecommendedActions", "aws-portal:GetConsoleActionSetEnforced", "ce:GetConsoleActionSetEnforced", "purchase-orders:GetConsoleActionSetEnforced"`	For recommended actions related to IAM permissions.
Review budget alerts	`"bcm-recommended-actions:ListRecommendedActions", "budgets:DescribeBudgetNotificationsForAccount", "budgets:DescribeBudget"`	For budget-related recommended actions.
Review budgets exceeded	`"bcm-recommended-actions:ListRecommendedActions", "budgets:DescribeBudgets"`	For budget-related recommended actions.

Recommended action type	Required permission name	Description
Review Free Tier usage alerts	`"bcm-recommended-actions:ListRecommendedActions", "freetier:GetFreeTierUsage"`	For recommended actions related to Free Tier.
Review anomalies	`"bcm-recommended-actions:ListRecommendedActions", "ce:GetAnomalies"`	For recommended actions related to cost anomaly detection.
Review expiring reservations	`"bcm-recommended-actions:ListRecommendedActions", "ce:GetReservationUtilization"`	For recommended actions related to cost optimization.
Review expiring Savings Plans	`"bcm-recommended-actions:ListRecommendedActions", "ce:GetSavingsPlansUtilizationDetails"`	For recommended actions related to cost optimization.
Review savings opportunity recommendations	`"bcm-recommended-actions:ListRecommendedActions", "cost-optimization-hub:ListEnrollmentStatuses", "cost-optimization-hub:ListRecommendationSummaries"`	For recommended actions related to cost optimization.

Recommended action type	Required permission name	Description
Enable Cost Optimization Hub	`"bcm-recommended-actions:ListRecommendedActions", "cost-optimization-hub:ListEnrollmentStatuses"`	For recommended actions related to cost optimization.
Create a budget	`"bcm-recommended-actions:ListRecommendedActions", "budgets:DescribeBudgets"`	For budget-related recommended actions.
Create a reservation budget	`"bcm-recommended-actions:ListRecommendedActions", "budgets:DescribeBudgets", "ce:GetReservationUtilization"`	For budget-related recommended actions.
Create a Savings Plans budget	`"bcm-recommended-actions:ListRecommendedActions", "budgets:DescribeBudgets", "ce:GetSavingsPlansUtilizationDetails"`	For budget-related recommended actions.
Add an alternate billing contact	`"bcm-recommended-actions:ListRecommendedActions", "account:GetAlternateContact"`	For account-related recommended actions.

Recommended action type	Required permission name	Description
Create an anomaly monitor	`"bcm-recommended-actions:ListRecommendedActions", "ce:GetAnomalyMonitors"`	For recommended actions related to cost anomaly detection.

Managed policies

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

Managed policies are standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account. You can use AWS managed policies to control access in Billing and Cost Management.

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases. AWS managed

policies make it easier for you to assign appropriate permissions to users, groups, and roles than if you had to write the policies yourself.

You can't change the permissions defined in AWS managed policies. AWS occasionally updates the permissions defined in an AWS managed policy. When this occurs, the update affects all principal entities (users, groups, and roles) that the policy is attached to.

Billing and Cost Management provides several AWS managed policies for common use cases.

Topics

- Allows full access to AWS Budgets including budgets actions
- Allows read only access to AWS Budgets
- Allows AWS Budgets to call services required to verify billing view access
- Allows permission to control AWS resources
- Allows Cost Optimization Hub to call services required to make the service work
- Allows read-only access to Cost Optimization Hub
- Allows admin access to Cost Optimization Hub
- Allows split cost allocation data to call services required to make the service work
- Allows Data Exports to access other AWS services

Allows full access to AWS Budgets including budgets actions

Managed policy name: `AWSBudgetsActionsWithAWSResourceControlAccess`

This managed policy is focused on the user, ensuring that you have the proper permissions to grant permission to AWS Budgets to run the defined actions. This policy provides full access to AWS Budgets, including budgets actions, to retrieve the status of your policies and run AWS resources using the AWS Management Console.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "budgets:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "budgets.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ModifyBilling",
                "ec2:DescribeInstances",
                "iam:ListGroups",
                "iam:ListPolicies",
                "iam:ListRoles",
                "iam:ListUsers",
                "organizations:ListAccounts",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListPolicies",
                "organizations:ListRoots",
                "rds:DescribeDBInstances",
                "sns:ListTopics"
            ],
            "Resource": "*"
        }
    ]
}
```

Allows read only access to AWS Budgets

Managed policy name: `AWSBudgetsReadOnlyAccess`

This managed policy allows read only access to AWS Budgets through the AWS Management Console. The policy can be attached to your users, groups, and roles.

JSON

```
{
  "Version":"2012-10-17",
  "Statement" : [
    {
      "Sid": "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Allows AWS Budgets to call services required to verify billing view access

Managed policy name: `BudgetsServiceRolePolicy`

Allows AWS Budgets to verify access to billing views shared across account boundaries.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "billing:GetBillingViewData"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Service-linked roles for Budgets.

Allows permission to control AWS resources

Managed policy name:
`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

This managed policy is focused on specific actions that AWS Budgets takes on your behalf when completing a specific action. This policy gives permission to control AWS resources. For example, starts and stops Amazon EC2 or Amazon RDS instances by running AWS Systems Manager (SSM) scripts.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "rds:DescribeDBInstances",
                "rds:StartDBInstance",
                "rds:StopDBInstance"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "ssm.amazonaws.com"
                    ]
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
                "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
                "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
                "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
                "arn:aws:ssm:*:*:automation-execution/*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
            ]
        }
    ]
}
```

Allows Cost Optimization Hub to call services required to make the service work

Managed policy name: `CostOptimizationHubServiceRolePolicy`

Allows Cost Optimization Hub to retrieve organization information and collect optimization-related data and metadata.

To view the permissions for this policy, see CostOptimizationHubServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

For more information, see Service-linked roles for Cost Optimization Hub.

Allows read-only access to Cost Optimization Hub

Managed policy name: `CostOptimizationHubReadOnlyAccess`

This managed policy provides read-only access to Cost Optimization Hub.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries"
            ],
            "Resource": "*"
        }
    ]
}
```

Allows admin access to Cost Optimization Hub

Managed policy name: `CostOptimizationHubAdminAccess`

This managed policy provides admin access to Cost Optimization Hub.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationHubAdminAccess",
            "Effect": "Allow",
            "Action": [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:UpdateEnrollmentStatus",
                "cost-optimization-hub:GetPreferences",
                "cost-optimization-hub:UpdatePreferences",
                "cost-optimization-hub:GetRecommendation",
                "cost-optimization-hub:ListRecommendations",
                "cost-optimization-hub:ListRecommendationSummaries",
                "organizations:EnableAWSServiceAccess"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "cost-optimization-
hub.bcm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowAWSServiceAccessForCostOptimizationHub",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "cost-optimization-hub.bcm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Allows split cost allocation data to call services required to make the service work

Managed policy name: `SplitCostAllocationDataServiceRolePolicy`

Allows split cost allocation data to retrieve AWS Organizations information, if applicable, and collect telemetry data for the split cost allocation data services that the customer has opted in to.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AmazonManagedServiceForPrometheusAccess",
            "Effect": "Allow",
            "Action": [
                "aps:ListWorkspaces",
                "aps:QueryMetrics"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Service-linked roles for split cost allocation data.

Allows Data Exports to access other AWS services

Managed policy name: `AWSBCMDataExportsServiceRolePolicy`

Allows Data Exports to access other AWS services such as Cost Optimization Hub on your behalf.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CostOptimizationRecommendationAccess",
            "Effect": "Allow",
            "Action":  [
                "cost-optimization-hub:ListEnrollmentStatuses",
                "cost-optimization-hub:ListRecommendations"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Service-linked roles for Data Exports.

AWS Cost Management updates to AWS managed policies

View details about updates to AWS managed policies for AWS Cost Management since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Cost Management Document history page.

Change	Description	Date
Update to existing policy AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	We updated the policy with require `automation-execution` and `document` permissions to use `ssm:StartAutomationExecution` .	04/07/2026
Update to existing policies	We updated the policy to add the "`cost-optimization`	11/20/2025

Change	Description	Date
CostOptimizationHubReadOnlyAccess CostOptimizationHubAdminAccess	`-hub:ListEfficiencyMetrics"` action.	
Addition of a new policy BudgetsServiceRolePolicy	Budgets added a new policy to be used with service-linked roles, which enables access to AWS services and resources used or managed by Budgets.	08/06/2025
Update to existing policy CostOptimizationHubServiceRolePolicy	We updated the policy to add the `ce:GetDimensionValues` action.	07/23/2025
Update to existing policy CostOptimizationHubServiceRolePolicy	We updated the policy to add the `organizations:ListDelegatedAdministrators` and `ce:GetCostAndUsage` actions.	07/05/2024
Update to existing policy AWSBudgetsReadOnlyAccess	We updated the policy to add the `budgets:ListTagsForResource` action.	06/17/2024
Addition of a new policy AWSBCMDataExportsServiceRolePolicy	Data Exports added a new policy to be used with service-linked roles, which enables access to other AWS services such as Cost Optimization Hub.	06/10/2024

Change	Description	Date
Addition of a new policy SplitCostAllocationDataServiceRolePolicy	Split cost allocation data added a new policy to be used with service-linked roles, which enables access to AWS services and resources used or managed by split cost allocation data.	04/16/2024
Update to existing policy AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	We updated the policy with scoped down permissions. The `ssm:StartAutomationExecution` action is only allowed for specific resources used by Budget actions.	12/14/2023

Change	Description	Date
Update to existing policies CostOptimizationHubReadOnlyAccess CostOptimizationHubAdminAccess	Cost Optimization Hub updated the following two managed policies: • `CostOptimizationHubReadOnlyAccess` : Fixed typo in "GetRecommendation"; removed permissions covered by the SLR policy. • `CostOptimizationHubAdminAccess` : Fixed typo in "GetRecommendation"; removed permissions covered by the SLR policy; added permissions to enable service access and to create the SLR, so that the policy provides all necessary permissions to opt in and use Cost Optimization Hub.	12/14/2023
Addition of a new policy CostOptimizationHubServiceRolePolicy	Cost Optimization Hub added a new policy to be used with service-linked roles, which enables access to AWS services and resources used or managed by Cost Optimization Hub.	11/02/2023
AWS Cost Management started tracking changes	AWS Cost Management started tracking changes for its AWS managed policies	11/02/2023

AWS Cost Management policy examples

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic contains example policies that you can attach to your IAM role or group to control access to your account's billing information and tools. The following basic rules apply to IAM policies for Billing and Cost Management:

- `Version` is always `2012-10-17`.
- `Effect` is always `Allow` or `Deny`.
- `Action` is the name of the action or a wildcard (`*`).

  The action prefix is `budgets` for AWS Budgets, `cur` for AWS Cost and Usage Reports, `aws-portal` for AWS Billing, or `ce` for Cost Explorer.
- `Resource` is always `*` for AWS Billing.

  For actions performed on a `budget` resource, specify the budget Amazon Resource Name (ARN).
- It's possible to have multiple statements in one policy.

For a list of policy examples for the Billing console, see Billing policy examples in the *Billing user guide*.

> **Note**
>
> These policies require that you activate user access to the Billing and Cost Management console on the Account Settings console page. For more information, see Activating access to the Billing and Cost Management console.

Topics

- Deny users access to the Billing and Cost Management console
- Deny AWS Console cost and usage widget access for member accounts
- Deny AWS Console cost and usage widget access for specific users and roles
- Allow full access to AWS services but deny users access to the Billing and Cost Management console
- Allow users to view the Billing and Cost Management console except for account settings
- Allow users to modify billing information
- Allow users to create budgets
- Deny access to account settings, but allow full access to all other billing and usage information
- Deposit reports into an Amazon S3 bucket
- View costs and usage
- Enable and disable AWS Regions
- View and update the Cost Explorer preferences page
- View, create, update, and delete using the Cost Explorer reports page
- View, create, update, and delete reservation and Savings Plans alerts
- Allow read-only access to AWS Cost Anomaly Detection
- Allow AWS Budgets to apply IAM policies and SCPs
- Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances
- Allow users to create, list, and add usage to workload estimates in Pricing Calculator
- Allow users to create, list, and add usage and commitments to bill scenarios in Pricing Calculator
- Allow users to create a bill estimate in Pricing Calculator
- Allow users to create preferences in Pricing Calculator

- Allow users to create, manage, and share custom billing views
- Allow users to access Cost Explorer when accessing a specific custom billing view

Deny users access to the Billing and Cost Management console

To explicitly deny a user access to the all Billing and Cost Management console pages, use a policy similar to this example policy.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "aws-portal:*",
            "Resource": "*"
        }
    ]
}
```

Deny AWS Console cost and usage widget access for member accounts

To restrict member (linked) account access to cost and usage data, use your management (payer) account to access the Cost Explorer preferences tab and uncheck **Linked Account Access**. This will deny access to cost and usage data from the Cost Explorer (AWS Cost Management) console, Cost Explorer API, and AWS Console Home page's cost and usage widget regardless of the IAM actions a member account's user or role has.

Deny AWS Console cost and usage widget access for specific users and roles

To deny AWS Console cost and usage widget access for specific users and roles, use the permissions policy below.

> **Note**
>
> Adding this policy to a user or role will deny users access to Cost Explorer (AWS Cost Management) console and Cost Explorer APIs as well.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ce:*",
            "Resource": "*"
        }
    ]
}
```

Allow full access to AWS services but deny users access to the Billing and Cost Management console

To deny users access to everything on the Billing and Cost Management console, use the following policy. In this case, you should also deny user access to AWS Identity and Access Management (IAM) so that the users can't access the policies that control access to billing information and tools.

> **Important**
>
> This policy doesn't allow any actions. Use this policy in combination with other policies that allow specific actions.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aws-portal:*",
                "iam:*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Allow users to view the Billing and Cost Management console except for account settings

This policy allows read-only access to all of the Billing and Cost Management console, including the **Payments Method** and **Reports** console pages, but denies access to the **Account Settings** page, thus protecting the account password, contact information, and security questions.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "aws-portal:View*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "aws-portal:*Account",
            "Resource": "*"
        }
    ]
}
```

Allow users to modify billing information

To allow users to modify account billing information in the Billing and Cost Management console, you must also allow users to view your billing information. The following policy example allows a user to modify the **Consolidated Billing**, **Preferences**, and **Credits** console pages. It also allows a user to view the following Billing and Cost Management console pages:

- **Dashboard**

- **Cost Explorer**
- **Bills**
- **Orders and invoices**
- **Advance Payment**

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "aws-portal:*Billing",
            "Resource": "*"
        }
    ]
}
```

Allow users to create budgets

To allow users to create budgets in the Billing and Cost Management console, you must also allow users to view your billing information, create CloudWatch alarms, and create Amazon SNS notifications. The following policy example allows a user to modify the **Budget** console page.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1435216493000",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling",
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
```

```
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216514000",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216552000",
            "Effect": "Allow",
            "Action": [
                "sns:*"
            ],
            "Resource": [
                "arn:aws:sns:us-east-1::"
            ]
        }
    ]
}
```

Deny access to account settings, but allow full access to all other billing and usage information

To protect your account password, contact information, and security questions, you can deny user access to **Account Settings** while still enabling full access to the rest of the functionality in the Billing and Cost Management console, as shown in the following example.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:*Billing",
                "aws-portal:*Usage",
                "aws-portal:*PaymentMethods"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "aws-portal:*Account",
            "Resource": "*"
        }
    ]
}
```

Deposit reports into an Amazon S3 bucket

The following policy allows Billing and Cost Management to save your detailed AWS bills to an Amazon S3 bucket, as long as you own both the AWS account and the Amazon S3 bucket. Note that this policy must be applied to the Amazon S3 bucket, instead of to a user. That is, it's a resource-based policy, not a user-based policy. You should deny user access to the bucket for users who don't need access to your bills.

Replace *bucketname* with the name of your bucket.

For more information, see Using Bucket Policies and User Policies in the *Amazon Simple Storage Service User Guide*.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": [
```

```
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::bucketname"
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::bucketname/*"
  }
  ]
}
```

View costs and usage

To allow users to use the AWS Cost Explorer API, use the following policy to grant them access.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Enable and disable AWS Regions

For an example IAM policy that allows users to enable and disable Regions, see AWS: Allows Enabling and Disabling AWS Regions in the *IAM User Guide*.

View and update the Cost Explorer preferences page

This policy allows a user to view and update using the **Cost Explorer preferences page**.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:UpdatePreferences"
       ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to view or edit the **Preferences** page.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to edit the **Preferences** page.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

View, create, update, and delete using the Cost Explorer reports page

This policy allows a user to view, create, update, and delete using the **Cost Explorer reports page**.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:CreateReport",
        "ce:UpdateReport",
        "ce:DeleteReport"
       ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to view or edit the **Reports** page.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:DescribeReport",
                "ce:CreateReport",
                "ce:UpdateReport",
                "ce:DeleteReport"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but deny permission to edit the **Reports** page.

View, create, update, and delete reservation and Savings Plans alerts

This policy allows a user to view, create, update, and delete reservation expiration alerts and Savings Plans alerts. To edit reservation expiration alerts or Savings Plans alerts, a user needs all three granular actions: `ce:CreateNotificationSubscription`, `ce:UpdateNotificationSubscription`, and `ce:DeleteNotificationSubscription`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:CreateNotificationSubscription",
        "ce:UpdateNotificationSubscription",
        "ce:DeleteNotificationSubscription"
       ],
      "Resource": "*"
    }
  ]
```

```
}
```

The following policy allows users to view Cost Explorer, but denies permission to view or edit the **Reservation Expiration Alerts** and **Savings Plans alert** pages.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:DescribeNotificationSubscription",
                "ce:CreateNotificationSubscription",
                "ce:UpdateNotificationSubscription",
                "ce:DeleteNotificationSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows users to view Cost Explorer, but denies permission to edit the **Reservation Expiration Alerts** and **Savings Plans alert** pages.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:CreateNotificationSubscription",
                "ce:UpdateNotificationSubscription",
                "ce:DeleteNotificationSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow read-only access to AWS Cost Anomaly Detection

To allow users read-only access to AWS Cost Anomaly Detection, use the following policy to grant them access. `ce:ProvideAnomalyFeedback` is optional as a part of the read-only access.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "ce:Get*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Allow AWS Budgets to apply IAM policies and SCPs

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs) on behalf of the user.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs), and to target Amazon EC2 and Amazon RDS instances on behalf of the user.

Trust policy

> **Note**
>
> This trust policy allows AWS Budgets to assume a role that can call other services on your behalf. For more information on the best practices for cross-service permissions like this, see Cross-service confused deputy prevention.

JSON

```
{
"Version":"2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "budgets.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:budgets::123456789012:budget/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
]
}
```

Permissions policy

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance",
        "ssm:StartAutomationExecution"
      ],
      "Resource": "*"
    }
  ]
}
```

Allow users to create, list, and add usage to workload estimates in Pricing Calculator

This policy allows IAM users to create, list, and add usage to workload estimates, along with permissions to query Cost Explorer data to get historical cost and usage data.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "WorkloadEstimate",
            "Effect": "Allow",
            "Action": [
                "ce:GetCostCategories",
                "ce:GetDimensionValues",
                "ce:GetCostAndUsage",
                "ce:GetTags",
```

```
                "bcm-pricing-calculator:GetWorkloadEstimate",
                "bcm-pricing-calculator:ListWorkloadEstimateUsage",
                "bcm-pricing-calculator:CreateWorkloadEstimate",
                "bcm-pricing-calculator:ListWorkloadEstimates",
                "bcm-pricing-calculator:CreateWorkloadEstimateUsage",
                "bcm-pricing-calculator:UpdateWorkloadEstimateUsage"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to create, list, and add usage and commitments to bill scenarios in Pricing Calculator

This policy allows IAM users to create, list, and add usage and commitments to bill scenarios. Cost Explorer permissions aren't added, so you won't be able to load historical data.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "BillScenario",
            "Effect": "Allow",
            "Action": [
                "bcm-pricing-calculator:CreateBillScenario",
                "bcm-pricing-calculator:GetBillScenario",
                "bcm-pricing-calculator:ListBillScenarios",
                "bcm-pricing-calculator:CreateBillScenarioUsageModification",
                "bcm-pricing-calculator:UpdateBillScenarioUsageModification",
                "bcm-pricing-calculator:ListBillScenarioUsageModifications",

                "bcm-pricing-calculator:ListBillScenarioCommitmentModifications"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to create a bill estimate in Pricing Calculator

This policy allows IAM users to create bill estimate and list bill estimate line items.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "BillEstimate",
            "Effect": "Allow",
            "Action": [
                "bcm-pricing-calculator:CreateBillEstimate",
                "bcm-pricing-calculator:GetBillEstimate",
                "bcm-pricing-calculator:UpdateBillEstimate",
                "bcm-pricing-calculator:ListBillEstimates",
                "bcm-pricing-calculator:ListBillEstimateLineItems",
                "bcm-pricing-calculator:ListBillEstimateCommitments",
                "bcm-pricing-calculator:ListBillEstimateInputUsageModifications",
                "bcm-pricing-
calculator:ListBillEstimateInputCommitmentModifications"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to create preferences in Pricing Calculator

This policy allows IAM users to create and get rate preferences.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "RatePreferences",
            "Effect": "Allow",
```

```
            "Action": [
                "bcm-pricing-calculator:GetPreferences",
                "bcm-pricing-calculator:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to create, manage, and share custom billing views

This policy allows IAM users to create, manage, and share custom billing views. They will need the ability to create and manage custom billing views using Billing View, and the ability to create and associate resource shares using AWS Resource Access Manager (AWS RAM).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
           "Effect": "Allow",
           "Action": [
               "billing:CreateBillingView",
               "billing:UpdateBillingView",
               "billing:DeleteBillingView",
               "billing:GetBillingView",
               "billing:ListBillingViews",
               "billing:ListTagsForResource",
               "billing:PutResourcePolicy",
               "ce:GetCostAndUsage",
               "ce:GetTags",
               "organizations:ListAccounts",
               "ram:ListResources",
               "ram:ListPermissions",
               "ram:CreateResourceShare",
               "ram:AssociateResourceShare",
               "ram:GetResourceShares",
               "ram:GetResourceShareAssociations",
               "ram:ListResourceSharePermissions",
               "ram:ListResourceTypes",
```

```
                "ram:ListPrincipals",
                "ram:DisassociateResourceShare"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to access Cost Explorer when accessing a specific custom billing view

This policy allows IAM users to access Cost Explorer when accessing a specific custom billing view (`custom-1a2b3c4d`). Replace `123456789012` with the 12-digit AWS account ID and `1a2b3c4d` with the unique identifier of the custom billing view.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "ce:GetDimensionValues",
               "ce:GetCostAndUsageWithResources",
               "ce:GetCostAndUsage",
               "ce:GetCostForecast",
               "ce:GetTags",
               "ce:GetUsageForecast",
               "ce:GetCostCategories"
           ],
           "Resource": [
               "arn:aws:billing::123456789012:billingview/custom-1a2b3c4d"
           ]
       },
       {
           "Effect": "Allow",
           "Action": [
               "billing:ListBillingViews",
               "billing:GetBillingView"
           ],
           "Resource": "*"
```

```
        }
    ]
}
```

Migrating access control for AWS Cost Management

> **Note**
>
> The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:
>
> - *aws-portal* namespace
> - *purchase-orders:ViewPurchaseOrders*
> - *purchase-orders:ModifyPurchaseOrders*
>
> If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
> For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
> If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You can use fine-grained access controls to provide individuals in your organization access to AWS Billing and Cost Management services. For example, you can provide access to Cost Explorer without providing access to the AWS Billing console.

To use the fine-grained access controls, you'll need to migrate your policies from under `aws-portal` to the new IAM actions.

The following IAM actions in your permission policies or service control policies (SCP) require updating with this migration:

- `aws-portal:ViewAccount`
- `aws-portal:ViewBilling`

- `aws-portal:ViewPaymentMethods`
- `aws-portal:ViewUsage`
- `aws-portal:ModifyAccount`
- `aws-portal:ModifyBilling`
- `aws-portal:ModifyPaymentMethods`
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

To learn how to use the **Affected policies** tool to identify your impacted IAM policies, see How to use the affected policies tool.

> **Note**
>
> Programmatic requests to AWS Cost Explorer, AWS Cost and Usage Reports, and AWS Budgets remains unaffected.
> Activating access to the Billing and Cost Management console remain unchanged.

Topics

- Managing access permissions
- How to use the affected policies tool

Managing access permissions

AWS Cost Management integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization has access to specific pages on the AWS Cost Management console. You can control access to AWS Cost Management features. For example, AWS Cost Explorer, Savings Plans, and reservation recommendations, Savings Plans and reservations utilization and coverage reports.

Use the following IAM permissions for granular control for the AWS Cost Management console.

Using fine-grained AWS Cost Management actions

This table summarizes the permissions that allow or deny IAM users and roles access to your cost and usage information. For examples of policies that use these permissions, see AWS Cost Management policy examples.

For a list of actions for the AWS Billing console, see AWS Billing actions policies in the *AWS Billing user guide*.

Feature name in the AWS Cost Management console	IAM action	Description

AWS Cost Management Home	`ce:GetCostAndUsage`
	`ce:GetDimensionValues`
	`ce:GetCostForecast`
	`ce:GetReservationUtilization`
	`ce:GetReservationPurchaseRecommendation`
	`ce:DescribeReport`
		Allow or deny users permission to view the **AWS Cost Management Home** page. All IAM actions are required to view the page.

AWS Cost Explorer	`ce:GetCostCategories`
	`ce:GetDimensionValues`
	`ce:GetCostAndUsageWithResources`
	`ce:GetCostAndUsage`
	`ce:GetCostForecast`
	`ce:GetTags`
		Allow or deny users permission to view the **AWS Cost Explorer** page.

Feature name in the AWS Cost Management console	IAM action	Description

	`ce:GetUsageForecast`
	
	`ce:DescribeReport`	

	`ce:CreateReport`	Allow or deny users permission to save Cost Explorer reports.
Reports	`ce:DescribeReport`	Allow or deny users permission to view a list of saved reports.
	`ce:DeleteReport`	Allow or deny users permission to delete a saved report.

AWS Budgets	`budgets:ViewBudget`
	
	`budgets:DescribeBudgetActionsForBudget`
	
	`budgets:DescribeBudgetAction`
	
	`budgets:DescribeBudgetActionsForAccount`
	
	`budgets:DescribeBudgetActionHistories`
		Allow or deny users permission to view the **Budgets** page.

Feature name in the AWS Cost Management console	IAM action	Description
	budgets:CreateBudgetAction budgets:ExecuteBudgetAction budgets:DeleteBudgetAction budgets:UpdateBudgetAction budgets:ModifyBudget	Allow or deny users permission to create, delete, and modify Budgets and Budgets actions.

Feature name in the AWS Cost Management console	IAM action	Description
AWS Cost Anomaly Detection	ce:GetDimensionValues ce:GetCostAndUsage ce:CreateAnomalyMonitor ce:GetAnomalyMonitors ce:UpdateAnomalyMonitor ce:DeleteAnomalyMonitor ce:CreateAnomalySubscription ce:GetAnomalySubscriptions ce:UpdateAnomalySubscription ce:DeleteAnomalySubscription ce:GetAnomalies ce:ProvideAnomalyFeedback	Allow or deny users permission to view, create, delete, and update on the **Cost Anomaly Detection** page.

Feature name in the AWS Cost Management console	IAM action	Description
Rightsizing recommendations	ce:GetDimensionValues ce:GetTags ce:GetRightsizingRecommendation	Allow or deny users permission to view the **Savings Plans Overview** page.
Savings Plans overview	ce:GetSavingsPlansUtilizationDetails ce:GetSavingsPlansPurchaseRecommendation	
	ce:DescribeNotificationSubscription	Allow or deny users permission to view the existing notification settings for expiring and queued Savings Plans alerts.
	ce:CreateNotificationSubscription ce:UpdateNotificationSubscription ce:DeleteNotificationSubscription	Allow or deny users permission to update the existing notification settings for expiring and queued Savings Plans alerts.
Savings Plans inventory	savingsplans:DescribeSavingsPlans ce:GetSavingsPlansUtilizationDetails	Allow or deny users permissions to view purchased Savings Plans.

Feature name in the AWS Cost Management console	IAM action	Description
	savingsplans:DescribeSavingsPlansOfferings	Allow or deny users permissions to add the Savings Plans they wish to renew to the cart.
Savings Plans recommendations	ce:GetSavingsPlansPurchaseRecommendation ce:ListSavingsPlansPurchaseRecommendationGeneration	Allow or deny users permission to view generated Savings Plans recommendations.
	ce:StartSavingsPlansPurchaseRecommendationGeneration	Allow or deny users permission to calculate a new set of recommendations based on the latest usage and Savings Plans inventory.
Purchase Savings Plans	savingsplans:DescribeSavingsPlansOfferings	Allow or deny users permission to add Savings Plans to the cart.
Savings Plans utilization report	ce:DescribeReport ce:GetSavingsPlansUtilization ce:GetSavingsPlansUtilizationDetails ce:GetDimensionValues	Allow or deny users permission to view utilization of your existing Savings Plans.

Feature name in the AWS Cost Management console	IAM action	Description
	savingsplans:DescribeSavingsPlanRates	Allow or deny users permission to view the Savings Plans rate.
Savings Plans coverage report	ce:GetDimensionValues ce:GetSavingsPlansCoverage ce:GetCostCategories ce:DescribeReport ce:GetSavingsPlansPurchaseRecommendation	Allow or deny users permission to view the eligible spends covered by Savings Plans.
Savings Plans cart	savingsplans:DescribeSavingsPlansOfferings	Allow or deny users permission to purchase Savings Plans.
	savingsplans:DescribeSavingsPlans	
	savingsplans:CreateSavingsPlan	

Feature name in the AWS Cost Management console	IAM action	Description

Reservations overview	`ce:GetReservationUtilization`
	`ce:GetReservationCoverage`
	`ce:GetReservationPurchaseRecommendation`
	`ce:DescribeReport`
		Allow or deny users permission to view the **Reservations Overview** page.

	`ce:DescribeNotificationSubscription`	Allow or deny users permission to view existing notification settings for expiring reserved instances (RI) alerts.

	`ce:CreateNotificationSubscription`
	`ce:UpdateNotificationSubscription`
	`ce:DeleteNotificationSubscription`
		Allow or deny users permission to update notification settings for expiring RI alerts.

Reservations recommendations	`ce:GetReservationPurchaseRecommendation` `ce:GetDimensionValues`	Allow or deny users permission to view reservations recommendations.

Feature name in the AWS Cost Management console	IAM action	Description
Reservations utilization reports	ce:GetDimensionValues ce:GetReservationUtilization ce:DescribeReport	Allow or deny users permission to view utilization of your existing RI.
	ce:CreateReport	Allow or deny users permission to save RI reports.
Reservations coverage report	ce:GetReservationCoverage ce:GetReservationPurchaseRecommendation ce:DescribeReport ce:GetDimensionValues ce:GetCostCategories	Allow or deny users permission to view eligible spends covered by Reservations (RIs).
	ce:CreateReport	Allow or deny users permission to save RI coverage reports.
Preferences	ce:GetPreferences	Allow or deny users permission to view AWS Cost Management preferences.
	ce:UpdatePreferences	Allow or deny users permission to update AWS Cost Management preferences.

How to use the affected policies tool

Note

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- *aws-portal* namespace
- *purchase-orders:ViewPurchaseOrders*
- *purchase-orders:ModifyPurchaseOrders*

If you're using AWS Organizations, you can use the bulk policy migrator scripts to update polices from your payer account. You can also use the old to granular action mapping reference to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You can use the **Affected policies** tool in the Billing console to identify IAM policies (excluding SCPs), and reference the IAM actions affected by this migration. Use the **Affected policies** tool to do the following tasks:

- Identify IAM policies and reference the IAM actions affected by this migration
- Copy the updated policy to your clipboard
- Open the affected policy in IAM policy editor
- Save the updated policy for your account
- Turn on the fine-grained permissions and disable the old actions

This tool operates within the boundaries of the AWS account you're signed into, and information regarding other AWS Organizations accounts are not disclosed.

To use the Affected policies tool

1. Sign in to the AWS Management Console and open the AWS Billing and Cost Management console at https://console.aws.amazon.com/costmanagement/.
2. Paste the following URL into your browser to access the **Affected policies** tool: https://console.aws.amazon.com/poliden/home?region=us-east-1#/.

   > **Note**
   >
   > You must have the `iam:GetAccountAuthorizationDetails` permission to view this page.

3. Review the table that lists the affected IAM policies. Use the **Deprecated IAM actions** column to review specific IAM actions referenced in a policy.
4. Under the **Copy updated policy** column, choose **Copy** to copy the updated policy to your clipboard. The updated policy contains the existing policy and the suggested fine-grained actions appended to it as a separate `Sid` block. This block has the prefix `AffectedPoliciesMigrator` at the end of the policy.
5. Under the **Edit Policy in IAM Console** column, choose **Edit** to go to IAM policy editor. You will see the JSON of your existing policy.
6. Replace the entire existing policy with the updated policy that you copied in step 4. You can make any other changes as needed.
7. Choose **Next** and then choose **Save changes**.
8. Repeat steps 3 to 7 for all affected policies.
9. After you update your policies, refresh the **Affected policies** tool to confirm there are no affected policies listed. The **New IAM Actions Found** column should have **Yes** for all policies and the **Copy** and **Edit** buttons will be disabled. Your affected policies are updated.

To enable fine-grained actions for your account

After you update your policies, follow this procedure to enable the fine-grained actions for your account.

Only the management account (payer) of an organization or individual accounts can use the **Manage New IAM Actions** section. An individual account can enable the new actions for itself. A management account can enable new actions for the entire organization or a subset of member

accounts. If you're a management account, update the affected policies for all member accounts and enable the new actions for your organization. For more information, see the How to toggle accounts between new fine-grained actions or existing IAM actions? section in the AWS blog post.

> **Note**
>
> To do this, you must have the following permissions:
>
> - `aws-portal:GetConsoleActionSetEnforced`
> - `aws-portal:UpdateConsoleActionSetEnforced`
> - `ce:GetConsoleActionSetEnforced`
> - `ce:UpdateConsoleActionSetEnforced`
> - `purchase-orders:GetConsoleActionSetEnforced`
> - `purchase-orders:UpdateConsoleActionSetEnforced`

If you don't see the **Manage New IAM Actions** section, this means your account has already enabled the fine-grained IAM actions.

1. Under **Manage New IAM Actions**, the **Current Action Set Enforced** setting will have the **Existing** status.

   Choose **Enable New actions (Fine Grained)** and then choose **Apply changes**.
2. In the dialog box, choose **Yes**. The **Current Action Set Enforced** status will change to **Fine Grained**. This means the new actions are enforced for your AWS account or for your organization.
3. (Optional) You can then update your existing policies to remove any of the old actions.

Example: Before and after IAM policy

The following IAM policy has the old `aws-portal:ViewPaymentMethods` action.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewPaymentMethods"
            ],
            "Resource": "*"
        }
    ]
}
```

After you copy the updated policy, the following example has the new `Sid` block with the fine-grained actions.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewPaymentMethods"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AffectedPoliciesMigrator0",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "invoicing:GetInvoicePDF",
                "payments:GetPaymentInstrument",
                "payments:GetPaymentStatus",
                "payments:ListPaymentPreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

Related resources

For more information, see Sid in the *IAM User Guide*.

For more information about the new fine-grained actions, see the Mapping fine-grained IAM actions reference and Using fine-grained AWS Cost Management actions.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions to the resource that AWS Cost Management features can give another service. If you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (*) for the unknown portions of the ARN. For example, `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`. For AWS Budgets, the value of `aws:SourceArn` must be `arn:aws:budgets::`*`123456789012`*`:budget/*`.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in AWS Budgets to prevent the confused deputy problem.

JSON

```
{
"Version":"2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "budgets.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:budgets::123456789012:budget/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
]
}
```

Troubleshooting AWS Cost Management identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Cost Management and IAM.

Topics

- I am not authorized to perform an action in AWS Cost Management
- I am not authorized to perform iam:PassRole
- I want to view my access keys
- I'm an administrator and want to allow others to access AWS Cost Management
- I want to allow people outside of my AWS account to access my AWS Cost Management resources

I am not authorized to perform an action in AWS Cost Management

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person who provided you with your sign-in credentials.

The following example error occurs when the `mateojackson` user tries to use the console to view details about a fictional *`my-example-widget`* resource but does not have the fictional `ce:GetWidget` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ce:GetWidget on resource: my-example-widget
```

In this case, Mateo asks his administrator to update his policies to allow him to access the *`my-example-widget`* resource using the `ce:GetWidget` action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to AWS Cost Management.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in AWS Cost Management. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a

user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
>
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your AWS account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access AWS Cost Management

To allow others to access AWS Cost Management, you must grant permission to the people or applications that need access. If you are using AWS IAM Identity Center to manage people and applications, you assign permission sets to users or groups to define their level of access. Permission sets automatically create and assign IAM policies to IAM roles that are associated with the person or application. For more information, see Permission sets in the *AWS IAM Identity Center User Guide*.

If you are not using IAM Identity Center, you must create IAM entities (users or roles) for the people or applications that need access. You must then attach a policy to the entity that grants them the correct permissions in AWS Cost Management. After the permissions are granted, provide the credentials to the user or application developer. They will use those credentials to access AWS. To learn more about creating IAM users, groups, policies, and permissions, see IAM Identities and Policies and permissions in IAM in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my AWS Cost Management resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether AWS Cost Management supports these features, see How AWS Cost Management works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Service-linked roles for AWS Cost Management

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Using service-linked roles

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

Topics

- Service-linked roles for Cost Optimization Hub
- Service-linked roles for split cost allocation data
- Service-linked roles for Data Exports
- Service-linked roles for Budgets

- Service-linked roles for user attributes for cost allocation

Service-linked roles for Cost Optimization Hub

Cost Optimization Hub uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Cost Optimization Hub. Service-linked roles are predefined by Cost Optimization Hub and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Cost Optimization Hub easier because you don't have to manually add the necessary permissions. Cost Optimization Hub defines the permissions of its service-linked roles, and unless defined otherwise, only Cost Optimization Hub can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Cost Optimization Hub

Cost Optimization Hub uses the service-linked role named `AWSServiceRoleForCostOptimizationHub`, which enables access to AWS services and resources used or managed by Cost Optimization Hub.

The `AWSServiceRoleForCostOptimizationHub` service-linked role trusts the `cost-optimization-hub.bcm.amazonaws.com` service to assume the role.

The role permissions policy, `CostOptimizationHubServiceRolePolicy`, allows Cost Optimization Hub to complete the following actions on the specified resources:

- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListParents
- organizations:DescribeOrganizationalUnit
- organizations:ListDelegatedAdministrators
- ce:ListCostAllocationTags

- ce:GetCostAndUsage
- ce:GetDimensionValues

For more information, see Allows Cost Optimization Hub to call services required to make the service work.

To view the full permissions details of the service-linked role `CostOptimizationHubServiceRolePolicy`, see CostOptimizationHubServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating the Cost Optimization Hub service-linked role

You don't need to manually create a service-linked role. When you enable Cost Optimization Hub, the service automatically creates the service-linked role for you. You can enable Cost Optimization Hub through the AWS Cost Management console, or via the API or AWS CLI. For more information, see Enable Cost Optimization Hub in this user guide.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the Cost Optimization Hub service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForCostOptimizationHub` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForCostOptimizationHub` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
```

```
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
    "Condition": {"StringLike": {"iam:AWSServiceName": "cost-optimization-
hub.bcm.amazonaws.com"}}
}
```

Deleting the Cost Optimization Hub service-linked role

If you no longer need to use Cost Optimization Hub, we recommend that you delete the `AWSServiceRoleForCostOptimizationHub` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must opt out of Cost Optimization Hub.

To opt out of Cost Optimization Hub

For information about opting out of Cost Optimization Hub, see Opting out of Cost Optimization Hub.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForCostOptimizationHub` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Cost Optimization Hub service-linked roles

Cost Optimization Hub supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS service endpoints.

Service-linked roles for split cost allocation data

Split cost allocation data uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to split cost allocation data. Service-linked roles are predefined by split cost allocation data and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up split cost allocation data easier because you don’t have to manually add the necessary permissions. Split cost allocation data defines the permissions of its service-linked roles, and unless defined otherwise, only split cost allocation data can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for split cost allocation data

Split cost allocation data uses the service-linked role named `AWSServiceRoleForSplitCostAllocationData`, which enables access to AWS services and resources used or managed by split cost allocation data.

The `AWSServiceRoleForSplitCostAllocationData` service-linked role trusts the `split-cost-allocation-data.bcm.amazonaws.com` service to assume the role.

The role permissions policy, `SplitCostAllocationDataServiceRolePolicy`, allows split cost allocation data to complete the following actions on the specified resources:

- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListParents
- aps:ListWorkspaces
- aps:QueryMetrics

For more information, see Allows split cost allocation data to call services required to make the service work.

To view the full permissions details of the service-linked role `SplitCostAllocationDataServiceRolePolicy`, see `SplitCostAllocationDataServiceRolePolicy` in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating the split cost allocation data service-linked role

You don't need to manually create a service-linked role. When you opt in to split cost allocation data, the service automatically creates the service-linked role for you. You can enable split cost

allocation data through the AWS Cost Management console. For more information, see Enabling split cost allocation data.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the split cost allocation data service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForSplitCostAllocationData` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForSplitCostAllocationData` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/split-cost-allocation-
data.bcm.amazonaws.com/AWSServiceRoleForSplitCostAllocationData",
    "Condition": {"StringLike": {"iam:AWSServiceName": "split-cost-allocation-
data.bcm.amazonaws.com"}}
}
```

Deleting the split cost allocation data service-linked role

If you no longer need to use split cost allocation data, we recommend that you delete the `AWSServiceRoleForSplitCostAllocationData` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must opt out of split cost allocation data.

To opt out of split cost allocation data

For information about opting out of split cost allocation data, see Enabling split cost allocation data.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForSplitCostAllocationData` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for split cost allocation data service-linked roles

Split cost allocation data supports using service-linked roles in all of the AWS Regions where split cost allocation data is available. For more information, see AWS service endpoints.

Service-linked roles for Data Exports

Data Exports uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Data Exports. Service-linked roles are predefined by Data Exports and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Data Exports easier because you don't have to manually add the necessary permissions. Data Exports defines the permissions of its service-linked role, and unless defined otherwise, only Data Exports can assume that role. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Data Exports

Data Exports uses the service-linked role named `AWSServiceRoleForBCMDataExports`, which enables access to AWS service data for exporting the data to a target location, such as Amazon S3, on behalf of the customer. This service-linked role is used for read-only actions to collect the least amount of AWS service data necessary. The service-linked role is used over time to ensure security and to continue refreshing the export data in the target location.

The `AWSServiceRoleForBCMDataExports` service-linked role trusts the `bcm-data-exports.amazonaws.com` service to assume the role.

The role permissions policy, `AWSBCMDataExportsServiceRolePolicy`, allows Data Exports to complete the following actions on the specified resources:

- cost-optimization-hub:ListEnrollmentStatuses
- cost-optimization-hub:ListRecommendation

For more information, see Allows Data Exports to access other AWS services.

To view the full permissions details of the service-linked role `AWSBCMDataExportsServiceRolePolicy`, see AWSBCMDataExportsServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating the Data Exports service-linked role

You don't need to manually create the Data Exports service-linked role. On the Data Exports console page, when you attempt to create an export of a table that requires the service-linked role, the service automatically creates the role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the Data Exports service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForBCMDataExports` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForBCMDataExports` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/bcm-data-exports.amazonaws.com/
AWSServiceRoleForBCMDataExports",
```

```
    "Condition": {"StringLike": {"iam:AWSServiceName": "bcm-data-
exports.amazonaws.com"}}
}
```

Deleting the Data Exports service-linked role

If you no longer need to use Data Exports, we recommend that you delete the `AWSServiceRoleForBCMDataExports` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must first delete any Data Exports that require the service-linked role.

To delete an export

For information about deleting an export, see Editing and deleting exports.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForBCMDataExports` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Data Exports service-linked roles

Data Exports supports using service-linked roles in all of the AWS Regions where Data Exports is available. For more information, see AWS service endpoints.

Service-linked roles for Budgets

Budgets uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Budgets. Service-linked roles are predefined by Budgets and include all the permissions that the service requires to call other AWS services on your behalf.

Budgets defines the permissions of its service-linked roles, and unless defined otherwise, only Budgets can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Budgets

Budgets uses the service-linked role named `AWSServiceRoleForBudgets`, which enables Budgets to verify access to billing views that are shared across account boundaries.

The purpose of this service-linked role is to verify that customers have access to the underlying billing view data associated with a Budget when updating the spend of a Budget.

The `AWSServiceRoleForBudgets` service-linked role trusts the `budgets.amazonaws.com` service to assume the role.

The role permissions policy, `BudgetsServiceRolePolicy`, allows Budgets to complete the following action on all Billing View resources that the customer has access to:

- billing:GetBillingViewData

For more information, see Allows Budgets to call services required to verify billing view access.

To view the full permissions details of the service-linked role `BudgetsServiceRolePolicy`, see BudgetsServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating the Budgets service-linked role

You don't need to manually create a service-linked role. When you make a request to CreateBudget or UpdateBudget with a BillingView from another account that you have access to, the service automatically creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the Budgets service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForBudgets` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

To allow an IAM entity to edit the description of the `AWSServiceRoleForBudgets` service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/budgets.amazonaws.com/
AWSServiceRoleForBudgets",
    "Condition": {"StringLike": {"iam:AWSServiceName": "budgets.amazonaws.com"}}
}
```

Deleting the Budgets service-linked role

If you no longer need to use Budgets, we recommend that you delete the `AWSServiceRoleForBudgets` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must delete any Budgets in your account that are associated with a Billing View from another account. If you try deleting the service-linked role before this is done, the request will fail.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS Command Line Interface (AWS CLI), or the AWS API to delete the `AWSServiceRoleForBudgets` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Budgets service-linked roles

Budgets supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS service endpoints.

Service-linked roles for user attributes for cost allocation

User attributes for cost allocation uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to user attributes for cost allocation. Service-linked roles are predefined by user attributes for cost allocation and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up user attributes for cost allocation easier because you don't have to manually add the necessary permissions. User attributes for cost allocation defines

the permissions of its service-linked role, and unless defined otherwise, only user attributes for cost allocation can assume that role. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for user attributes for cost allocation

User attributes for cost allocation uses the service-linked role named `AWSServiceRoleForUserAttributeCostAllocation`, which grants user attributes for cost allocation permissions to read user attributes from AWS IAM Identity Center on your behalf.

The `AWSServiceRoleForUserAttributeCostAllocation` service-linked role trusts the `user-attribute-cost-allocation-data.amazonaws.com` service to assume the role.

The service-linked role uses two types of policies:

- **Inline role permissions policy:** Contains the permissions that allow user attributes for cost allocation to access user information from your AWS IAM Identity Center instance through Identity Store APIs. This policy includes the necessary KMS permissions when customers encrypt their Identity Center data, and is scoped to your specific account and Identity Center instance.
- **AWS managed policy (AWSUserAttributeCostAllocationPolicy):** Provides additional permissions to the service to fetch the service-linked role for internal usage.

For more information on updates to the AWSUserAttributeCostAllocationPolicy managed policy, see AWS managed policies for AWS Billing and Cost Management.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating the user attributes for cost allocation service-linked role

You don't need to manually create a service-linked role. When you enable user attributes for cost allocation in the AWS Cost Management console, the service automatically creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you enable user attributes for cost allocation, the service creates the service-linked role for you again.

Editing the user attributes for cost allocation service-linked role

You can't edit the name or permissions of the `AWSServiceRoleForUserAttributeCostAllocation` service-linked role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

Deleting the user attributes for cost allocation service-linked role

If you no longer need to use user attributes for cost allocation, we recommend that you delete the `AWSServiceRoleForUserAttributeCostAllocation` service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, before you can manually delete the service-linked role, you must first opt out of user attributes for cost allocation.

Cleaning up the service-linked role

Before you can use IAM to delete the service-linked role, you must first opt out of user attributes for cost allocation by disabling all user attributes in the user attributes for cost allocation preferences.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForUserAttributeCostAllocation` service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for user attributes for cost allocation service-linked roles

User attributes for cost allocation supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see AWS service endpoints.

AWS managed policies for AWS Billing and Cost Management

Creating IAM customer managed policies with only the permissions your team needs requires time and expertise. To get started quickly, you can use AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

AWSUserAttributeCostAllocationPolicy

This policy provides permissions for the user attributes for cost allocation service-linked role to fetch role information for internal service operations.

This policy is attached to the `AWSServiceRoleForUserAttributeCostAllocation` service-linked role.

AWS Billing and Cost Management updates to AWS managed policies

View details about updates to AWS managed policies for AWS Billing and Cost Management since this service began tracking these changes.

Policy	Version	Change
AWSUserAttributeCostAllocationPolicy	1	**December 15, 2025:** Initial policy creation. This policy provides permissions for the user attributes for cost allocation service-linked role to fetch role information for internal service operations.

Logging and monitoring in AWS Cost Management

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS account. There are several tools available to monitor your Billing and Cost Management usage.

AWS Cost and Usage Reports

AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products,

usage type, and operation that you use in your AWS account. You can customize the AWS Cost and Usage Reports to aggregate the information either by the hour or by the day.

For more information about AWS Cost and Usage Reports, see the *Cost and Usage Report Guide*.

AWS Cost Explorer

Cost Explorer enables you to view and analyze your costs and usage. You can monitor data for up to the last 13 months, forecast how much you're likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase. You can use Cost Explorer to identify areas that need further inquiry and see trends that you can use to understand your costs.

For more information about Cost Explorer, see the Analyzing your costs and usage with AWS Cost Explorer.

AWS Budgets

Budgets enables you to track your AWS cost and usage by using the cost visualization provided by Cost Explorer. Budgets shows the status of your budgets, provides forecasts of your estimated costs, and tracks your AWS usage, including Free Tier. You can also receive notifications when your estimated costs exceed your budgets.

For more information about Budgets, see the Managing your costs with AWS Budgets.

AWS CloudTrail

Billing and Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Billing and Cost Management. CloudTrail captures all write and modify API calls for Billing and Cost Management as events, including calls from the Billing and Cost Management console and from code calls to the Billing and Cost Management APIs.

For more information about AWS CloudTrail, see the Logging AWS Cost Management API calls with AWS CloudTrail.

AWS Pricing Calculator

The in-console AWS Pricing Calculator is an AWS Billing and Cost Management feature that enables you to estimate your planned cloud costs using your discount and purchase commitments. You can use Pricing Calculator to assess the cost impact for migrating workloads, planning new or growth of existing workloads, and plan for commitment purchases.

For more information about the in-console Pricing Calculator, see the Generating estimates with Pricing Calculator.

Logging AWS Cost Management API calls with AWS CloudTrail

AWS Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Cost Management. CloudTrail captures API calls for AWS Cost Management as events. The calls captured include API calls from the AWS Cost Management console and from your applications.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Cost Management. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Cost Management, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

AWS Cost Management information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Cost Management, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for AWS Cost Management, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the CloudTrail console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partitions and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to analyze and act on the event data collected in CloudTrail logs.

For more information, see the following in the *CloudTrail User Guide*:

- Creating a trail for your AWS account (overview)
- CloudTrail supported services and integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions

- Receiving CloudTrail log files from multiple accounts

AWS Cost Management actions are logged by CloudTrail and documented in the AWS Billing and Cost Management API Reference. For example, calls to the `GetDimensionValues`, `GetCostCategories`, and `GetCostandUsage` endpoints generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine whether the request was made:

- With root or user role credentials.
- With temporary security credentials for a role or federated user.
- By another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding AWS Cost Management log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on.

CloudTrail log files contain one or more log entries. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry for the `GetCostandUsage` endpoint.

```
{
        "eventVersion":"1.08",
        "userIdentity":{
            "accountId":"111122223333",
            "accessKeyId":"AIDACKCEVSQ6C2EXAMPLE"
        },
        "eventTime":"2022-05-24T22:38:51Z",
        "eventSource":"ce.amazonaws.com",
        "eventName":"GetCostandUsage",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.100.10.10",
        "requestParameters":{
           "TimePeriod":{
```

```
            "Start":"2022-01-01",
            "End":"2022-01-31"
         },
         "Metrics":[
            "UnblendedCost",
            "UsageQuantity"
         ],
         "Granularity":"MONTHLY",
         "GroupBy":[
            {
               "Type":"DIMENSION",
               "Key":"SERVICE"
            }
         ]
      },
      "responseElements":null,
      "requestID":"3295c994-063e-44ac-80fb-b40example9f",
      "eventID":"5923c499-063e-44ac-80fb-b40example9f",
      "readOnly":true,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"1111-2222-3333",
      "eventCategory":"Management",
      "tlsDetails":{
         "tlsVersion":"TLSv1.2",
         "clientProvidedHostHeader":"ce.us-east-1.amazonaws.com"
      }
}
```


Understanding Cost Optimization Hub log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following examples show CloudTrail log entries that demonstrate API actions and exceptions for Cost Optimization Hub.

Examples

- Exceptions

- Throttling Exception
- Access denied exception

- API actions
  - ListEnrollmentStatus
  - ListRecommendations
  - ListRecommendationSummaries
  - GetRecommendation
  - UpdateEnrollmentStatus
  - UpdatePreferences

Throttling Exception

The following example shows a log entry for a throttling exception.


```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "john-doe": "Admin"
      },
      "attributes": {
        "creationDate": "2023-10-14T00:48:50Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-10-14T01:16:45Z",
  "eventSource": "cost-optimization-hub.amazonaws.com",
  "eventName": "ListEnrollmentStatuses",
```

```
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "errorCode": "ThrottlingException",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "cc04aa10-7417-4c46-b1eb-EXAMPLE1df2b",
      "eventID": "754a3aad-1b54-456a-ac1f-EXAMPLE0e9c3",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "localhost:8080"
      }
    }
```

Access denied exception

The following example shows a log entry for an `AccessDenied` exception.

```
{
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FTKD2BZKUK:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/ReadOnly/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FTKD2BZKUK",
            "arn": "arn:aws:iam::111122223333:role/ReadOnly",
            "accountId": "111122223333",
            "john-doe": "ReadOnly"
          },
          "attributes": {
            "creationDate": "2023-10-16T19:08:36Z",
            "mfaAuthenticated": "false"
          }
        }
      },
```

```
      "eventTime": "2023-10-16T19:11:04Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "ListEnrollmentStatuses",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:sts::111122223333:assumed-role/ReadOnly/john-
doe is not authorized to perform: cost-optimization-hub:ListEnrollmentStatuses
 on resource: * because no identity-based policy allows the cost-optimization-
hub:ListEnrollmentStatuses action",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "1e02d84a-b04a-4b71-8615-EXAMPLEdcda7",
      "eventID": "71c86695-d4ec-4caa-a106-EXAMPLEe0d94",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "localhost:8080"
      }
    }
```

ListEnrollmentStatus

The following example shows a log entry for the `ListEnrollmentStatus` API action.

```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
```

```
        },
        "attributes": {
          "creationDate": "2023-10-14T00:48:50Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2023-10-14T01:16:43Z",
    "eventSource": "cost-optimization-hub.amazonaws.com",
    "eventName": "ListEnrollmentStatuses",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.28.3",
    "requestParameters": {
      "includeOrganizationInfo": false
    },
    "responseElements": null,
    "requestID": "cba87aa3-4678-41b8-a840-EXAMPLEaf3b8",
    "eventID": "57f04d0e-61f7-4c0f-805c-EXAMPLEbbbf5",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "localhost:8080"
    }
  }
```

ListRecommendations

The following example shows a log entry for the `ListRecommendations` API action.

```
  {
    "eventVersion": "1.09",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
      "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
      "accountId": "111122223333",
      "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
```

```
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T23:47:55Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-17T00:45:29Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "ListRecommendations",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "filter": {
          "resourceIdentifiers": [
            "arn:aws:ecs:us-east-1:111122223333:service/
EXAMPLEAccountsIntegrationService-EcsCluster-ClusterEB0386A7-7fsvP2MMmxZ5/
EXAMPLEAccountsIntegrationService-EcsService-Service9571FDD8-Dqm4mPMLstDn"
          ]
        },
        "includeAllRecommendations": false
      },
      "responseElements": null,
      "requestID": "a5b2df72-2cfd-4628-8a72-EXAMPLE7560a",
      "eventID": "a73bef13-6af7-4c11-a708-EXAMPLE6af5c",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
      }
    }
```


ListRecommendationSummaries

The following example shows a log entry for the `ListRecommendationSummaries` API action.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2023-10-16T23:47:55Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-10-17T00:46:16Z",
  "eventSource": "cost-optimization-hub.amazonaws.com",
  "eventName": "ListRecommendationSummaries",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "PostmanRuntime/7.28.3",
  "requestParameters": {
    "groupBy": "ResourceType"
  },
  "responseElements": null,
  "requestID": "ab54e6ad-72fe-48fe-82e9-EXAMPLEa6d1e",
  "eventID": "9288d9fa-939d-4e5f-a49a-EXAMPLEeb14b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
  }
}
```

GetRecommendation

The following example shows a log entry for the `GetRecommendation` API action.


```
    {
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T23:47:55Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-17T00:47:48Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "GetRecommendation",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "recommendationId":
"EXAMPLEwMzEwODU5XzQyNTFhNGE4LWZkZDItNDUyZi1hMjY4LWRkOTFkOTA1MTc1MA=="
      },
      "responseElements": null,
      "requestID": "e289a76a-182c-4bc9-8093-EXAMPLEbed0e",
      "eventID": "f1ed7ee6-871c-41fd-bb27-EXAMPLE24b64",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
```

```
      "tlsDetails": {
        "clientProvidedHostHeader": "cost-optimization-hub.us-east-1.amazonaws.com"
      }
    }
```

UpdateEnrollmentStatus

The following example shows a log entry for the `UpdateEnrollmentStatus` API action.

```
{
      "eventVersion": "1.09",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "EXAMPLEAIZ5FYRFP3POCC",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "john-doe": "Admin"
          },
          "attributes": {
            "creationDate": "2023-10-16T19:11:30Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-10-16T19:12:35Z",
      "eventSource": "cost-optimization-hub.amazonaws.com",
      "eventName": "UpdateEnrollmentStatus",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "PostmanRuntime/7.28.3",
      "requestParameters": {
        "status": "Inactive"
      },
      "responseElements": {
        "status": "Inactive"
      },
      "requestID": "6bf0c8a3-af53-4c4e-8f50-EXAMPLE477f0",
```

```
    "eventID": "d2bfa850-ef3d-4317-8ac4-EXAMPLEc16b1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
      "clientProvidedHostHeader": "localhost:8080"
    }
  }
```

UpdatePreferences

The following example shows a log entry for the `UpdatePreferences` API action.

```
  {
    "eventVersion": "1.09",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "EXAMPLEAIZ5FYRFP3POCC:john-doe",
      "arn": "arn:aws:sts::111122223333:assumed-role/Admin/john-doe",
      "accountId": "111122223333",
      "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "EXAMPLEAIZ5FYRFP3POCC",
          "arn": "arn:aws:iam::111122223333:role/Admin",
          "accountId": "111122223333",
          "john-doe": "Admin"
        },
        "attributes": {
          "creationDate": "2023-10-16T19:11:30Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2023-10-16T19:16:00Z",
    "eventSource": "cost-optimization-hub.amazonaws.com",
    "eventName": "UpdatePreferences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.28.3",
    "requestParameters": {
```

```
        "costMetricsType": "AfterDiscounts"
      },
      "responseElements": {
        "costMetricsType": "AfterDiscounts",
        "memberAccountDiscountVisibility": "None"
      },
      "requestID": "01e56ca3-47af-45f0-85aa-EXAMPLE30b42",
      "eventID": "7350ff23-35f5-4760-98b2-EXAMPLE61f13",
      "readOnly": false,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333",
      "eventCategory": "Management",
      "tlsDetails": {
        "clientProvidedHostHeader": "localhost:8080"
      }
    }
```


Understanding AWS Pricing Calculator log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specifyincluding events for AWS Pricing Calculator. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to AWS Pricing Calculator, the IP address from which the request was made, who made the request, when it was made, and additional details.

AWS Pricing Calculator CloudTrail events

This section shows a full list of the CloudTrail events related to Pricing Calculator.

> **Note**
>
> The event source for the following events is `bcm-pricing-calculator.amazonaws.com`.

Event name	Definition
CreateWorkloadEstimate	Mutating operation. Allows customers to create a Workload estimate.
UpdateWorkloadEstimate	Mutating operation. Allows customers to update a Workload estimate metadata.
DeleteWorkloadEstimate	Mutating operation. Allows customers to delete a Workload estimate.
GetWorkloadEstimate	Non-mutating operation. Allows customers to get details of a Workload estimate.
ListWorkloadEstimates	Non-mutating operation. Allows customers to list all Workload estimates in their account.
ListWorkloadEstimateUsage	Non-mutating operation. Allows customers to list all usage lines in a Workload estimate.
BatchCreateWorkloadEstimateUsage	Mutating operation. Allows customers to create usage lines in their Workload estimate.
BatchUpdateWorkloadEstimateUsage	Mutating operation. Allows customers to modify existing usage lines in their Workload estimate.
BatchDeleteWorkloadEstimateUsage	Mutating operation. Allows customers to delete added usage lines in their Workload estimate.
CreateBillScenario	Mutating operation. Allows customers to create a Bill scenario.
GetBillScenario	Mutating operation. Allows customers to get details of a Bill scenario.
UpdateBillScenario	Mutating operation. Allows customers to update metadata of a Bill scenario.
DeleteBillScenario	Mutating operation. Allows customers to delete a Bill scenario.

Event name	Definition
ListBillScenarios	Non-mutating operation. Allows customers to list all Bill scenarios in their account.
BatchCreateBillScenarioUsageModifications	Mutating operation. Allows customers to create usage lines in their Bill scenario.
BatchUpdateBillScenarioUsageModifications	Mutating operation. Allows customers to modify existing usage lines in their Bill scenario.
BatchDeleteBillScenarioUsageModifications	Mutating operation. Allows customers to delete existing usage lines in their Bill scenario.
ListBillScenarioUsageModifications	Non-mutating operation. Allows customers to list all usage lines in a Bill scenario.
BatchCreateBillScenarioCommitmentModifications	Mutating operation. Allows customers to model commitments in their Bill scenario.
BatchUpdateBillScenarioCommitmentModifications	Mutating operation. Allows customers to modify modeled commitment lines in their Bill scenario.
BatchDeleteBillScenarioCommitmentModifications	Mutating operation. Allows customers to delete modeled commitment lines in their Bill scenario.
ListBillScenarioCommitmentModifications	Non-mutating operation. Allows customers to list all modeled commitments in a Bill scenario.
CreateBillEstimate	Mutating operation. Allows customers to create a new Bill estimate from a Bill scenario.

Event name	Definition
GetBillEstimate	Mutating operation. Allows customers to get details of a Bill estimate.
UpdateBillEstimate	Mutating operation. Allows customers to update metadata of a Bill estimate.
DeleteBillEstimate	Mutating operation. Allows customers to delete a Bill estimate.
ListBillEstimates	Non-mutating operation. Allows customers to list all Bill estimates in their account.
ListBillEstimateLineItems	Non-mutating operation. Allows customers to list all result lines of a successfull completed Bill estimate.
ListBillEstimateCommitments	Non-mutating operation. Allows customers to list all commitments of a successfull completed Bill estimate.
ListBillEstimateInputUsageModifications	Non-mutating operation. Allows customers to list all commitments modeled in a Bill scenario that contributed to creating a Bill estimate.
GetPreferences	Non-mutating operation. Allows customers to get rate preferences set by the payer or standalone account
UpdatePreferences	Mutating operation. Allows customers to set rate preferences for use in Workload estimates. This is a payer or standalone account only API operation.
TagResource	Mutating operation. Allows customers to tag a Pricing Calculator resource.
UntagResource	Mutating operation. Allows customers to un-tag a Pricing Calculator resource.
ListTagsForResource	Non-mutating operation. Allows customers to list all tags attached to a Pricing Calculator resource.

CreateWorkloadEstimate

The following example shows a CloudTrail log entry that uses the `CreateWorkloadEstimate` API action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
    },
    "eventTime": "2024-11-11T02:09:08Z",
    "eventSource": "bcm-pricing-calculator.amazonaws.com",
    "eventName": "CreateWorkloadEstimate",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "requestParameters": {
        "name": "example-estimate-name",
        "resourceTags": [],
        "rateType": "BEFORE_DISCOUNTS"
    },
    "responseElements": {
        "costCurrency": "USD",
        "costSummary": {
            "cost": 0,
            "costStatus": "VALID",
            "currency": "USD"
        },
        "createdAt": 1731290948.299,
        "expiresAt": 1765418948.299,
        "id": "15cf39cc-ce14-4943-9dcb-35ccec39ae21",
        "name": "example-estimate-name",
        "rateDescription": "BEFORE_DISCOUNTS|2024-11-11T02:09:08.299974018Z",
        "rateTimestamp": 1731290948.299,
        "rateType": "BEFORE_DISCOUNTS",
        "status": "READY",
        "totalCost": 0
    },
    "eventID": "22bb9d97-6f0c-4482-830d-cde1c9ea00be",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
```

```
}
```

Compliance validation for AWS Cost Management

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs. AWS Cost Management is not in scope of any AWS compliance programs.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS Cost Management is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub CSPM – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in AWS Cost Management

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in AWS Cost Management

As a managed service, AWS Cost Management is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Billing and Cost Management through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Quotas and restrictions

The following table describes the current quotas, restrictions, and naming constraints within AWS Cost Management features.

For a list of quotas and restrictions for features in the AWS Billing console, see Quotas and restrictions in the *AWS Billing User Guide*.

Topics

- Budgets
- Budget reports
- Cost Explorer
- AWS Cost Anomaly Detection
- AWS Pricing Calculator
- Billing View
- AWS Billing and Cost Management Dashboards

Budgets

Number of free budgets with actions per account	2
Number of actions per budget	10
Number of budget actions per account	100
Total number of budgets per management account	20,000
Total number of budgets using a custom billing view	150
Characters allowed in a budget name	• `0-9` • `A-Z` and `a-z`

	• Space • The following symbols: _ . : / = + - % @

Budget reports

Maximum number of budget reports	50
Maximum number of budgets per budget report	50
Maximum email recipients in a budget report	50

Cost Explorer

Maximum number of reports that you can save per account	300
Maximum number of filters in the `GetCostAndUsage` operation (API)	100

AWS Cost Anomaly Detection

AWS Managed Monitor Quotas

AWS managed monitor for AWS services per account (management and member)	1
Additional AWS managed monitors (linked account, cost allocation tag, or cost category) per management account	1
Total AWS managed monitors per management account	2

Total AWS managed monitors per member account	1
Values tracked per AWS managed monitor	5,000

Customer Managed Monitor Quotas

Total customer managed monitors per management account	500
Values per customer managed monitor (linked accounts or tag values)	10
Values per customer managed monitor (cost category values)	1

General Quotas (Apply to Both)

Alert subscriptions per account	100
Email recipients per subscription	10
Amazon SNS topics per subscription	1
Monitors per alert subscription	502 maximum (all monitors can be attached)
Time to detect anomaly after usage	Up to 24 hours
Historical data required for detection	10 days minimum
Unsupported services	• AWS Marketplace (except third-party foundation models on Amazon Bedrock) • AWS Support • WorkSpaces • Cost Explorer • Budgets

	• AWS Shield • Amazon Route 53 • AWS Certificate Manager • Only analyzes Usage charge type and NetUnblendedCost

AWS Pricing Calculator

Maximum number of workload estimates an account can create in a month	50
Maximum number of modifications that can be made in a single workload estimate	350
Maximum number of usage lines that can be added to a single workload estimate	2000
Maximum number of usage lines that can be added to a single bill estimate	2000

Billing View

Maximum number of billing views that you can create per account	3000

AWS Billing and Cost Management Dashboards

Maximum number of widgets per dashboard	20
Maximum number of dashboards per account	50
Maximum number of scheduled reports per account	100

Minimum schedule frequency	Hourly
Maximum schedule period (endTime)	3 years from current time
Pre-signed URL expiry (report download link)	15 days

Document history

The following table describes the documentation for this release of the AWS Cost Management console.

Change	Description	Date
Launching Amazon Bedrock product attributes	You can now filter and group your Amazon Bedrock costs by product attributes (provider, model, inference type, and feature) in Cost Explorer and Dashboards, and filter budgets by these attributes in AWS Budgets.	October 8, 2026
Updated AWS managed policies	Updated the following managed policies. • AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	April 7, 2026
Launching user attributes for cost allocation	User attributes for cost allocation enables you to allocate costs based on user attributes from AWS IAM Identity Center. Introduced the following managed policy: AWSUserAttributeCostAllocationPolicy.	December 15, 2025
Launching Cost efficiency metric in Cost Optimization Hub	Cost efficiency is a metric that measures how effectively a customer is optimizing their AWS cloud resources.	November 19, 2025

AWS Cost Anomaly Detection expands AWS managed monitoring	AWS Cost Anomaly Detection now enables you to monitor all linked accounts, cost allocation tags, or cost categories with a single AWS managed monitor.	November 19, 2025
Enhanced cost management capabilities in Amazon Q	Amazon Q now provides enhanced cost managemen t capabilities, including improved analytical capabilit ies and additional service integrations.	November 18, 2025
Launched pricing capabilities in Amazon Q Developer	You can use Amazon Q Developer, the generativ e AI assistant for AWS, to understand service pricing and estimate the cost of new workloads.	October 8, 2025
AWS Billing and Cost Management Dashboards	Added AWS Billing and Cost Management Dashboards to create customized views combining AWS cost and usage data in a single page. You can now add multiple visualization widgets and share dashboards across accounts.	August 19, 2025

Updated AWS managed policies	Updated the following managed policies. • AWSBudgetsActionsWithAWSResourceControlAccess • AWSBudgetsReadOnlyAccess	August 15, 2025
Updated AWS managed policies	Updated the following managed policies. • AWSBudgetsActionsWithAWSResourceControlAccess • AWSBudgetsReadOnlyAccess	August 15, 2025
AWS Billing and Cost Management Recommended Actions	Added 6 new recommended actions to the existing list of 15 recommended actions in the console. All recommended actions are now categorized as critical, advisory, or informational, enabling you to prioritize and resolve any identified billing issues.	August 15, 2025
Added the ability to create budgets with billing views	You can create budgets based on billing views from your own account or from billing views that have been shared with you. • Viewing and creating budgets using billing views • BudgetsServiceRolePolicy	August 6, 2025

Updated AWS managed policy	Cost Optimization Hub updated the CostOptimizationHubServiceRolePolicy.	July 23, 2025
Launched cost optimization capability in Amazon Q Developer	You can use Amazon Q Developer, the generative AI assistant for AWS, to identify cost-saving opportunities from Cost Optimization Hub, AWS Compute Optimizer, and Savings Plans and reservation recommendations.	June 2, 2025
Added Amazon Aurora recommendations to Cost Optimization Hub	Cost Optimization Hub supports instance and cluster storage recommendations for Amazon Aurora databases	June 2, 2025
In-console AWS Pricing Calculator	Added a new in-console Pricing Calculator feature that enables you to estimate your planned cloud costs using your discount and purchase commitments.	May 29, 2025
New Cost Comparison in AWS Cost Explorer	Added the capability for customers to gain insights into monthly cost changes across their organization and identify key drivers of spending changes.	May 28, 2025
Added commitment preferences in Cost Optimization Hub	Added the capability to customize preferred term length and payment options for reservations and Savings Plans recommendations.	May 28, 2025

Advanced alerting through AWS User Notifications in AWS Cost Anomaly Detection	Added the capability for customers to create enhanced alerting capabilities in the AWS User Notifications console.	May 20, 2025
Added new features in AWS Budgets	Added new budget filtering capabilities and cost metrics to better track and manage your costs.	April 29, 2025
Added MemoryDB and DynamoDB reservation recommendations to Cost Optimization Hub	Added cost optimization recommendations for MemoryDB reserved instances and DynamoDB reserved capacity.	April 8, 2025
Added EC2 Auto Scaling group recommendations to Cost Optimization Hub	Added cost optimization recommendations for EC2 Auto Scaling groups, including those with single and mixed instance types.	February 6, 2025
New Billing View	Added a new Billing View feature that allows you to share visibility to cloud finance data, enabling teams to access relevant cost management data across multiple member accounts.	December 20, 2024
Launched cost analysis capability in Amazon Q Developer (GA)	You can use Amazon Q Developer, the generative AI assistant for AWS, to retrieve and analyze your cost data from AWS Cost Explorer.	November 26, 2024

Enhanced root cause analysis in AWS Cost Anomaly Detection	Added the capability for faster anomaly resolution with enhanced root cause analysis in AWS Cost Anomaly Detection.	November 24, 2024
In-console AWS Pricing Calculator (Preview)	Added a new in-console Pricing Calculator feature that enables you to estimate your planned cloud costs using your discount and purchase commitments.	November 22, 2024
Added DynamoDB reservation recommendations to Cost Explorer	You can purchase recommendations for Amazon DynamoDB reserved capacity, allowing you to cover your provisioned capacity with reserved capacity at a discounted rate.	September 18, 2024
Added delegated administrator for Cost Optimization Hub	You can delegate a member account in your organization as an administrator for Cost Optimization Hub.	August 6, 2024
Updated AWS managed policy	Cost Optimization Hub updated the CostOptimizationHubServiceRolePolicy.	July 5, 2024
Updated AWS managed policy	Updated the AWSBudgetsReadOnlyAccess policy.	June 17, 2024
Added AWS managed policy	Data Exports added the AWSBCMDataExportsServiceRolePolicy.	June 10, 2024

Launched cost analysis capability in Amazon Q (preview)	You can use Amazon Q, the generative AI assistant for AWS, to retrieve and analyze your cost data from AWS Cost Explorer.	April 29, 2024
Added AWS managed policy	Split cost allocation data added the SplitCostAllocationDataServiceRolePolicy.	April 16, 2024
Updated AWS managed policy	Updated the AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM policy.	December 14, 2023
Updated AWS managed policies	Cost Optimization Hub updated the following two managed policies: • CostOptimizationHubReadOnlyAccess • CostOptimizationHubAdminAccess	December 14, 2023

Updated documentation	For an overview of your AWS cloud financial management data, use the AWS Billing and Cost Management widgets on the Billing and Cost Management home page. See the following updates: • Using the AWS Billing and Cost Management home page • Understanding the differences between AWS Billing data and AWS Cost Explorer data	November 26, 2023
New Cost Optimization Hub	Added a new Cost Optimization Hub feature that helps you consolidate and prioritize cost optimization recommendations across your AWS accounts and AWS Regions.	November 26, 2023
Added AWS managed policy	Cost Optimization Hub added the CostOptimizationHubServiceRolePolicy.	November 26, 2023
Updated documentation	Updated information about how to use the affected IAM policies tool.	November 17, 2023
Added multi-year and granular data to Cost Explorer	You can now enable up to 38 months of multi-year data (at monthly granularity) and more granular data (at hourly and daily granularity) for the previous 14 days.	November 16, 2023

New AWS Cost Anomaly Detection anomaly monitors limit	Increased the number of anomaly monitors you can create for other monitor types (linked account, cost category, cost allocation tag).	September 12, 2023
New AWS Cost Anomaly Detection configuration by default	Added automatic configuration of AWS Cost Anomaly Detection for all new AWS Cost Explorer users.	March 27, 2023
New AWS Cost Anomaly Detection percentage-based thresholds	Added support for percentage-based thresholds in AWS Cost Anomaly Detection for anomaly alerting.	December 15, 2022
New AWS Cost Anomaly Detection details in alert notifications	Added important details such as account name, monitor name, and monitor type in alert emails, the console, and notifications sent through SNS to Slack or Chime.	December 8, 2022
New templates and tutorials in AWS Budgets	Added a new feature to create a budget using a template with recommended configurations as well as walk-through tutorials to learn about creating different kinds of budgets.	September 27, 2022
New AWS Cost Anomaly Detection history values	Added information about new values in the AWS Cost Anomaly Detection history tab into the AWS Cost Management guide to align with the console.	August 16, 2022

New split-view panel in AWS Budgets	Added a new feature to enhance the console experience by adding a split-view panel that allows you to view budget details without leaving the Budgets Overview page.	June 15, 2022
New AWS Cost Management guide	Split the Billing and Cost Management user guide and aligned the feature details into the Billing guide and AWS Cost Management guide to align with the console.	October 20, 2021
New AWS Cost Anomaly Detection	Added a new AWS Cost Anomaly Detection feature that uses machine learning to continuously monitor your cost and usage to detect unusual spends.	December 16, 2020
Updated AWS managed policies	Cost Optimization Hub updated the following two managed policies: • CostOptimizationHubReadOnlyAccess • CostOptimizationHubAdminAccess	November 19, 2020
Launched RI/SP Sharing in AWS Pricing Calculator	You can specify a group sharing preference in Bill Estimates for designating reserved instance and savings plans sharing settings.	November 19, 2020

New Purchase Order Management	Added a new purchase order feature to configure how your purchases are reflected on your invoices.	October 15, 2020
New Budget Actions	Added a new AWS Budgets actions feature to run an action on your behalf when a budget exceeds a certain cost or usage threshold.	October 15, 2020
New China bank redirect payment method	Added a new payment method that allows China CNY customers using AWS to pay their overdue payments using China Bank Redirect.	February 20, 2020
New security chapter	Added a new security chapter that provides informati on about various security controls. Former "Controlling Access" chapter contents have been migrated here.	February 6, 2020
New reporting method using AWS Budgets	Added a new reporting functionality using AWS Budgets reports.	June 27, 2019
Added normalized units to AWS Cost Explorer	AWS Cost Explorer reports now include normalized units.	February 5, 2019
New payment behavior	AWS India customers can now enable the auto-charge ability for their payments.	December 20, 2018
Updated the AWS Cost Explorer UI	Updated the AWS Cost Explorer UI.	November 15, 2018

Added budget history	Added the ability to see the history of a budget.	November 13, 2018
Expanded budget services	Expanded RI budgets to Amazon OpenSearch Service.	November 8, 2018
Added a new payment method	Added the SEPA Direct Debit payment method.	October 25, 2018
Redesigned budget experience	Updated the budget UI and workflow.	October 23, 2018
New Reserved Instance recommendation columns	Added new columns to the AWS Cost Explorer RI recommendations.	October 18, 2018
Added a new Reserved Instance report	Expanded RI reports to Amazon OpenSearch Service.	October 10, 2018
AWS Cost Explorer walkthrough	AWS Cost Explorer now provides a walkthrough for the most common functionality.	September 24, 2018
Added a new payment method	Added the ACH Direct Debit payment method.	July 24, 2018
Added RI purchase recommendations for additional services	Added RI purchase recommendations for additional services in AWS Cost Explorer.	July 11, 2018
Added RI purchase recommendations for linked accounts	Added RI purchase recommendations for linked accounts in AWS Cost Explorer.	June 27, 2018
Added AWS CloudFormation for budgets	Added Budgets templates for AWS CloudFormation.	May 22, 2018

Updated RI allocation behavior for linked accounts	Updated the RI allocation behavior size-flexible RI for linked accounts.	May 9, 2018
RI coverage alerts	Added RI coverage alerts.	May 8, 2018
Unblend linked account bills	Linked account bills no longer show the blended rate for the organization.	May 7, 2018
Added Amazon RDS recommendations to AWS Cost Explorer	Added Amazon RDS Recommendations to AWS Cost Explorer.	April 19, 2018
Added a new AWS Cost Explorer dimension and AWS Cost and Usage Reports line item	Added a new AWS Cost Explorer dimension and AWS Cost and Usage Reports line item.	March 27, 2018
Added purchase recommendations to the AWS Cost Explorer API	Added access to the Amazon EC2 Reserved Instance (RI) purchase recommendations via the AWS Cost Explorer API.	March 20, 2018
Added RI coverage for Amazon RDS, Amazon Redshift, and ElastiCache	Reserved Instance (RI) coverage for Amazon RDS, Amazon Redshift, and ElastiCache .	March 13, 2018
Added RI coverage to the AWS Cost Explorer API	Added `GetReservationCoverage` to the AWS Cost Explorer API.	February 22, 2018
RI recommendations	Added RI recommendations based on previous usage.	November 20, 2017
AWS Cost Explorer API	Enabled programmatic access to AWS Cost Explorer via API.	November 20, 2017

RI utilization alerts for additional services	Added notifications for additional services.	November 10, 2017
Added RI reports	Expanded RI reports to Amazon RDS, Redshift, and ElastiCache.	November 10, 2017
Discount sharing preferences	Updated preferences so that AWS credits and RI discount sharing can be turned off.	November 6, 2017
RI utilization alerts	Added notifications for when RI utilization drops below a preset percentage-based threshold.	August 21, 2017
Updated AWS Cost Explorer UI	Released a new AWS Cost Explorer UI.	August 16, 2017
AWS Marketplace data integration	Added AWS Marketplace so that customers can see their data reflected in all billing artifacts, including the Bills page, AWS Cost Explorer, and more.	August 10, 2017
Linked account access and usage type groups in budgets	Added support for creating cost and usage budgets based on specific usage types and usage type groups, and extended budget creation capabilities to all account types.	June 19, 2017

Added AWS Cost Explorer advanced options	You can now filter AWS Cost Explorer reports by additiona l advanced options, such as refunds, credits, RI upfront fees, RI recurring charges, and support charges.	March 22, 2017
Added a AWS Cost Explorer report	You can now track your Reserved Instance (RI) coverage in AWS Cost Explorer.	March 20, 2017
Added AWS Cost Explorer filters	You can now filter AWS Cost Explorer reports by tenancy, platform, and the Amazon EC2 Spot and Scheduled Reserved Instance purchase options.	March 20, 2017
AWS Cost Explorer and budgets for AWS India	AWS India users can now use AWS Cost Explorer and budgets.	March 6, 2017
Added grouping for AWS Cost Explorer usage types	AWS Cost Explorer supports grouping for both cost and usage data, enabling customers to identify their cost drivers by cross-ref erencing their cost and usage charts.	February 24, 2017
Added a AWS Cost Explorer report	You can now track your monthly Amazon EC2 Reserved Instance (RI) utilizati on in AWS Cost Explorer.	December 16, 2016

Added a AWS Cost Explorer report	You can now track your daily Amazon EC2 Reserved Instance (RI) utilization in AWS Cost Explorer.	December 15, 2016
Added AWS Cost Explorer advanced options	You can now exclude tagged resources from your AWS Cost Explorer reports.	November 18, 2016
Expanded budget functionality	You can now use budgets to track usage data.	October 20, 2016
Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by usage type groups.	September 15, 2016
AWS Cost Explorer report manager	You can now save AWS Cost Explorer queries.	November 12, 2015
Budgets and forecasting	You can now manage your AWS usage and costs using budgets and cost forecasts.	June 29, 2015
Amazon Web Services India Private Limited	You can now manage your account settings and payment methods for an Amazon Web Services India Private Limited (AWS India) account.	June 1, 2015
Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by Availability Zone, API operation, purchase option, or multiple cost allocation tags.	February 19, 2015
Preferred payment currencies	You can now change the currency associated with your credit card.	February 16, 2015

Expanded AWS Cost Explorer functionality	You can now use AWS Cost Explorer to visualize your costs by Amazon EC2 instance type or region.	January 5, 2015
User permissions	You can now enable federated users or roles to access and manage your account settings, view your bills, and perform cost managemen t. For example, you can grant people in your finance department full access to the financial setup and control of your AWS account, without having to give them access to your production AWS environment.	July 7, 2014
AWS Cost Explorer launched	AWS Cost Explorer provides a visualization of your AWS costs that enables you to analyze your costs in multiple ways.	April 8, 2014
Version 2.0 published for the Billing guide	The *AWS Billing User Guide* has been reorganized and rewritten to use the new Billing and Cost Management console.	October 25, 2013