AWS Config FAQs - Amazon Web Services

aws.amazon.com (https://aws.amazon.com/config/faq/)

General

Q: What is AWS Config?

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Q: What is a Config Rule?

A Config Rule represents desired configurations for a resource and is evaluated against configuration changes on the relevant resources, as recorded by AWS Config. The results of evaluating a rule against the configuration of a resource are available on a dashboard. Using Config Rules, you can assess your overall compliance and risk status from a configuration perspective, view compliance trends over time and pinpoint which configuration change caused a resource to drift out of compliance with a rule.

Q: What are the benefits of AWS Config?

AWS Config makes it easy to track your resource's configuration without the need for up-front investments and avoiding the complexity of installing and updating agents for data collection or maintaining large databases. Once you enable AWS Config, you can view continuously updated details of all configuration attributes associated with AWS resources. You are notified via Amazon Simple Notification Service (SNS) of every configuration change.

Q: How can AWS Config help with audits?

AWS Config gives you access to resource configuration history. You can relate configuration changes with AWS CloudTrail events that possibly contributed to the change in configuration. This information provides you full visibility, right from details, such as "Who made the change?", "From what IP address?" to the effect of this change on AWS resources and related resources. You can use this information to generate reports to aid auditing and assessing compliance over a period of time.

Q: Who should use AWS Config and Config Rules?

Any AWS customer looking to improve their security and governance posture on AWS by continuously evaluating the configuration of their resources would benefit from this capability. Administrators within larger organizations who recommend best practices for configuring resources can codify these rules as Config Rules, and enable self-governance among users. Information Security experts who monitor usage activity and configurations to detect vulnerabilities can benefit from Config Rules. Customers with workloads that need to comply with specific standards (e.g. PCI-DSS or HIPAA) can use this capability to assess compliance of their AWS infrastructure configurations, and generate reports for their auditors. Operators who manage large AWS infrastructure or components that change frequently can also benefit from Config Rules for troubleshooting.Customers who want to track changes to resources configuration, answer questions about resource configurations, demonstrate compliance, troubleshoot or perform security analysis should turn on AWS Config.

Q: Does the service guarantee that my configurations are never out of compliance?

Config Rules provides information about whether your resources are compliant with configuration rules you specify. It will evaluate rules as soon as updated Configuration Items (http://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#config-item-table) (CIs) for the resource are available within AWS Config. It does not guarantee that resources will be compliant or prevent users from taking non-compliant actions. Further, Config Rules does not automatically snap non-compliant resources back into compliance.

Q: Does the service prevent users from taking non-compliant actions?

Config Rules does not directly affect how end-users consume AWS. It evaluates resource configurations only after a configuration change has been completed and recorded by AWS Config. Config Rules does not prevent the user from making changes that could be non-compliant. To control what a user can provision on AWS and configuration parameters allowed during provisioning, please use AWS Identity and Access Management (IAM) Policies and AWS Service Catalog respectively.

Q: Can rules be evaluated prior to provisioning a resource?

Config Rules evaluates rules after the Configuration Item (CI) for the resource is captured by AWS Config. It does not evaluate rules prior to provisioning a resource or prior to making configuration changes on the resource.

Q: How does AWS Config work with AWS CloudTrail?

AWS CloudTrail records user API activity on your account and allows you to access information about this activity. You get full details about API actions, such as identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service. AWS Config records point-in-time configuration details for your AWS resources as Configuration Items (http://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#config-item-table) (CIs). You can use a CI to answer “What did my AWS resource look like?” at a point in time. You can use AWS CloudTrail to answer “Who made an API call to modify this resource?” For example, you can use the AWS Management Console for AWS Config to detect security group “Production-DB” was incorrectly configured in the past. Using the integrated AWS CloudTrail information, you can pinpoint which user misconfigured “Production-DB” security group.

Q: Can I monitor compliance information of multiple accounts and regions via a central account?

AWS Config makes it easy to monitor compliance status across multiple accounts and regions using the multi-account, multi-region data aggregation (https://docs.aws.amazon.com/config/latest/developerguide/config-concepts.html) capability. You can create a configuration aggregator in any account and aggregate the compliance details from other accounts. This capability is also integrated with AWS Organizations, so you can aggregate data from all accounts within your organization.

Getting started

Q: How do I get started with this service?

The quickest way to get started with AWS Config is to use the AWS Management Console. You can turn on AWS Config in a few clicks. For additional details, see the Getting Started (http://docs.aws.amazon.com/config/latest/developerguide/gs-console.html) documentation.

Q: How do I access my resources’ configuration?

You can lookup current and historical resource configuration using the AWS Management Console, AWS Command Line Interface or SDKs.

For additional details, please refer to AWS Config documentation.

Q: Do I turn on AWS Config regionally or globally?

You turn on AWS Config on a per-region basis for your account.

Q: Can AWS Config aggregate data across different AWS accounts?

Yes, you can set up AWS Config to deliver configuration updates from different accounts to one S3 bucket, once the appropriate IAM policies are applied to the S3 bucket. You can also publish notifications to the one SNS Topic, within the same region, once appropriate IAM policies are applied to the SNS Topic.

Q: Is API activity on AWS Config itself logged by AWS CloudTrail?

Yes. All AWS Config API activity, including use of AWS Config APIs to read configuration data, is logged by AWS CloudTrail.

Q: What time and timezones are displayed in the timeline view of a resource? What about daylight savings?

AWS Config displays the time at which Configuration Items (CIs) were recorded for a resource on a timeline. All times are captured in Coordinated Universal Time (UTC). When the timeline is visualized on the management console, the services uses the current time zone (adjusted for daylight savings, if relevant) to display all times in the timeline view.

Config Rules

Q: What is a resource's configuration?

Configuration of a resource is defined by the data included in the Configuration Item (CI) of AWS Config. The initial release of Config Rules makes the CI for a resource available to relevant rules. Config Rules can use this information along with any other relevant information such as other attached resource, business hours, etc. to evaluate compliance of a resource's configuration.

Q: What is a rule?

A rule represents desired Configuration Item (CI) attribute values for resources and are evaluated by comparing those attribute values with CIs recorded by AWS Config. There are two types of rules:

AWS managed rules: AWS managed rules are pre-built and managed by AWS. You simply choose the rule you want to enable, then supply a few configuration parameters to get started. Learn more (http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html) »

Customer managed rules: Customer managed rules are custom rules, defined and built by you. You can create a function in AWS Lambda that can be invoked as part of a custom rule and these functions execute in your account. Learn more (http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html) »

The quickest way to get started with AWS Config is to use the AWS Management Console. You can turn on AWS Config in a few clicks. For additional details, see the Getting Started (http://docs.aws.amazon.com/config/latest/developerguide/gs-console.html) documentation.

Q: How are rules created?

Rules are typically set up by the AWS account administrator. They can be created by leveraging AWS managed rules – a predefined set of rules provided by AWS or through customer managed rules. With AWS managed rules updates to the rule are automatically applied to any account using that rule. In the customer-managed model, the customer has a full copy of the rule, and executes the rule within his/her own account. These rules are maintained by the customer.

Q: How many rules can I create?

You can create up to 150 rules in your AWS account by default. Additionally, you can request an increase for the limit on the number of rules in your account by visiting the AWS Service Limits (http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_config) page.

Q: How are rules evaluated?

Any rule can be setup as a change-triggered rule or as a periodic rule. A change-triggered rule is executed when AWS Config records a configuration change for any of the resources specified. Additionally, one of the following must be specified:

Tag Key:(optional Value): A tag key:value implies any configuration changes recorded for resources with the specified tag key:value will trigger an evaluation of the rule.

Resource type(s): Any configuration changes recorded for any resource within the specified resource type(s) will trigger an evaluation the rule.

Resource ID: Any changes recorded to the resource specified by the resource type and resource ID will trigger an evaluation of the rule.

A periodic rule is triggered at a specified frequency. Available frequencies are 1hr, 3hr, 6hr, 12hr or 24hrs. A periodic rule has a full snapshot of current Configuration Items (CIs) for all resources available to the rule.

Q: What is an evaluation?

Evaluation of a rule determines whether a rule is compliant with a resource at a particular point in time. It is the result of evaluating a rule against the configuration of a resource. Config Rules will capture and store the result of each evaluation. This result will include the resource, rule, time of evaluation and a link to Configuration Item (CI) that caused non-compliance.

Q: What does compliance mean?

A resource is compliant if complies with all rules that apply to it. Otherwise it is noncompliant. Similarly, a rule is compliant if all resources evaluated by the rule comply with the rule. Otherwise it is noncompliant. In some cases, such as when inadequate permissions are available to the rule, an evaluation may not exist for the resource, leading to a state of insufficient data. This state is excluded from determining the compliance status of a resource or rule.

Q: What information does the Config Rules dashboard provide?

The Config Rules dashboard gives you an overview of resources tracked by AWS Config, and a summary of current compliance by resource and by rule. When you view compliance by resource, you can determine if any rule that applies to the resource is currently not compliant. You can view compliance by rule, which tells you if any resource under the purview of the rule is currently non-compliant. Using these summary views, you can dive deeper into the Config timeline view of resources, to determine which configuration parameters changed. Using this dashboard, you can start with an overview and drill into fine-grained views that give you full information about changes in compliance status, and which changes caused non-compliance.

Multi-account, multi-region data aggregation

Q: What is multi-account, multi-region data aggregation?

Data aggregation in AWS Config allows you to aggregate AWS Config data from multiple accounts and regions into a single account. Multi-Account data aggregation is useful for central IT administrators to monitor compliance for multiple AWS accounts in the enterprise.

Q: Can I use the data aggregation capability to centrally provision Config rules across multiple accounts?

The data aggregation capability cannot be used for provisioning rules across multiple accounts. It is purely a reporting capability that provides visibility into your compliance. You can use CloudFormation StackSets (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html) to provision rules across accounts and regions. Here is a useful blog (https://aws.amazon.com/blogs/aws/use-cloudformation-stacksets-to-provision-resources-across-multiple-aws-accounts-and-regions/).

Q: How do I enable data aggregation in my account?

Once Config and Config rules are enabled in your account, as well as the accounts being aggregated, you can enable data aggregation by creating an aggregator in your account. Learn more (https://docs.aws.amazon.com/config/latest/developerguide/setup-aggregator-console.html).

Q: What is an aggregator?

An aggregator is an AWS Config resource type that collects AWS Config data from multiple accounts and regions. Use an aggregator to view the resource configuration and compliance data recorded in AWS Config for multiple accounts and regions.

Q: What information does the Aggregated view provide?

The Aggregated view displays the total count of non-compliant rules across the organization, the top five non-compliant rules by number of resources, and the top five AWS accounts that have the most number of non-compliant rules. You can then drill down to view more details about the resources that are violating the rule and the list of rules that are being violated by an account.

Q: I am not an AWS Organizations customer. Can I still use the data aggregation capability?

You can specify the accounts to aggregate the Config data from, by uploading a file or by individually entering accounts. Note that since these accounts are not part of any AWS organization, you will need each account to explicitly authorize the aggregator account. Learn more (https://docs.aws.amazon.com/config/latest/developerguide/authorize-aggregator-account-console.html).

Q: I only have a single account, can I still take advantage of the data aggregation capability?

The data aggregation capability is useful for multi-region aggregation as well. So you can aggregate the Config data for your account across multiple regions using this capability.

Q: In what regions is the multi-account, multi-region data aggregation capability available?

The data aggregation capability is available in the following nine regions: US East (N.Virginia), US East (Ohio), US West (Oregon), US West (San Francisco), EU (Ireland), EU (Frankfurt), Asia Pacific (Tokyo), Asia Pacific (Sydney), and Asia Pacific (Singapore).

Q: What if I have an account that includes a region not supported by this feature?

When you create an aggregator, you specify the regions from where you can aggregate data. This list only shows regions where this feature is available. You can also select “all regions”, in which case as soon as support is added in other regions, it will automatically aggregate the data.

Services and region support

Q: What AWS resources types are covered by AWS Config?

Review our documentation (http://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#supported-resources) for a complete list of supported resource types.

Q: What regions is AWS Config available in?

For details on the regions where AWS Config is available, please visit this page:

http://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

Resource configuration

Q: What is a configuration item?

A Configuration Item (CI) is the configuration of a resource at a given point-in-time. A CI consists of 5 sections:

1. Basic information about the resource that is common across different resource types (e.g., Amazon Resource Names, tags),
2. Configuration data specific to the resource (e.g., EC2 instance type),
3. Map of relationships with other resources (e.g., EC2::Volume vol-3434df43 is “attached to instance” EC2 Instance i-3432ee3a),
4. AWS CloudTrail event IDs that are related to this state,
5. Metadata that helps you identify information about the CI, such as the version of this CI, and when this CI was captured.

Q: What are AWS Config relationships and how are they used?

AWS Config takes the relationships among resources into account when recording changes. For example, if a new Amazon EC2 Security Group is associated with an Amazon EC2 Instance, AWS Config records the updated configurations of both the primary resource, the Amazon EC2 Security Group, and related resources, such as the Amazon EC2 Instance, if these resources actually changed.

Q: Does AWS Config record every state a resource has been in?

AWS Config detects change to resource's configuration and records the configuration state that resulted from that change. In cases where several configuration changes are made to a resource in quick succession (e.g. within a span of few minutes), Config will only record the latest configuration of that resource that represents cumulative impact of the set of changes. In these situations, Config will only list the latest change in the *relatedEvents* field of the Configuration Item.This allows users and programs to continue to change infrastructure configurations without having to wait for Config to record intermediate transient states.

Q: Does AWS Config record configuration changes that did not result from API activity on that resource?

Yes, AWS Config will regularly scan configuration of resources for changes that haven't yet been recorded and record these changes. CIs recorded from these scans will not have a *relatedEvent* field in the payload, and only the latest state that is different from state already recorded is picked up.

Q: Does AWS Config record configuration changes to software within EC2 instances?

Yes. AWS Config enables you to record configuration changes to software within EC2 instances in your AWS account and also virtual machines (VMs), or servers in your on-premises environment. The configuration information recorded by AWS Config includes Operating System updates, network configuration, installed applications, etc. You can evaluate whether your instances, VMs, and servers are in compliance with your guidelines using AWS Config Rules. The deep visibility and continuous monitoring capabilities provided by AWS Config allow you to assess compliance and troubleshoot operational issues.

Q: Does AWS Config continue to send notifications if a resource that was previously non-compliant is still non-compliant after a periodic rule evaluation?

AWS Config sends notifications only when the compliance status changes. If a resource was previously non-compliant and is still non-compliant, Config will not send a new notification. If the compliance status changes to “compliant”, you will receive a notification for the change in status.

Q: Can I flag or exempt resources from being evaluated by Config rules?

When you configure Config rules, you can specify whether your rule runs evaluations against specified resource types or resources with a specific tag.

Pricing

Q: How will I be charged for AWS Config and AWS Config rules?
With AWS Config, you are charged based on the number configuration items (CIs) recorded for supported resources in your AWS account. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording.

For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted. You are charged for recording the CI, as it represents the change. There is no additional fee for retaining the CI or any up-front commitment. You can stop recording CIs at any time and continue to access the CIs previously recorded. Charges per CI are rolled up into your monthly bill. See pricing details.

If you are using AWS Config rules, you will be charged a monthly amount based on the number of active AWS Config rules. When a rule runs checks against a resource, the result is recorded as an 'evaluation' based on active AWS Config rules in that month. A rule is considered active if it has one or more evaluations in a month.

Pricing tiers with AWS Config rules are designed to accommodate usage at scale. As rules are evaluated across multiple accounts in your organization during a month, the first 10 active rules in a given Region are charged at $2.00 each, the next 40 active rules are charged at $1.50 each and any additional active rules are charged at $1.00 each. Similar tiers are applied across other Regions. Details on pricing by Region are available on the AWS Config pricing page.

AWS Config also delivers configuration snapshot and history files to your Amazon S3 bucket and sends notifications to your Amazon SNS topic. Standard rates for Amazon S3 and Amazon SNS apply. If you are creating your own AWS Lambda functions for authoring custom AWS Config rules, then standard rates for AWS Lambda apply.

Q: Does the pricing for AWS Config Rules include the costs for AWS Lambda functions?

You can choose from a set of managed rules provided by AWS or you can author your own rules, written as AWS Lambda functions. Managed rules are fully maintained by AWS and you do not pay any additional AWS Lambda charges to run them. Simply enable managed rules, provide any required parameters, and pay a single rate for each active AWS Config rule in a given month. Custom rules give you full control as they are executed as AWS Lambda functions in your account. In addition to monthly charges for an active rule, standard AWS Lambda free tier* and function execution rates apply to custom AWS Config rules.

*AWS Free Tier is not available in the AWS China (Beijing) Region or the AWS China (Ningxia) Region.

Q: I want to change the Lambda function for my custom AWS Config rule. What is the recommended approach?

Charges are incurred whenever a new rule is created and it becomes active. If you need to update or replace the Lambda function associated with a rule, the recommended approach is to update the rule instead of deleting it and creating a new rule.

Q: I want to set up 10 AWS Config rules in two AWS Regions across 100 accounts in each AWS Region. Can you help me understand my monthly costs for AWS Config rules?

With consolidated billing, you will be charged based on tiered pricing in each AWS Region as applicable.

In this example, the maximum cost you can incur if all your rules are active across all accounts is:

10 rules X 100 accounts = 1000 rules per Region

First 10 rules at $2.00 each: = 10 X $2 = $20

Next 40 rules at $1.50 each = 40 X $1.5 = $60

Next 950 rules at $1.00 each = $950

Total possible cost per Region= $20+$60+$950 = $1,030

Total possible cost for 2 Regions = $1,030 X2 = $2,060

Note: Prices are for illustration only. For actual pricing, see AWS Config Pricing Page.

The percentage of rules that are active in a particular month may vary widely. In the above example, if only 30% of total rules in your account were active in a given month, the tiering would only apply for the 300 active rules in the Region, bringing the total cost in that Region to $330.

Partner solutions

Q: What AWS partner solutions are available for AWS Config?

Ecosystem partners such as Splunk, ServiceNow, Evident.IO, CloudCheckr, Redseal Networks and RedHat CloudForms provide offerings that are fully integrated with data from AWS Config. Managed Service Providers, such as 2ndWatch and CloudNexa have also announced integrations with AWS Config. Additionally, with Config Rules, partners such as CloudHealth Technologies, AlertLogic and TrendMicro are providing integrated offerings that can be used by customers. These solutions include capabilities such as change management and security analysis and allow you to visualize, monitor and manage AWS resource configurations.

For more information, click here.

Learn more about AWS Config

Visit the partners page
Ready to build?
Get started with AWS Config (https://console.aws.amazon.com/config/home)

Have more questions?

Contact us

Register for re:Invent Bootcamps

Learn from AWS experts at exam prep bootcamps - space is limited!

(https://reinvent.awsevents.com/learn/bootcamps/?sc_icampaign=aware_reinvent_bootcamps2019_aws&sc_ichannel=ha&sc_icontent=awssm-2448&sc_iplace=2up&trk=ha_awssm-2448)

Get AWS Certified

AWS Certifications can help you advance your career and boost your earning power

(https://pages.awscloud.com/tc_get-aws-certified.html?sc_icampaign=aware_getcertified_evergreen2019&sc_ichannel=ha&sc_icontent=awssm-2655&sc_iplace=2up&trk=ha_awssm-2655)

AWS re:Invent | December 2 – 6, 2019 | Las Vegas, Nevada

Reserved seating opens October 15th. Register now to save your spot. View session catalog ≫

AWS re:Invent

(https://reinvent.awsevents.com/learn/?sc_icampaign=Event_reInvent_2019_1up_DG5_VIP&sc_ichannel=ha&sc_icontent=awssm-3019-a&sc_ioutcome=Strategic_Events&sc_iplace=1up&trk=ha_a131L0000058G7nQAE~ha_awssm-3019~ha_awssm-3019-a&trkCampaign=AWS_reInvent_2019)

Page Content

General Getting started AWS Config Rules Multi-account, multi-region data aggregation Services and region support Resource configuration Pricing Partner solutions

aws.amazon.com (https://aws.amazon.com/config/faq/)