AWS Sustainability User Guide

AWS Sustainability

AWS Sustainability: AWS Sustainability User Guide

Table of Contents

What is AWS Sustainability?

Welcome to the AWS Sustainability user guide.

The AWS Sustainability service provides a suite of features to help you understand your environmental impact from using AWS services. The vast majority of accounts with AWS usage can see their environmental impact. If data isn't available for your account, your account may be too new to show data (data is published the month after the usage occurs) or your impact may be immaterial (under 0.5 grams of carbon dioxide equivalent).

Topics

Features of AWS Sustainability

The AWS Sustainability service includes the following features:

- **Carbon emissions** — Visualize your carbon emissions over time. Deep dive into your emissions by scope, AWS Region, service, and more.
- **Reports** — Access your sustainability data in bulk. Create .csv reports to quickly see your data, integrate with the AWS Sustainability API, or create an ongoing data export (in Data Exports).
- **Release notes** — Learn about new features, methodology updates, bug fixes, and more.

Calculation methodology

The calculation methodology behind all the figures shown in the AWS Sustainability service is explained in the *Calculation methodology* section of this user guide.

Related services

AWS Organizations

If you're signed in as a management account of AWS Organizations, the AWS Sustainability service will report the consolidated environmental impact of all the member accounts within that management account, for the duration that those member accounts were a part of your organization.

If you're signed in as a member account, the AWS Sustainability service will report emission data for the member account only.

For more information, see the AWS Organizations User Guide.

Data Exports

AWS Data Exports enables you to create billing and cost management data exports and carbon emissions data exports using basic SQL, and visualize data by integrating with Amazon QuickSight.

For more information, see What is AWS Data Exports?

Key concepts

Described below are the key concepts and terms that apply to all visualizations within the AWS Sustainability console and the corresponding API.

Unit of measure

The unit of measurement for carbon emissions is metric tons of carbon dioxide-equivalent (MTCO2e), an industry-standard measure. This measurement considers multiple greenhouse gases, including carbon dioxide, methane, and nitrous oxide. All greenhouse gas emissions are converted to MTCO2e using their respective Global Warming Potential (GWP) values as defined by the Intergovernmental Panel on Climate Change (IPCC). This standardized approach enables organizations to express the climate impact of various greenhouse gases in a single, comparable unit.

Publishing timing

Carbon emissions data is available back to January 2022, though we limit how many records are displayed in the **Carbon emissions** page to maintain legibility of the data (the full historical

dataset can be accessed via API or Data Exports). New data is published monthly by the 21st of the month following the usage (e.g. January data is published by February 21st).

Data resolution

The AWS Sustainability service shows your carbon footprint at the 0.000001 MTCO2e (1 gram CO2e) resolution. If your emissions are lower than 0.0000005 MTCO2e (0.5 gMTCO2e) in the reporting month, it will appear as `0`.

AWS Region

AWS services are hosted in multiple locations world-wide. These locations are composed of AWS Regions, Availability Zones, Local Zones, and Wavelength Zones. Each Region is a separate geographic area. The AWS Sustainability service shows the environmental impact associated with each applicable AWS Region. For example, `US East (Ohio)`, `Europe (London)`. Emissions from global services, such as Amazon CloudFront, are reported under `Global`.

Services

AWS offers a broad set of services including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications. The AWS Sustainability service metrics include impact from all AWS Services. Currently, Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), and Amazon CloudFront are broken out in the AWS Sustainability console, while all other products are displayed as **Other**.

Fiscal year

By default, the AWS Sustainability service uses calendar year (January to December) for quarter and year aggregations. You can customize your own fiscal year if it differs from calendar year, for example, March to February. The label for this field corresponds to the year of the ending month. For example, a fiscal year that runs from March 2025 to February 2026 will be shown as FY 2026. Fiscal quarters are calculated from the fiscal year starting month. For example, for a fiscal year that runs from March 2025 to February 2026, Q1 will be March, April, and May 2025.

Methodology version

The environmental data presented in the AWS Sustainability service reflects the most recent methodology version available for a given month. When AWS releases a new version of the methodology, the release notes page is updated with information about the changes and historical data is recalculated using the updated version to ensure accurate comparisons over time. If you want to keep data calculated using previous versions of the methodology we recommend creating a Data Export, which exports your carbon data to Amazon S3. When a new version is released it has its own prefix and previous versions remain available.

AWS Organizations

If you're signed in as a management account of AWS Organizations, the AWS Sustainability service will report the consolidated environmental impact of all the member accounts within that management account, for the duration that those member accounts were a part of your organization. The field **usage account** shows the breakdown of each account with usage within the management account, so you can understand where your environmental impact comes from.

If you're signed in as a member account, the AWS Sustainability service will report emission data for the member account only.

Resources

This page compiles a non-exhaustive list of sustainability resources that may be helpful as you embark on your sustainability journey.

Carbon accounting

- Standards informing the data in the AWS Sustainability service
  - GHG Protocol and its underlying standard ISO 14064: Explore the globally recognized framework for measuring and managing greenhouse gas emissions that forms the basis of corporate carbon accounting.
  - GHG Protocol Product Life Cycle Accounting and Reporting Standard and associated Information and Communication Technology (ICT) sector guidance: Access comprehensive guidance on calculating product-level emissions throughout their lifecycle, with specific considerations for technology products and services.
  - ISO 14040 and ISO 14044 for Life Cycle Assessment (LCA): Review the international standards that establish principles and frameworks for conducting thorough environmental life cycle assessments.
  - GHG Protocol Scope 2 Guidance: Understand how to account for indirect emissions from purchased electricity, steam, heating, and cooling in your carbon footprint calculations and the differences between location-based and market-based emissions.
- AWS customer carbon footprint methodology: Discover how AWS calculates and reports the carbon footprint associated with your cloud usage, including the specific assumptions and data sources used.

- AWS customer carbon footprint methodology assurance letter: View the independent third-party verification letter that validates the accuracy and reliability of AWS's carbon footprint calculation approach.

Sustainability on AWS

- Sustainable cloud computing on AWS: Explore how AWS's cloud infrastructure helps organizations reduce their environmental impact while maintaining performance and innovation.
- AWS Sustainability service product page: Get an overview of the AWS Sustainability service and its key benefits.
- Sustainability Pillar - AWS Well-Architected Framework: Learn best practices for designing and operating cloud workloads that minimize environmental impact while meeting business requirements.

Amazon's sustainability goals and programs

- AWS Cloud sustainability: Discover AWS's commitment to sustainable operations, including renewable energy initiatives and efficiency improvements across data centers.
- Amazon sustainability: Learn about Amazon's broader environmental goals, including the path to net-zero carbon and investments in renewable energy and circular economy initiatives.
- The Climate Pledge: Learn about the commitment co-founded by Amazon to achieve net-zero carbon emissions by 2040, a decade ahead of the Paris Agreement.
- Amazon's sustainability exchange: Access Amazon's platform for sharing sustainability insights, best practices, and collaborative solutions across the business community.
- Amazon's carbon credit service: Explore how Amazon helps organizations invest in verified carbon removal and reduction projects to offset their remaining emissions.

Prerequisites

Before you use the AWS Sustainability service for the first time, complete the following tasks.

Topics

Have an AWS account with usage

In order to see data in the AWS Sustainability console, you need to have usage of AWS services, otherwise your environmental impact will be zero. The console shows data at the 0.000001 metric tons of carbon dioxide equivalent (MTCO2e), or 1 gram, resolution. If you have AWS usage but the console shows zero, it means your impact is lower than 0.5 grams of CO2e.

Set up IAM access

You must have the following IAM permissions in order to access your carbon emission data from AWS Sustainability. For more information regarding IAM permissions, see the section called "Identity and access management"

- `sustainability:GetEstimatedCarbonEmissions`
- `sustainability:GetEstimatedCarbonEmissionsDimensionValues`

Getting started with AWS Sustainability

This section provides information that you need to get started with using the AWS Sustainability console. Make sure you've met the prerequisites before you start. You can also customize your AWS Sustainability preferences.

Topics

Step 1: Review your environmental impact

Use features in the AWS Sustainability console to view your estimated environmental impact. The AWS Sustainability service publishes data monthly for the previous usage month (for example, data for October usage is published in November). Sustainability data is published by the 21st day of the month.

To open the AWS Sustainability console and view your environmental impact

1. Sign into the AWS Management Console and open the AWS Sustainability console at https://console.aws.amazon.com/sustainability/.
2. Choose **Carbon emissions** to see details about your estimated carbon emissions from using AWS.
3. Choose **Reports** to download csv reports with your environmental impact.
4. Choose **Release notes** to see the history of feature releases, bug fixes, methodology updates, and more.

For more information about the calculation methodology behind the numbers shown in the AWS Sustainability service, see *Calculation methodology*.

Step 2: Programmatically access your sustainability data

In addition to using the dashboards in the AWS Sustainability console to see your environmental impact, you have two ways to get your sustainability data programmatically. We recommend you use one of these options if you want to see your data with the maximum granularity available. For example, if you need data broken out by month, usage account, and AWS Region, for several years, getting your data programmatically is the best solution.

1. Call the AWS Sustainability API. See the AWS Sustainability API Reference to learn how.
2. Create a data export to send your monthly data to the S3 bucket of your choice. See *Get your data in bulk* to learn how.

Step 3: (Optional) Configure your fiscal year

By default, the AWS Sustainability service shows yearly visualizations using the calendar year (January to December). You can configure a different fiscal year in the **Settings** page within the console if you want to see your data aggregated differently (for example, you can set up your fiscal year to be March to February).

Next steps

Learn more about AWS Sustainability:

- Key concepts: the section called “Key concepts”
- Carbon emissions: *Use the console visualizations*
- Reports: *Get your data in bulk*
- Calculation methodology: *Calculation methodology*
- Calculate your energy usage: *Calculate your energy usage*

Use the console visualizations

The **carbon emissions** page provides estimates of the carbon emissions associated with your AWS products and services. The estimates include the full range of AWS services, and are provided in metric tons of carbon dioxide-equivalent (MTCO2e).

> **Note**
>
> Learn about new features, methodology updates, bug fixes, and more in the Release notes page in the AWS Sustainability console, accessible in the left navigation bar.

Topics

Your carbon emissions summary

This section shows your estimated AWS emissions and estimated emissions savings, calculated using both the market-based (MBM) and location-based methods (LBM). MBM reflects supplier-specific emissions intensity after accounting for Energy Attribute Certificates (EACs), such as AWS' carbon-free energy purchases. LBM reflects the average emissions intensity of the grid where energy consumption occurs.

Emissions savings are the difference between the carbon footprint emissions calculated using LBM and MBM. For more information about LBM and MBM, see the section called “Input data”.

Emissions by scope

This section shows your breakdown of emissions by Greenhouse Gas Protocol's three scopes, using both the MBM and LBM methods.

- **Scope 1**: Emissions are direct emissions from owned or controlled sources.

- **Scope 2**: Emissions are indirect emissions from the production of purchased energy.
- **Scope 3**: Emissions are all indirect emissions (not included in scope 2) that occur in the value chain of the reporting company, including both upstream and downstream emissions (for example, manufacturing of hardware, end-of-life emissions).

For the calculation methodology for each scope see *Calculation methodology*.

Carbon emissions graphs

These two charts present your carbon emissions estimates over time. It uses a stacked bar chart by default, and you can also see your data in an area chart or table formats by selecting the corresponding buttons in the top right corner of the chart. Similarly, the chart shows your emissions grouped by service by default, but you can see emissions grouped by AWS Region or usage account using the **Parameters** panel on the right side of the console.

To access your data in bulk, visit *Get your data in bulk*.

Modify your charts

You can modify your charts using the **Parameters** panel on the right hand side of the console.

Date range and granularity

By default, the console shows the last 12 months of data at a monthly grain. Use the calendar to select a different timeframe, and the **Granularity** drop down to choose a different time aggregation (monthly, quarterly, yearly). Data is available since January 2022, however, to preserve the quality of the visualizations we limit the amount of data points shown at once, as described below.

- Monthly: You can see up to 36 months of data at once.
- Quarterly: You can see up to 36 quarters at once.
- Yearly: You can see data for usage since 2022.

If your company uses a fiscal year that differs from the calendar year (January to December), you can configure it on the **Settings** page, accessible in the left navigation menu in the console, and see your data grouped by fiscal year or fiscal quarter. The fiscal year displayed corresponds to the end

year of your range. For example, if your fiscal year is March 2025 to February 2026, the fiscal year will be displayed as FY2026. Fiscal quarters are calculated from the fiscal year starting month. For example, for a fiscal year that runs from March 2025 to February 2026, Q1 will be March, April, and May 2025.

Group by

By default, the console graphs are aggregated by service. You can also aggregate by Region. If you are logged in as the management account you can also group by Usage account.

Filters

This section lets you filter the data based on your needs. Once you've selected all the filters you want, press Apply at the bottom of the filters. You can reset your filters by clicking **Clear**.

- Service
- Region
- Emissions scope
- Usage account: If you are logged in as a member account, the only usage account will be the member account. If you are logged in as a management account, you will be able to see all usage accounts under the management account.

Get your data in bulk

You have three options to access your data in bulk.

1. Download your data in csv format. See the section called “CSV reports” for details.
2. Access your data via API. See the AWS Sustainability API Reference for details.
3. Create a data export to S3 via Data Exports, a product in the Billing and Cost Management console. See What is AWS Data Exports? for details.

Topics

CSV reports

You can download csv reports in the **Reports** page. There are two preset reports ready to download.

- **Monthly carbon emissions**: This report offers monthly carbon data, both MBM and LBM, with details by AWS Region, service, emissions scope, and carbon-free energy savings.
- **Annual carbon emissions**: This report offers yearly carbon data, both MBM and LBM, with details by AWS Region, service, emissions scope, and carbon-free energy savings.

To download a preset report

1. Select the circle left of the report name and click **Download**.
2. You will be prompted to select a timeframe for the report. If you intend to make year over year comparisons, please select all months in a given year to ensure it is comparable.

You can also create a custom report by clicking **Download custom report** on the top right of the **Reports** page. You can configure which fields to include in the report, the granularity, and any filters you want to apply.

The columns available to select vary depending on the parameters you have set up for your report. For example, if you choose to aggregate data at the yearly granularity, the column usage_year will

be available, but not usage_month or usage_quarter. If you want the most granularity, aggregate by month.

If you want to see the carbon per usage account under a given payer account, you can use the AWS Sustainability API or create a Data Export.

Calculation methodology

The AWS Sustainability service quantifies customer-specific greenhouse gas (GHG) emissions associated with the use of AWS cloud services and covers the full range of said services.

The methodology adopted in the AWS Sustainability service is based on the data sources and allocation methods outlined in the following standards:

- GHG Protocol and its underlying standard ISO 14064
- GHG Protocol Product Life Cycle Accounting and Reporting Standard and associated Information and Communication Technology (ICT) sector guidance.
- ISO 14040 and ISO 14044 for Life Cycle Assessment (LCA)

The carbon emissions calculation methodology uses elements from these standards to define our system boundaries, input data, and allocation approach and is updated over time based on evolving data, climate science, and more. To see the full methodology document for the current version of the methodology and the third-party verification letter see Reports on the *Amazon Sustainability* page. When AWS releases a new version of the methodology, historical data is recalculated using the updated version to ensure accurate comparisons over time.

Regions, usage, and billing data factors

Electricity grids in different parts of the world use various sources of power. Some use carbon-intense fuels (for example, coal), and some are primarily low-carbon hydro or other renewables. The locations of Amazon's carbon-free energy projects also play a role, because the energy produced by these projects is accounted against our emissions from Regions on the same grid. As a result, not all AWS Regions have the same carbon intensity.

There are some Regions where high usage results in relatively low emissions. There are others where the low usage results in higher emissions. For example, emissions from usage in European AWS Regions often represents a smaller share of total emissions even if that is an area with high usage, because there are more renewables on the grid. AWS Regions in Asia Pacific can represent a larger share of total emissions even when customer usage in those Regions is smaller, given the lower availability of low carbon energy in some Asia Pacific Regions. Carbon estimates are based on usage only, and one-time charges such as upfront Savings Plan purchases, won't result in similar increases in carbon emissions.

AWS Sustainability service and Amazon's carbon footprint report

Amazon's carbon footprint report is a part of our annual sustainability report. It covers Scope 1 through 3 emissions for all Amazon operations, including Amazon Web Services. The customer carbon footprint data available in the AWS Sustainability console provides you with the emissions that are attributable to your own AWS usage. For more information, see Amazon Sustainability.

System boundary

The system boundary defines what activities and related emissions are accounted for in the carbon emissions calculations. The methodology is informed by the GHG Protocol's classification of emissions, which breaks down a company's emissions into three `scopes`.

- **Scope 1**: Emissions are direct emissions from owned or controlled sources.
- **Scope 2**: Emissions are indirect emissions from the production of purchased energy.
- **Scope 3**: Emissions are all indirect emissions (not included in scope 2) that occur in the value chain of the reporting company, including both upstream and downstream emissions (for example, manufacturing of hardware, end-of-life emissions).

Scope 1

The carbon emissions estimates include emissions from fuel combustion in emergency backup generators and emissions from refrigerant use and natural gas consumption in AWS-owned or controlled facilities. This includes locations where AWS has operational control on the server racks deployed that support cloud services (for example, "colo" data centers). The model also includes emissions from certain edge sites (CloudFront emissions are included).

Scope 2

The carbon emissions estimates include Scope 2 emissions from AWS owned or controlled facilities that support cloud services, as well as certain edge sites (For example, CloudFront emissions are included), using both the market-based method (MBM) and location-based method (LBM) calculations.

Scope 3

The carbon emissions estimates account for:

- Emissions from fuel- and energy-related activities (FERA under the GHG Protocol). This includes upstream emissions from purchased fuels and electricity, as well as emissions from transmission and distribution losses, for facilities within the system boundary.
- IT hardware embodied carbon - manufacturing emissions from server racks deployed in AWS-owned or operated data center facilities.
- Data center building embodied carbon - manufacturing emissions from AWS owned or operated data center buildings.
- Non-IT equipment embodied carbon - manufacturing emissions from non-IT equipment deployed in AWS owned or operated data center facilities.

The carbon emissions estimates exclude emissions associated with AWS warehouses, manufacturing facilities, and offices. These emissions are not attributable to the provision of cloud services. Any emissions stemming from sites ran in customer facilities (for example, Amazon Cloud Extension, Embedded Points of Presence, AWS Outposts sites) are not covered at this time. For more information, see the carbon emissions methodology document.

Input data

This section outlines the sources of data and transformations that occur upstream of the AWS Sustainability service to define Scope 1, Scope 2, and Scope 3 carbon emissions for each AWS cluster. To understand the full methodology, see the carbon emissions methodology document.

Scope 1

Amazon generates and assures Scope 1 activity data for its annual footprint every year. To bridge the gap between Amazon's annual reporting and AWS Sustainability service's monthly cadence, AWS uses unassured primary Scope 1 activity data to determine monthly emissions for the current month. Some of the activity data might not be available at the time of publishing the monthly report, therefore translating in an underestimation of Scope 1 emissions. We update our estimates when recasting, to align Scope 1 emissions reported in the AWS Sustainability service with the assured data.

Scope 2

Similar to Scope 1, the carbon emissions methodology closely follows Amazon's footprint methodology. In line with Amazon's approach, we prioritize accuracy of data at the time of publishing in the AWS Sustainability service, only falling back to other sources (for example, estimated energy consumption) when the primary source of data (for example, actual energy consumption) is not reasonably available.

AWS first estimates cluster and month level location-based (LBM) emissions by estimating energy consumption (MWh) and multiplies this by LBM emission factors.

> **Note**
>
> Location-based method (LBM) is a GHG Protocol method used in Scope 2 and Scope 3 FERA carbon emissions accounting that reflects the average emissions intensity of grids where energy consumption occurs.

After LBM, AWS considers market-based contractual instruments such as Energy Attribute Certificates (EACs), Power Purchase Agreements (PPA) etc., to reflect our carbon-free energy projects and calculate market-based (MBM) emissions. This is in line with the Quality Criteria outlined in the GHG Protocol Scope 2 guidance.

> **Note**
>
> Market-based method (MBM) is a GHG Protocol method used in Scope 2 and Scope 3 FERA carbon emissions accounting that reflects supplier-specific emissions intensity after accounting for Energy Attribute Certificates (EACs). For example, a company's carbon-free energy purchases.

To learn more about the differences between LBM and MBM, see GHG Protocol Scope 2 Guidance.

Scope 3

Described below is the input data for each Scope 3 category:

- **Fuel and energy related activities**: For upstream emissions from purchased fuels, AWS collects fuel activity data and applies emission factors for fuel extraction, production, and transportation.

For upstream emissions of purchased electricity and transmission and distribution (T&D) losses using location-based emissions (LBM), AWS multiplies the estimated energy consumption (MWh) by the relevant emission factor. For market-based emissions (MBM), AWS also accounts for Energy Attribute Certificates (EACs).

- **IT hardware**: AWS uses a comprehensive cradle-to-gate approach that tracks emissions from raw material extraction through manufacturing and transportation to AWS data centers. The methodology employs four calculation pathways: process-based life cycle assessment (LCA) with engineering attributes, extrapolation, representative category average LCA, and economic input-output LCA. AWS prioritizes the most detailed and accurate methods for components that contribute significantly to overall emissions.
- **Buildings and equipment**: AWS follows established whole building life cycle assessment (wbLCA) standards, considering emissions from construction, use, and end-of-life phases. The analysis covers data center shells, rooms, and long-lead equipment such as air handling units and generators. The methodology uses both process-based life cycle assessment models and economic input-output analysis to ensure comprehensive coverage.

The Scope 3 emissions are then amortized over the assets' service life (6 years for IT hardware, 50 years for buildings) to calculate monthly emissions that can be allocated to customers. This amortization ensures that we fairly distribute the total embodied carbon of each asset across its operational lifetime, accounting for scenarios such as early retirement or extended use.

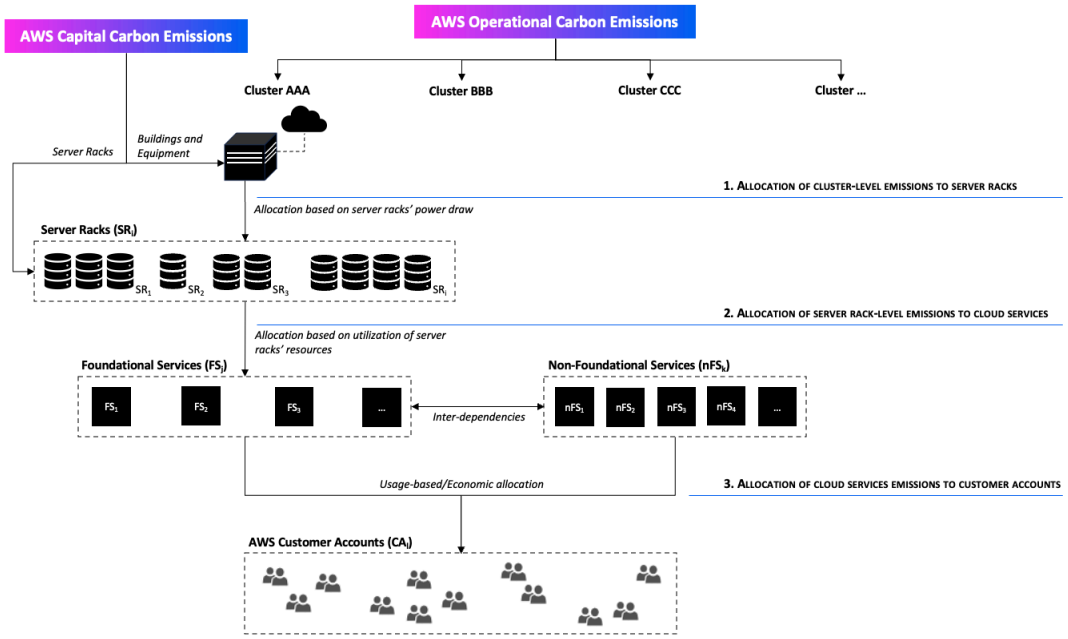
To ensure data quality, we use a Composite Quality Score (CQS) system and perform multiple validation checks throughout our calculation process. This systematic approach lets us provide customers with detailed, verifiable carbon footprint data while maintaining transparency about our calculations and assumptions.

Allocation approach

The carbon allocation model uses a top-down approach to calculate customers' carbon footprint associated with the AWS cloud service usage. AWS prioritizes `physical allocation` (also known as usage-based allocation) and consider `economic allocation` as a secondary option.

The model takes operational and capital emissions associated with each AWS cluster and performs a series of transformations to break down such emissions into several logical segments. Conceptually, the model works using the following logical transformation workflow:

1. Allocate cluster-level emissions (for example, operational carbon emissions as well as building and equipment amortized embodied carbon) to server racks in the cluster, using the server racks' power draw. Add the server racks amortized embodied carbon associated with each rack in that given cluster.
2. Allocate carbon emissions associated with server racks to AWS cloud services based on utilization of server racks resources, accounting for interdependencies. We use physical allocation for services with dedicated server racks, and economic allocation for other services.
3. Allocate carbon emissions associated with each cloud service to individual customer accounts. We use physical allocation for services with dedicated server racks, and economic allocation for other services.



Calculate your energy usage

Note

- The energy data calculated using this method is for informational purposes only. Do not use this information for optimization.
- This method is not supported in the Canada (Central) and Africa (Cape Town) Regions due to their specific power infrastructure.

The AWS Sustainability service provides data to calculate the energy use of your cloud carbon footprint. By combining Scope 2 location-based emissions (LBM) data with publicly available grid emissions factors, you can determine the estimated energy footprint of your AWS workloads. For more information about energy emission factors used by Amazon, see Amazon Carbon Methodology Document.

To determine the estimated energy consumption behind your cloud carbon footprint, divide the Scope 2 location-based emissions by the corresponding grid emissions factor. Be sure to apply unit conversions as needed:

```
Energy consumption = Location-based emissions / Grid emissions factor
```

Example calculation

If the grid emissions factor was 500 kg CO2e/MWh, and your cloud usage generated Scope 2 LBM emissions are 100 MTCO2e in the US West (Oregon) Region in 2025, calculate energy usage as follows:

1. Multiply 100 MTCO2e by 1,000 to convert metric tons to kilograms.
2. Divide the result by the grid emissions factor of 500 kgCO2e for the US West (Oregon) Region.

```
(100 MTCO2e * 1000) / 500 kgCO2e/MWh = 200 MWh
```

Security in AWS Sustainability

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are 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 Sustainability, 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 AWS Sustainability. The following topics show you how to configure AWS Sustainability to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your AWS Sustainability resources.

Topics

Data protection in AWS Sustainability

The AWS shared responsibility model applies to data protection in AWS Sustainability. 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 Sustainability 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 Sustainability

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 Sustainability resources. IAM is an AWS service that you can use with no additional charge.

Topics

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 Sustainability identity and access)
- **Service administrator** - determine user access and submit permission requests (see How AWS Sustainability works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for AWS Sustainability)

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*.

How AWS Sustainability works with IAM

Before you use IAM to manage access to AWS Sustainability, learn what IAM features are available to use with AWS Sustainability.

IAM feature	AWS Sustainability support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	No
Policy condition keys	No
ACLs	No
ABAC (tags in policies)	No
Temporary credentials	Yes

IAM feature	AWS Sustainability support
Principal permissions	Yes
Service roles	No
Service-linked roles	No

To get a high-level view of how AWS Sustainability 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 Sustainability

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 Sustainability

To view examples of AWS Sustainability identity-based policies, see Identity-based policy examples for AWS Sustainability.

Resource-based policies within AWS Sustainability

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 Sustainability

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 Sustainability actions, see Actions Defined by AWS Sustainability in the *Service Authorization Reference*.

Policy actions in AWS Sustainability use the following prefix before the action:

```
sustainability
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
   "sustainability:GetEstimatedCarbonEmissions",
   "sustainability:GetEstimatedCarbonEmissionsDimensionValues"
]
```

To view examples of AWS Sustainability identity-based policies, see Identity-based policy examples for AWS Sustainability.

Policy resources for AWS Sustainability

Supports policy resources: No

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 Sustainability resource types and their ARNs, see Resources Defined by AWS Sustainability in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions Defined by AWS Sustainability .

To view examples of AWS Sustainability identity-based policies, see Identity-based policy examples for AWS Sustainability.

Policy condition keys for AWS Sustainability

Supports service-specific policy condition keys: No

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 Sustainability condition keys, see Condition Keys for AWS Sustainability in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions Defined by AWS Sustainability .

To view examples of AWS Sustainability identity-based policies, see Identity-based policy examples for AWS Sustainability.

ACLs in AWS Sustainability

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.

ABAC with AWS Sustainability

Supports ABAC (tags in policies): No

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 Sustainability

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*.

Cross-service principal permissions for AWS Sustainability

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 Sustainability

Supports service roles: No

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 Sustainability functionality. Edit service roles only when AWS Sustainability provides guidance to do so.

Service-linked roles for AWS Sustainability

Supports service-linked roles: No

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.

Identity-based policy examples for AWS Sustainability

By default, users and roles don't have permission to create or modify AWS Sustainability 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 Sustainability, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for AWS Sustainability in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the AWS Sustainability console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete AWS Sustainability 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 Sustainability console

To access the AWS Sustainability console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS Sustainability 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 Sustainability console, also attach the AWS Sustainability *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": "*"
        }
    ]
}
```

Troubleshooting AWS Sustainability identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Sustainability and IAM.

Topics

- I am not authorized to perform an action in AWS Sustainability
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my AWS Sustainability resources

I am not authorized to perform an action in AWS Sustainability

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `sustainability:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sustainability:GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `sustainability:GetWidget` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

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 Sustainability.

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 Sustainability. 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 allow people outside of my AWS account to access my AWS Sustainability 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 Sustainability supports these features, see How AWS Sustainability 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*.

Compliance validation for AWS Sustainability

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. 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 services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. For more information about your compliance responsibility when using AWS services, see AWS Security Documentation.

Resilience in AWS Sustainability

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.

In the case of a service disruption, AWS Sustainability will fail over to region `us-west-2`. When using the SDK, it is recommended to use the following authentication configuration in order to allow requests to fail over to the secondary region:

```
export AWS_AUTH_SCHEME_PREFERENCE="sigv4a,sigv4"
export AWS_SIGV4A_SIGNING_REGION_SET="*"
```

For more information on SDK Authentication, see Authentication scheme.

Infrastructure Security in AWS Sustainability

As a managed service, AWS Sustainability 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 AWS Sustainability 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 DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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.

Monitoring AWS Sustainability

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Sustainability and your other AWS solutions. AWS provides the following monitoring tools to watch AWS Sustainability, report when something is wrong, and take automatic actions when appropriate:

- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify.
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Monitoring AWS Sustainability with Amazon CloudWatch

You can monitor AWS Sustainability using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

AWS Sustainability Metrics

Dimension	Value
Namespace	AWS/Usage
Metric name	CallCount
Service	AWS Sustainability
Type	API
Resource	GetEstimatedCarbonEmissionsDimensionValues, GetEstimatedCarbonEmissions

Logging AWS Sustainability API calls using AWS CloudTrail

AWS Sustainability is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Sustainability. CloudTrail captures all API calls for AWS Sustainability as events. The calls captured include calls from the AWS Sustainability console and code calls to the AWS Sustainability API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Sustainability. 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 Sustainability, 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.

> **Note**
>
> For resiliency purposes, AWS Sustainability can fail over to a secondary region. During a fail-over event, CloudTrail logs can be found in region us-west-2.

AWS Sustainability information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Sustainability, 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 Sustainability, 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 console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail

- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

All AWS Sustainability actions are logged by CloudTrail and are documented in the AWS Sustainability API Reference. For example, calls to the `GetEstimatedCarbonEmissions` and `GetEstimatedCarbonEmissionsDimensionValues` actions 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 the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding AWS Sustainability 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 example shows a CloudTrail log entry that demonstrates the `GetEstimatedCarbonEmissions` action.


```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "accountId": "111122223333",
    "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "attributes": {
        "creationDate": "2026-03-11T21:15:59Z",
        "mfaAuthenticated": "false"
```

```
      }
    }
  },
  "eventTime": "2026-03-11T21:22:23Z",
  "eventSource": "sustainability.amazonaws.com",
  "eventName": "GetEstimatedCarbonEmissions",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "123.123.123.123",
  "requestParameters": {
    "EmissionsTypes": [
      "TOTAL_LBM_CARBON_EMISSIONS",
      "TOTAL_MBM_CARBON_EMISSIONS",
      "TOTAL_SCOPE_1_CARBON_EMISSIONS",
      "TOTAL_SCOPE_2_LBM_CARBON_EMISSIONS",
      "TOTAL_SCOPE_2_MBM_CARBON_EMISSIONS",
      "TOTAL_SCOPE_3_LBM_CARBON_EMISSIONS",
      "TOTAL_SCOPE_3_MBM_CARBON_EMISSIONS"
    ],
    "GroupBy": [
      "SERVICE"
    ],
    "TimePeriod": {
      "Start": "2025-03-01T00:00:00Z",
      "End": "2026-02-28T23:59:59.999Z"
    },
    "MaxResults": 5000,
    "Granularity": "MONTHLY"
  },
  "responseElements": null,
  "requestID": "abfb58f2-96c0-496c-9b95-9896d6482193",
  "eventID": "36316506-78f7-430d-8e16-fc49da7fb7f5",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}
```

Access AWS Sustainability using an interface endpoint (AWS PrivateLink)

You can use AWS PrivateLink to create a private connection between your VPC and AWS Sustainability. You can access AWS Sustainability as if it were in your VPC, without the use of an internet gateway, NAT device, VPN connection, or Direct Connect connection. Instances in your VPC don't need public IP addresses to access AWS Sustainability.

You establish this private connection by creating an *interface endpoint*, powered by AWS PrivateLink. We create an endpoint network interface in each subnet that you enable for the interface endpoint. These are requester-managed network interfaces that serve as the entry point for traffic destined for AWS Sustainability.

For more information, see Access AWS services through AWS PrivateLink in the *AWS PrivateLink Guide*.

Considerations for AWS Sustainability

Before you set up an interface endpoint for AWS Sustainability, review Considerations in the *AWS PrivateLink Guide*.

AWS Sustainability supports making calls to all of its API actions through the interface endpoint.

Create an interface endpoint for AWS Sustainability

You can create an interface endpoint for AWS Sustainability using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Create an interface endpoint in the *AWS PrivateLink Guide*.

Create an interface endpoint for AWS Sustainability using the following service name:

```
aws.api.us-east-1.sustainability
```

If you enable private DNS for the interface endpoint, you can make API requests to AWS Sustainability using its default Regional DNS name. For example, `sustainability.us-east-1.amazonaws.com`.

Create an endpoint policy for your interface endpoint

An endpoint policy is an IAM resource that you can attach to an interface endpoint. The default endpoint policy allows full access to AWS Sustainability through the interface endpoint. To control the access allowed to AWS Sustainability from your VPC, attach a custom endpoint policy to the interface endpoint.

An endpoint policy specifies the following information:

- The principals that can perform actions (AWS accounts, IAM users, and IAM roles).
- The actions that can be performed.
- The resources on which the actions can be performed.

For more information, see Control access to services using endpoint policies in the *AWS PrivateLink Guide*.

Example: VPC endpoint policy for AWS Sustainability actions

The following is an example of a custom endpoint policy. When you attach this policy to your interface endpoint, it grants access to the listed AWS Sustainability actions for all principals on all resources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "sustainability:GetEstimatedCarbonEmissions",
            "sustainability:GetEstimatedCarbonEmissionsDimensionValues",
         ],
         "Resource":"*"
      }
   ]
}
```

Troubleshooting

The following topics provide troubleshooting advice for errors and issues that you could encounter when using the AWS Sustainability service. If you find an issue that isn't listed here, you can use the feedback button on this page to report it.

For more troubleshooting advice and answers to common support questions, visit the AWS Knowledge Center.

Why do I get an Access Denied error when I access the console?

You need to set up IAM permissions to see data in the AWS Sustainability service. See *Prerequisites* to learn how.

Why are all the numbers zero in the AWS Sustainability console?

In order to see data in the AWS Sustainability console, you need to have usage of AWS services, otherwise your environmental impact will be zero. The console shows data at the 0.000001 metric tons of carbon dioxide equivalent (MTCO2e), or 1 gram, resolution. If you have AWS usage but the console shows zero, it means your impact is lower than 0.5 grams of CO2e.

Why can't I see data for 2021?

You can see your carbon data back to January 2022 or whenever your usage started, whichever happened later.

Why did my data change?

The calculation methodology is updated over time based on evolving data, climate science, and more. We will also update your data to fix any bugs we identify. All updates are documented in the **Release notes** page in the AWS Sustainability console.

What's the difference between LBM and MBM?

LBM and MBM are GHG Protocol methods used in Scope 2 and Scope 3 fuel- and energy- related activities (FERA) carbon emissions. Location-based emissions (LBM) reflect the average emissions

intensity of the grid where energy consumption occurs. Market-based emissions (MBM) reflect supplier-specific emissions intensity after account for Energy Attribute Certificates (EACs), such as AWS' carbon-free energy purchases.

Why is carbon intensity different depending on the AWS Region?

Electricity grids in different parts of the world use various sources of power. Some use carbon-intense fuels (for example, coal), and some are primarily low-carbon hydro or other renewables. The locations of Amazon's carbon-free energy projects also play a role, because the energy produced by these projects is accounted against our emissions from Regions on the same grid. As a result, not all AWS Regions have the same carbon intensity.

Why can’t I see data from older methodology versions?

We publish data using the latest methodology version to ensure your estimated emissions are as accurate as possible. If you create a carbon emissions export on Data Exports, you will be able to preserve historical data calculated with all methodology versions from that point on. Data Exports publishes your data into an S3 bucket, with each methodology version having its own prefix. When a new version is released, historical data calculated using previous versions will remain in your bucket unless you delete it.

> **Note**
>
> We do not maintain previous methodology versions. To access your data from historical versions, you must create a Data Export *before* a new version is released. If this is important to you, create a data export now.

Quotas for AWS Sustainability

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

To view the quotas for AWS Sustainability, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **AWS Sustainability**.

To request a quota increase, see Requesting a Quota Increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the limit increase form.

Your AWS account has the following quotas related to AWS Sustainability.

Name	Quota	Can be increased
Rate of GetEstimatedCarbonEmissions request	10 requests per second	No
Rate of GetEstimatedCarbonEmissionsDimensionValues request	10 requests per second	No

Document history for the AWS Sustainability User Guide

The following table describes changes to the *AWS Sustainability User Guide*. For notifications about these document changes, subscribe to the RSS feed using the link near the top of this page.

To see changes to the feature set in the AWS Sustainability service, visit the **Release notes** page in the AWS Sustainability console.

Latest documentation update: March 31st, 2026

Change	Description	Date
Initial release	This is the first release of the AWS Sustainability User Guide	March 31, 2026