Alibaba Cloud CloudConfig

Product Introduction

Issue: 20200429

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
Courier font	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 What is Cloud Config?

Cloud Config is a specialized service for evaluating resources. Cloud Config tracks configuration changes of your resources and evaluates configuration compliance. Cloud Config can help you evaluate numerous resources and maintain the continuous compliance of your cloud infrastructure.

How Cloud Config works

The following figure shows how Cloud Configure works.

Features

Feature	Description
Manage the monitoring scope	Cloud Config monitors the changes of resources under your account, tracks configuration changes, and evaluates configuration compliance in real time. You can manage the scope of resources to be monitored through simple configuration. If you select all supported resource types and more services are connected to Cloud Config, new resource types supported by Cloud Config are automatically added to the monitoring scope by default. If you customize resource types, the resource types are not automatically added to the monitoring scope.
Manage the resource list	After you activate Cloud Config, you can view the resources of different regions under your account in Cloud Config. You can search for a resource and view the configuration snapshots of the resource. After finding the specified resource, you can go to the management page of the resource in the corresponding cloud service console from Cloud Config to manage the resource.
View the compliance timeline of a resource	Cloud Config records each detailed configuration change of the resources it monitors, and displays the configuration changes over time in a configuration timeline. You can query the events related to each configuration change and event details, including the username, source IP address, time, and API operation name.
Evaluate resource compliance	Cloud Config supports managed rules and custom rules. After configuring rules, you can view the compliance evaluation results and compliance timeline of each resource and re-evaluate non-compliant resources. You can modify, delete, or deactivate the rules that fail to meet your requirements.

Feature	Description
Subscribe to resource events	You can subscribe to resource change events, resource non-compliance events, and resource snapshot delivery events in Cloud Config and receive notifications in a timely manner.
Remediate non-compliant resources	You can specify a remediation template for a rule. When a resource is evaluated by the rule as **Non-compliant**, Cloud Config automatically remediates non-compliant resources. You can also manually remediate non-compliant resources as required.
Store resource snapshots to an OSS bucket	If you specify the target Object Storage Service (OSS) bucket, Cloud Config stores configuration snapshots and compliance evaluation snapshots as objects in the OSS bucket.
Screen resources based on Baseline for Classified Protection of Cybersecurity 2.0	Cloud Config provides the protection screening feature free of charge. The feature monitors the compliance of your cloud resources in an automatic and continuous manner based on Baseline for Classified Protection of Cybersecurity 2.0. The feature simplifies the rectification process and helps you pass the official evaluation with ease.

Benefits

Cloud Config provides the following benefits:

- An aggregated list of resources in multiple regions: Cloud Config displays an integrated view of resources in different regions and allows you to search for resources with ease.
- Configuration change tracking based on operations logs: Cloud Config creates a configuration snapshot for each configuration change and tracks the operation that triggered the change. When an issue occurs, you can easily attribute the issue to a specific change for troubleshooting.
- Continuous compliance evaluation: Cloud Config tracks configuration changes of resources and automatically evaluates configuration compliance. This automates the compliance review process.
- Protection screening based on Baseline for Classified Protection of Cybersecurity 2.0: Cloud Config interprets the specifications of Baseline for Classified Protection of Cybersecurity 2.0 as rules. Before the official evaluation, you can enable continuous protection screening with one-click.

Before you start

Before using Cloud Config, you must familiarize yourself with the following instructions:

- Cloud Config is expanding its monitoring scope to include more Alibaba Cloud services . Currently, Cloud Config only supports some Alibaba cloud services. Therefore, the resource list may only display a part of your resources. After Cloud Config supports a new resource type, the new resource type is automatically added to the monitoring scope. You can later remove the resource type from the monitoring scope as required.
- Cloud Config detects configuration changes at a regular interval of 10 minutes. Cloud Config may fail to identify a change if it occurs and is restored within the same 10-minute interval.
- Data accuracy is not guaranteed when Cloud Config is in public preview. If the resource list, configuration details, or evaluation results displayed in Cloud Config are not as expected or you have other requirements, we recommend that you submit a ticket.

2 Scenarios

If you use large-scale resources, Cloud Config can help you automatically monitor resources and evaluate the configuration compliance of the resources. Cloud Config can help you monitor resources in the following scenarios.

Centralized resource management

The management of resources deployed in different regions poses a huge challenge. Cloud Config aggregates resources of different regions to accelerate the query of resources, and records configuration snapshots of the resources. After you activate Cloud Config, you can view the resources of different regions under your account in Cloud Config. You can search for a resource and view the configuration snapshots of the resource.

Note:
Currently, Cloud Config only supports some Alibaba Cloud services. Therefore, the resource list may only display a part of your resources. Cloud Config will support more Alibaba Cloud services and display more resources in the resource list soon.

Configuration compliance evaluation

After you activate Cloud Config, you can create rules and bind them with specific resource types. You can use managed rules in Cloud Config or create custom rules.

When the configurations of the resources of a specified type change, the rules bound with the resource type are triggered to evaluate the compliance of the configuration changes.

Continuous protection screening based on Baseline for Classified Protection of Cybersecurity 2.0 on the cloud

Cloud Config interprets the specifications of Baseline for Classified Protection of Cybersecurity 2.0 as rules and evaluates resources on the cloud based on the rules. You can enable protection screening based on Baseline for Classified Protection of Cybersecurity 2.0 with one-click. The protection screening feature evaluates resource compliance in a continuous manner. You can also download the protection screening report and provide it as evidence to authorized agencies.

Configuration change tracking and remediation of non-compliant resources

After you activate Cloud Config, Cloud Config records configuration snapshots of your resources every 10 minutes. You can view the configuration changes for each resource.

Cloud Config integrates with ActionTrail. You can view the events for each configurat ion change. This allows you to quickly locate the time point when a configuration error occurred and view the operations log at that time point. In this way, you can quickly locate and troubleshoot issues.

3 Concepts

This topic describes the basic concepts in Cloud Config to help you understand and use this service.

Resource type

Cloud Config is a specialized service for evaluating resources. A resource type is a category of resources. For example, the resource type of an Elastic Compute Service (ECS) instance is Instance. The resource type code is ACS::ECS::Instance. Resources can be divided into the following categories:

- Resources, such as compute instances and storage instances
- Management elements of application products, such as workspaces and workflows
- Management resources related to permissions, such as roles and policies

Resource configuration

You can query the configurations of all resources under the current account through the API operations provided by the corresponding cloud services.

Monitoring scope

The monitoring scope refers to the scope of the resource types to be tracked. The monitoring granularity is the resource type.

- If a resource type is added to the monitoring scope, Cloud Config tracks all resources of this type under the current account and records their configuration snapshots every 10 minutes.
- If a resource type is removed from the monitoring scope, Cloud Config stops recording configuration changes for all resources of this type under the current account.

Configuration timeline

Cloud Config provides you with the configuration timeline for each resource that is monitored.

- If a resource is created before you activate Cloud Config, the start point of the configurat ion timeline is the time when you activate Cloud Config.
- If a resource is created after you activate Cloud Config, the start point of the configurat ion timeline is the time when the resource is created. Cloud Config checks the configurat ion changes every 10 minutes. If a configuration changes at a time point, a node is

generated on the configuration timeline. You can view the configurations, configuration changes, and related operations at the time point.

Rule

A rule is a rule function used to determine whether a resource configuration is compliant. Rules in Cloud Config are developed by using the rule functions created in Function Compute. A rule checks whether the value of an input parameter is as required. Assume that a rule is bound with a resource type in Cloud Config. If the configurations of a resource of this type change, Cloud Config automatically re-evaluates the resource based on the rule and checks whether the configuration changes are compliant. Cloud Config can also trigger rules at the frequency you specify to periodically evaluate the compliance of all resources. For more information about how to manage rules, see #unique_6.

Rules in Cloud Config are divided into two categories.

- Managed rules

  Cloud Config provides you with more than 40 managed rules. For more information, see #unique_7.
- Custom rules

  To create a custom rule, log on to the Function Compute console and create a rule function. When you create a custom rule in the Cloud Config console, enter the Alibaba Cloud Resource Name (ARN) of the rule function. For more information, see #unique_8. You can use custom rules to complete the compliance evaluation in different scenarios.

Compliance timeline

Cloud Config evaluates a resource based on rules if the configurations of the resource change, and generates compliance evaluation records every time. The historical compliance evaluation records are presented in the form of a timeline for the resource. The compliance evaluation records displayed in the compliance timeline depend on the trigger method of rules.

- If the trigger method is Periodic, the compliance timeline displays the records of periodical compliance evaluations.
- If the trigger method is Configuration Changes, the compliance timeline displays the records of compliance evaluations for configuration changes.
- If both trigger methods are selected, the compliance timeline displays the records of all compliance evaluations.

4 Alibaba Cloud services that support Cloud Config

This topic lists the Alibaba Cloud services that support Cloud Config.

Service	Resource type	ARN
Elastic Compute Service	Instance	ACS::ECS::Instance
	Network interface	ACS::ECS::NetworkInterface
	Security group	ACS::ECS::SecurityGroup
	Disk	ACS::ECS::Disk
	Snapshot	ACS::ECS::Snapshot
	Automatic snapshot policy	ACS::ECS::AutoSnapshotPolicy
	Cloud Assistant command	ACS::ECS::Command
	Dedicated host	ACS::ECS::DedicatedHost
	Launch template	ACS::ECS::LaunchTemplate
ApsaraDB for RDS	Instance	ACS::RDS::DBInstance
ActionTrail	Trail	ACS::ActionTrail::Trail
Virtual Private Cloud	VPC-connected instance	ACS::VPC::VPC
	Route table	ACS::VPC::RouteTable
	VSwitch	ACS::VPC::VSwitch
VPN Gateway	VPN gateway	ACS::VPN::VpnGateway
	VPN connection	ACS::VPN::VpnConnection
	Customer gateway	ACS::VPN::CustomerGateway
Elastic IP Address	Elastic IP address	ACS::EIP::EipAddress
Resource Access Management	Role	ACS::RAM::Role
	Policy	ACS::RAM::Policy
	User	ACS::RAM::User
Server Load Balancer	Instance	ACS::SLB::LoadBalancer
	CA certificate	ACS::SLB::CACertificate

Service	Resource type	ARN
	Server certificate	ACS::SLB::ServerCertificate
	Access control list	ACS::SLB::AccessControlList
CDN	Domain name	ACS::CDN::Domain
Auto Scaling	Scaling group	ACS::ESS::ScalingGroup
	Scaling rule	ACS::ESS::ScalingRule
	Scaling configuration	ACS::ESS::ScalingConfiguration
Object Storage Service	Bucket	ACS::OSS::Bucket
ApsaraDB for Redis	Redis instance	ACS::Redis::DBInstance
Apsara PolarDB	PolarDB cluster	ACS::PolarDB::DBCluster
ApsaraDB for MongoDB	MongoDB instance	ACS::MongoDB::DBInstance
Shared Bandwidth	Shared bandwidth package	ACS::CBWP::CommonBandwidthPackage
Cloud Enterprise Network	Instance	ALIYUN::CEN::CenInstance
	Bandwidth plan	ALIYUN::CEN::CenBandwidthPackage
	Flow log	ACS::CEN::Flowlog
Web Application Firewall	Instance	ACS::ECS::Instance
	Domain name	ACS::CDN::Domain
Anti-DDoS Pro	Instance	ACS::DdosCoo::Instance
Apsara File Storage NAS	File system	ACS::NAS::FileSystem
ApsaraDB for Hbase	Cluster	ACS::HBase::Cluster
Alibaba Cloud Container Service for Kubernetes	Cluster	ACS::ACK::Cluster