

Cloud Front

Amazon Cloud Front is a web service that gives businesses and web application developers an easy and cost effective way to distribute content with low latency and high data transfer speeds.

Like other AWS services, Amazon Cloud Front is self-service, pay-per-use offering, requiring no long term commitments or minimum fees.

With Cloud Front, your files are delivered to end-users using a global network of edge locations.

Edge location

Cloud Front delivers your content through a worldwide network of data centers called edge locations. The regional edge caches are located between your origin web server and the global edge locations that serve content directly to your viewers. This helps improve performance for your viewers while lowering the operational burden and cost of scaling your origin resources.

Regional Edge cache

They are located between your origin web server and the global edge locations that serve content directly to your viewers. As objects become less popular, individual edge locations may remove those objects to make room for more popular content. Regional Edge Caches have a larger cache width than any individual edge location, so objects remain in the cache longer at the nearest regional edge caches. This

helps keep more of your content closer to your viewers, reducing the need for Cloud Front to go back to your origin web server and improving overall performance for viewers.

Origin Shield-

Cloud Front Origin Shield is an additional layer in the Cloud Front caching infrastructure that helps to minimize your origin's load, improve its availability, and reduce its operating costs.

Benefits:

1. **Better cache hit ratio**- Origin Shield can help improve the cache hit ratio of your Cloud Front distribution because it provides an additional layer of caching in front of your origin. When you use Origin Shield, all requests from all of Cloud Front's caching layers to your origin go through Origin Shield, increasing the likelihood of a cache hit. Cloud Front can retrieve each object with a single origin request from Origin Shield to your origin, and all other layers of the Cloud Front cache (edge locations and regional edge caches) can retrieve the object from Origin Shield.
2. **Reduced origin load**- Origin Shield can further reduce the number of simultaneous requests that are sent to your origin for the same object.
3. **Better network performance**-When you enable Origin Shield in the AWS Region that has the lowest latency to your origin, you can get better network performance. For origins in an AWS Region, Cloud Front network traffic remains on the high throughput Cloud Front network all the way to your origin.

Q. How does Amazon CloudFront speed up my entire website?

Amazon CloudFront uses standard cache control headers you set on your files to identify static and dynamic content. Delivering all your content using a single Amazon CloudFront distribution helps you make sure that performance optimizations are applied to your entire website or web application. When using AWS origins, you benefit from improved performance, reliability, and ease of use as a result of AWS's ability to track and adjust origin routes, monitor system health, respond quickly when any issues occur, and the integration of Amazon CloudFront with other AWS services. You also benefit from using different origins for different types of content on a single site – e.g. Amazon S3 for static objects, Amazon EC2 for dynamic content, and custom origins for third-party content – paying only for what you use.

Q. How is Amazon CloudFront different from Amazon S3?

Amazon CloudFront is a good choice for distribution of frequently accessed static content that benefits from edge delivery—like popular website images, videos, media files or software downloads.

Q. How is Amazon CloudFront different from traditional content delivery solutions?

Amazon CloudFront lets you quickly obtain the benefits of high performance content delivery without negotiated contracts or high prices. Amazon CloudFront gives all developers access to inexpensive, pay-as-you-go pricing – with a self-service model. Developers also benefit from tight integration with other Amazon Web Services. The solution is simple to use with Amazon S3, Amazon EC2, and Elastic Load Balancing as origin servers, giving developers a powerful combination of durable storage and high performance delivery. Amazon CloudFront also integrates with Amazon Route 53 and AWS CloudFormation for further performance benefits and ease of configuration.

Q. What types of content does Amazon CloudFront support?

Amazon CloudFront supports content that can be sent using the HTTP or WebSocket protocols. This includes dynamic web pages and applications, such as HTML or PHP pages or WebSocket-based applications, and any popular static files that are a part of your web application, such as website images, audio, video, media files or software

downloads. Amazon CloudFront also supports delivery of live or on-demand media streaming over HTTP.

Q. Does Amazon CloudFront work with non-AWS origin servers?

Yes. Amazon CloudFront works with any origin server that holds the original, definitive versions of your content, both static and dynamic. There is no additional charge to use a custom origin.

Q. How does Amazon CloudFront enable origin redundancy?

For every origin that you add to a CloudFront distribution, you can [assign a backup origin](#) that can be used to automatically serve your traffic if the primary origin is unavailable. You can choose a combination of HTTP 4xx/5xx status codes that, when returned from the primary origin, trigger the failover to the backup origin. The two origins can be any combination of AWS and non-AWS origins.

Q: Does Amazon CloudFront offer a Service Level Agreement (SLA)?

Yes. The Amazon CloudFront SLA provides for a service credit if a customer's monthly uptime percentage is below our service commitment in any billing cycle

Q: Can I use the AWS Management Console with Amazon CloudFront?

Yes. You can use the AWS Management Console to configure and manage Amazon CloudFront through a simple, point-and-click web interface. The AWS Management Console supports most of Amazon CloudFront's features, letting you get Amazon CloudFront's low latency delivery without writing any code or installing any software.

Q: What tools and libraries work with Amazon CloudFront?

There are a variety of tools for managing your Amazon CloudFront distribution and libraries for various programming languages available in our resource centre.

Q. Can I point my zone apex (example.com versus www.example.com) at my Amazon CloudFront distribution?

Yes. By using Amazon Route 53, AWS's authoritative DNS service, you can configure an 'Alias' record that lets you map the apex or root (example.com) of your DNS name to your Amazon CloudFront distribution. Amazon Route 53 will then respond to each request for an Alias record with the right IP address(es) for your CloudFront distribution. Route 53 doesn't charge for queries to Alias records that are mapped to a CloudFront distribution. These queries are listed as "Intra-AWS-DNS-Queries" on the Amazon Route 53 usage report.

Q. Is regional edge cache feature enabled by default?

Yes. You do not need to make any changes to your CloudFront distributions; this feature is enabled by default for all new and existing CloudFront distributions. There are no additional charges to use this feature.

Q. Can I choose to serve content (or not serve content) to specified countries?

Yes, the Geo Restriction feature lets you specify a list of countries in which your users can access your content. Alternatively, you can specify the countries in which your users cannot access your content. In both cases, CloudFront responds to a request from a viewer in a restricted country with an HTTP status code 403 (Forbidden).

Q. How accurate is your GeoIP database?

The accuracy of the IP Address to country lookup database varies by region. Based on recent tests, our overall accuracy for the IP address to country mapping is 99.8%.

Q. Can I serve a custom error message to my end users?

Yes, you can create custom error messages (for example, an HTML file or a .jpg graphic) with your own branding and content for a variety of HTTP 4xx and 5xx error responses. Then you can configure Amazon CloudFront to return your custom error messages to the viewer when your origin returns one of the specified errors to CloudFront.

Q. How long will Amazon CloudFront keep my files at the edge locations?

By default, if no cache control header is set, each edge location checks for an updated version of your file whenever it receives a request more than 24 hours after the previous time it checked the origin for changes to that file. This is called the "expiration period."

You can set this expiration period as short as 0 seconds, or as long as you'd like, by setting the cache control headers on your files in your origin. Amazon CloudFront uses these cache control headers to determine how frequently it needs to check the origin for an updated version of that file. For expiration period set to 0 seconds, Amazon CloudFront will revalidate every request with the origin server. If your files don't change very often, it is best practice to set a long expiration period and implement a versioning system to manage updates to your files.

Q. How do I remove an item from Amazon CloudFront edge locations?

There are multiple options for removing a file from the edge locations. You can simply delete the file from your origin and as content in the edge locations reaches the expiration period defined in each object's HTTP header, it will be removed. In the event that offensive or potentially harmful material needs to be removed before the specified expiration time, you can use the Invalidation API to remove the object from all Amazon CloudFront edge locations.

Q. Is there a limit to the number of invalidation requests I can make?

If you're invalidating objects individually, you can have invalidation requests for up to 3,000 objects per distribution in progress at one time. This can be one invalidation request for up to 3,000 objects, up to 3,000 requests for one object each, or any other combination that doesn't exceed 3,000 objects.

If you're using the * wildcard, you can have requests for up to 15 invalidation paths in progress at one time. You can also have invalidation requests for up to 3,000 individual objects per distribution in progress at the same time; the limit on wildcard invalidation requests is independent of the limit on invalidating objects individually. If you exceed this limit, further invalidation requests will receive an error response until one of the earlier request completes.

You should use invalidation only in unexpected circumstances; if you know beforehand that your files will need to be removed from cache frequently, it is recommended that you either implement a versioning system for your files and/or set a short expiration period.