AWS Audit Manager pricing

Pricing summary / tiers

AWS Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance. When you define and launch an assessment based on a framework, Audit Manager will execute a resource assessment for each individual resource, such as your Amazon EC2 instances, Amazon RDS instances, Amazon S3 buckets, or Amazon VPC subnets.

A resource assessment is a process that collects, stores, and manages evidence, which you can use to assess risk and compliance with industry standards and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). With AWS Audit Manager, you pay as you go based on the number of resource assessments performed, with no minimum fees or up-front commitment.

Each resource assessment generates one piece of evidence. Evidence can be one of three types:

- **Snapshot of a resource configuration** captured directly from an AWS service on a daily, weekly, or monthly frequency. You configure the frequency in Audit Manager. Examples of a resource configuration snapshot might be an Amazon VPC route table's list of routes, an RDS instance backup setting, or an S3 bucket encryption policy.
- **User activity** collected from AWS CloudTrail logs that is triggered when a user makes a change to a resource configuration. Some examples of user-driven changes include a route table update, an RDS instance backup setting change, and an S3 bucket encryption policy change.
- **Compliance check result** from AWS Security Hub or AWS Config collected on a periodic basis or when triggered by a change to the resource configuration. Examples of compliance checks are a Security Hub PCI DSS finding or a Config rule evaluation for HIPAA.

Additional charges:

AWS Audit Manager enables you to generate and store audit-ready assessment reports, which contain a summary document and evidence folders, in your S3 buckets. You pay normal Amazon S3 storage charges to store objects in your bucket, such as getting and putting the assessment report data in S3. The charges appear in the Amazon S3 portion of your AWS statement. Enabling AWS Config or AWS Security Hub within Audit Manager for evidence collection is an is an optional recommendation, and if enabled, you will have charges in their portion of the AWS statement. Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales tax. Additionally, enabling the evidence finder feature in Audit Manager triggers ingestion and storage of Audit Manager evidence into AWS CloudTrail Lake. CloudTrail Lake pricing applies.

AWS free tier

AWS Audit Manager offers a free tier for first-time customers. The free tier will expire in two calendar months after the first subscription. The free tier offers 35,000 AWS Audit Manager resource assessments per month for two calendar months.

Pricing

Region:

Europe (London)

Per 1,000 Audit Manager resource assessments per account per Region	$1.25

AWS Pricing Calculator

Calculate your AWS Audit Manager and architecture cost in a single estimate.

Create your custom estimate now »

Pricing examples

Example 1:
You are a first-time customer to AWS Audit Manager and you sign up for the free tier. You launch a PCI DSS assessment in Audit Manager that is active for one month (30 days) with the below resources:

- 20 accounts in one AWS region
- 100 Amazon EC2 instances per account
- 60 Amazon S3 buckets per account
- Free tier: 35,000 resource assessments per month

The following steps or user-driven changes take place:

- 1 EC2 configuration snapshot is set up per day in Audit Manager, which applies to all EC2 instances
- 3 EC2 configuration changes/user activities per day, which applies to all EC2 instances.
- 2 EC2 compliance checks are triggered via Security Hub checks for PCI DSS per day due to configuration changes to each EC2 instance
- 1 S3 configuration snapshot is setup per day in Audit Manager, which applies to all S3 buckets
- 2 S3 configuration changes/user activities per day, which applies to each S3 bucket
- 1 S3 compliance check is triggered via a Security Hub check for PCI DSS per day due to a configuration change to each S3 bucket

AWS Audit Manager resource assessments executed for EC2:

- The number of resource assessments for EC2 per day per account = (1 configuration snapshot + 3 user activities + 2 Security Hub checks) x 100 EC2 instances = 600 resource assessments per day per account
- The total daily resource assessments for EC2 = 20 accounts x 600 resource assessments per day per account= 12,000 resource assessments per day across accounts
- The total **monthly resource assessments for EC2** = 30 days x 12,000 resource assessments per day = **360,000 resource assessments per month**

AWS Audit Manager resource assessments executed for S3:

- The number of resource assessments for S3 per day per account = (1 configuration snapshot + 2 user activities + 1 Security Hub check) x 60 S3 buckets = 240 resource assessments per day per account
- The total daily resource assessments for S3 = 20 accounts x 240 resource assessments per day per account= 4,800 resource assessments per day across accounts
- The total **monthly resource assessments for S3** = 30 days x 4,800 resource assessments per day = **144,000 resource assessments per month**

The total one month cost = $1.25 x (360,000 resource assessments for EC2 + 144,000 resource assessments for S3 – 35,000 resource assessments from free tier)/1,000 = **$586.25**

Example 2:
You are an existing customer of AWS Audit Manager. You run AWS Audit Manager assessments that are active for one month (30 days) with the below resources:

- 100 accounts in one AWS region
- 150 Amazon EC2 instances per account
- 100 Amazon S3 buckets per account

The following steps or user-driven changes take place:

- 1 EC2 configuration snapshot is setup per day in Audit Manager, which applies to all EC2 instances
- 4 EC2 configuration changes/user activities per day, which applies to all EC2 instances.
- 2 EC2 compliance checks is triggered based on an AWS Config rule per day due to configuration changes to each EC2 instance
- 1 S3 configuration snapshot is setup per day in Audit Manager, which applies to all S3 buckets
- 2 S3 configuration changes/user activities per day, which applies to each S3 bucket
- 2 S3 compliance checks are triggered based on an AWS Config rule per day due to configuration changes to each S3 bucket

AWS Audit Manager resource assessments executed for EC2:

- The number of resource assessments for EC2 per day per account = (1 configuration snapshot + 4 user activities + 2 Config rule evaluations) x 150 EC2 instances = 1,050 per day per account
- The total daily resource assessments for EC2 = 100 accounts x 1,050 resource assessments per day per account= 105,000 per day
- The **total monthly resource assessments for EC2** = 30 days x 105,000 resource assessments per day = **3,150,000 resource assessments per month**

AWS Audit Manager resource assessments executed for S3:

- The number of resource assessments for S3 per day per account = (1 configuration snapshot + 2 user activities + 2 Config rule evaluations) x 100 S3 buckets = 500 per day per account
- The total daily resource assessments for S3 = 100 accounts x 500 resource assessments per day per account= 50,000 per day
- The **total monthly resource assessments for S3** = 30 days x 50,000 resource assessments per day = **1,500,000 resource assessments per month**

The total one month cost = $1.25 x (3,150,000 resource assessments for EC2 + 1,500,000 resource assessments for S3)/1,000 = **$5,812.50**

Get Started with AWS

Learn how to start using AWS in minutes

AWS Free Tier

Gain free, hands-on experience with AWS for 12 months

Proven Security to Accelerate Your Innovation

Find the resources you need to build, run, and scale your applications on the most secure cloud computing environment available today »

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