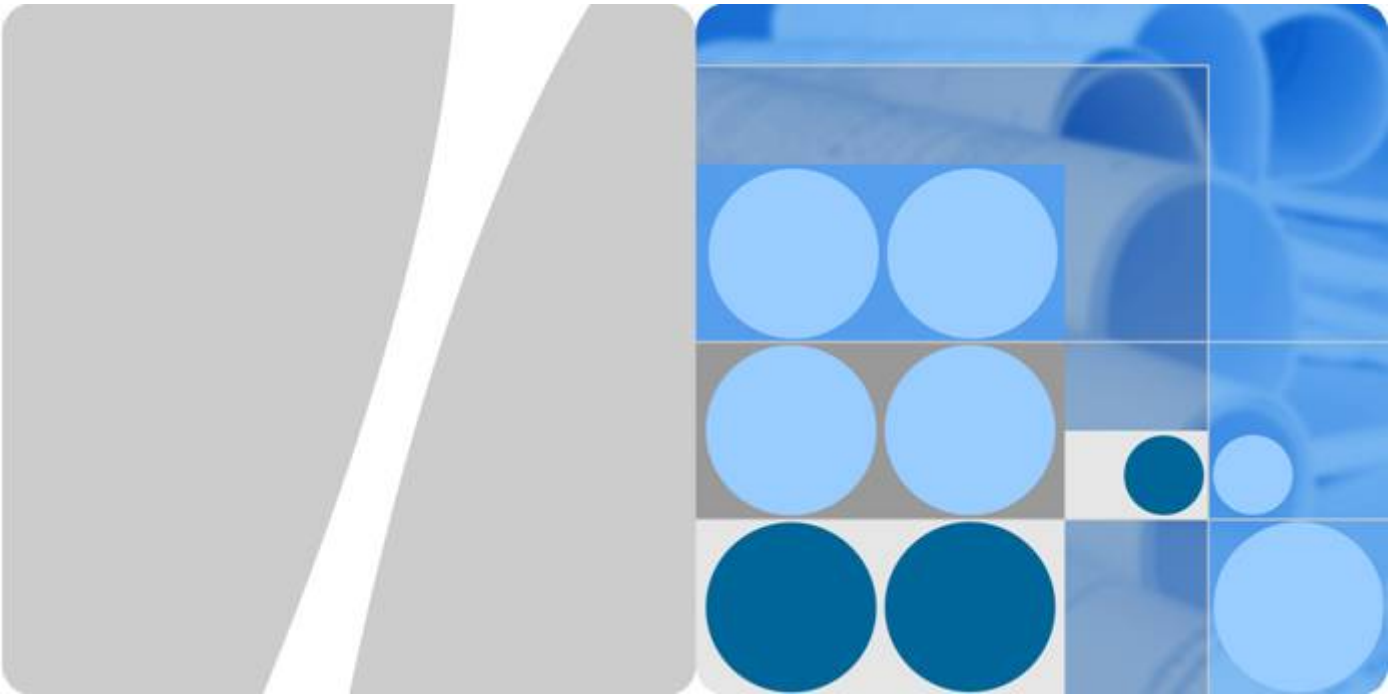


Identity and Access Management

Permissions Policies

Issue 01

Date 2019-10-26

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

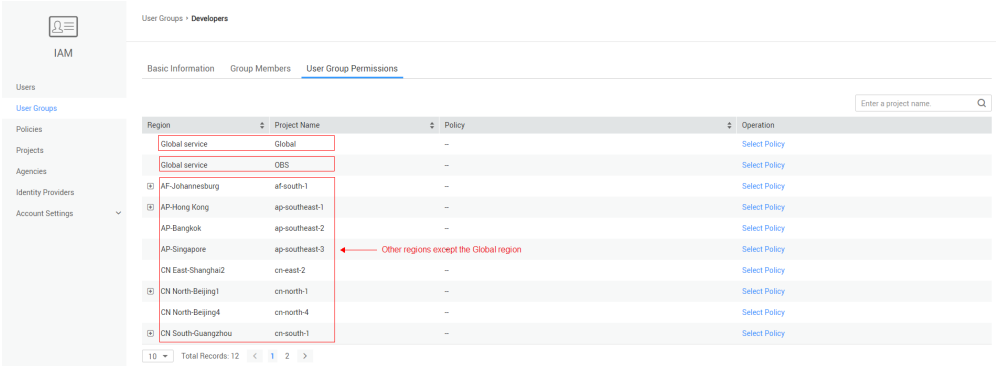
Contents

1 Permissions Policies

A policy is a set of permissions defined in JSON format. By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on cloud services based on the permissions. IAM provides system-defined policies that define the common permissions for different services, such as administrator and read-only permissions. You can directly use these system-defined policies to assign permissions.

Region: Regions where permissions take effect. Select regions where the cloud service to be accessed is deployed.

- Global region: Services in the global region are called global services, which are available to all users. Permissions for accessing these services need to be assigned in the Global region.
- Global region - OBS: Object Storage Service (OBS) is deployed independent from other services. Permissions for accessing OBS need to be assigned in the Global-OBS region.
- Specific regions: Services in specific regions are called project-level services. Permissions for accessing these services need to be assigned in specific regions and take effect only for these regions. To make the permissions take effect in all regions, assign the permissions in each of these regions.



Policy Type: There are fine-grained policies and role-based access control (RBAC) policies. Fine-grained policies are currently available for open beta testing. You can apply to use the **fine-grained access control function** free of charge.

- If the fine-grained access control function is not enabled, only RBAC policies can be used.
- For services (such as AOM) that only support fine-grained policies, if the fine-grained access control function is not enabled, permissions for accessing these services cannot be assigned to IAM users.
- **After the fine-gained access control function is enabled, preferably use fine-grained policies to assign permissions for accessing services that support both fine-grained and RBAC policies.**
- For services that support fine-grained access control, you can **create custom policies** as a supplement to system-defined policies to allow or deny access to specific types of resources. Click the **Fine-grained** link to view the supported policy actions.

System-Defined Policies

Service	Region	System-Defined Policies	Policy Type	Permissions
BASE	Global	Full Access	Fine-grained	Full permissions for all services
	All regions	Tenant Guest	RBAC	Read-only permissions for all services except IAM
	All regions	Tenant Administrator	RBAC	Full permissions for all services except IAM
	Global	Security Administrator	RBAC	Full permissions for IAM
	Global	Agent Operator	RBAC	Permissions for switching roles to access resources of delegating accounts
Object Storage Service (OBS)	Global - OBS	OBS Operator	**Fine-grained**	Basic object operation permissions, such as viewing buckets, uploading, obtaining, and deleting objects, and obtaining object ACLs
		OBS Viewer		Permissions for listing buckets, obtaining bucket metadata, listing objects in a bucket, and querying bucket locations

Service	Region	System-Defined Policies	Policy Type	Permissions
		OBS Buckets Viewer	RBAC	Permissions for listing buckets, obtaining bucket information, obtaining bucket metadata, and listing objects
Tag Management Service (TMS) (Global service)	Global	TMS Administrator	RBAC	Full permissions for TMS
Content Delivery Network (CDN) (Global service)	Global	CDN Domain Viewer	**Fine-grained**	Read-only permissions for CDN acceleration domain names
		CDN Statistics Viewer		Read-only permissions for CDN statistics
		CDN Logs Viewer		Read-only permissions for CDN logs
		CDN Domain Configuration Operator		Permissions for configuring CDN acceleration domain names
		CDN Refresh And Preheat Operator		Permissions for cache refreshing and preheating
		CDN Administrator	RBAC	Full permissions for CDN **This policy depends on the Tenant Guest policy in the same project.**

Service	Region	System-Defined Policies	Policy Type	Permissions
Enterprise Project Management Service (EPS) (Global service)	Global	EPS Admin	**Fine-grained**	● Administrator permissions for Enterprise Management, including enterprise project and personnel management. For example, creating organizations, migrating resources, adding/removing user groups, and attaching policies to user groups. These permissions can be assigned by the administrator in the Global region on the IAM console. ● Administrator permissions for a specific enterprise project, including modifying, enabling, disabling, and viewing the enterprise project. These permissions can be assigned by the administrator or an IAM user with EPS Admin permissions on the Enterprise Management console.

Service	Region	System-Defined Policies	Policy Type	Permissions
		EPS Viewer		Read-only permissions for a specific or all enterprise projects ● Read-only permissions for viewing all enterprise projects and user information. These permissions can be assigned by the administrator in the Global region on the IAM console. ● Read-only permission for viewing a specific enterprise project. These permissions can be assigned by the administrator or an IAM user with EPS Admin permissions on the Enterprise Management console.
Service Ticket (Global service)	Global	Ticket Administrator	RBAC	Full permissions for Service Ticket
Intelligent CAPTCHA Service (ICS) (Global service)	Global	ICS Administrator	RBAC	Full permissions for ICS
Business Support System (BSS) (Project-level service)	Specific regions	BSS Administrator	RBAC	Full permissions for Billing Center, Resource Center, and My Account

Service	Region	System-Defined Policies	Policy Type	Permissions
	NOTICE These are the regions where permissions of the policies supported by this service can be assigned.	BSS Operator		Query permissions for Billing Center and management permissions for Resource Center and My Account
		BSS Finance		● Topping up accounts, withdrawing money, and setting balance alerts ● Viewing, paying, and exporting orders, and renewing resources ● Viewing and exporting the expenditure summary, expenditure details, and income and expense details, and analyzing bills ● Viewing and activating coupons, issuing invoices, applying for online contracts, and viewing commercial discounts
		EnterpriseProject_ BSS_Administrator	Fine-grained	Permissions for accounting management of enterprise projects

Service	Region	System-Defined Policies	Policy Type	Permissions
Elastic Cloud Server (ECS) Elastic Volume Service (EVS) Virtual Private Cloud (VPC) Image Management Service (IMS) (Project-level service)	Specific regions	Server Administrator	RBAC	● Full permissions for ECS. **This policy depends on the Tenant Guest policy in the same project.** If a user needs to create, delete, or change resources of other services, the user must be granted **administrator permissions** in the same project. For example, if a user needs to create a new VPC when creating an ECS, the user must be granted **VPC Administrator** permissions. ● Full permissions for EVS. ● Permissions for performing operations on EIPs, security groups, and ports. **This policy depends on the Tenant Guest policy in the same project.** ● Permissions for creating, deleting, querying, modifying, and uploading images. **This policy depends on the IMS Administrator policy in the same project.**

Service	Region	System-Defined Policies	Policy Type	Permissions
Elastic Cloud Server (ECS) (Project-level service)	Specific regions	ECS Admin	Fine-grained	Full permissions for ECS
		ECS Viewer		Read-only permissions for ECS
		ECS User		Permissions for starting, stopping, restarting, and querying ECSs
Bare Metal Server (BMS) (Project-level service)	Specific regions	BMS Admin	Fine-grained	Full permissions for BMS
		BMS Viewer		Read-only permissions for BMS
		BMS User		Permissions for starting, stopping, restarting, and querying BMSs
Auto Scaling (AS) (Project-level service)	Specific regions	AutoScaling Admin	Fine-grained	Full permissions for all AS resources
		AutoScaling Viewer		Read-only permissions for all AS resources
		AutoScaling Administrator	RBAC	Full permissions for all AS resources **This policy depends on the ELB Administrator and CES Administrator policies in the same project.**
Image Management Service (IMS) (Project-level service)	Specific regions	IMS Admin	Fine-grained	Full permissions for IMS
		IMS Viewer		Read-only permissions for IMS
		IMS Administrator	RBAC	Full permissions for IMS **This policy depends on the Tenant Administrator policy in the OBS project.**

Service	Region	System-Defined Policies	Policy Type	Permissions
Elastic Volume Service (EVS) (Project-level service)	Specific regions	EVS Admin	Fine-grained	Full permissions for EVS
		EVS Viewer		Read-only permissions for EVS
Storage Disaster Recovery Service (SDRS) (Project-level service)	Specific regions	SDRS Administrator	RBAC	Full permissions for SDRS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Cloud Server Backup Service (CSBS) (Project-level service)	Specific regions	CSBS Administrator	RBAC	Full permissions for CSBS **This policy depends on the Server Administrator policy in the same project.**
Volume Backup Service (VBS) (Project-level service)	Specific regions	VBS Administrator	RBAC	Full permissions for VBS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Dedicated Distributed Storage Service (DSS) (Project-level service)	Specific regions	DSS Admin	RBAC	Full permissions for DSS
		DSS Viewer		Read-only permissions for DSS
Virtual Private Cloud (VPC) (Project-level service)	Specific regions	VPC Admin	Fine-grained	Full permissions for VPC
		VPC Viewer		Read-only permissions for VPC

Service	Region	System-Defined Policies	Policy Type	Permissions
		VPC Administrator	RBAC	Full permissions for VPC **This policy depends on the Tenant Guest policy in the same project.**
Cloud Container Engine (CCE) (Project-level service)	Specific regions	CCE Admin	**Fine-grained**	Full permissions for CCE
		CCE Viewer		Read-only permissions for CCE and all operations on Kubernetes resources
		CCE Administrator	RBAC	Full permissions for CCE **This policy depends on the Tenant Guest, Server Administrator, SFS Administrator, SWR Admin, and APM Admin policies in the same project and the OBS Operator policy in the OBS project.**
Cloud Container Instance (CCI) (Project-level service)	Specific regions	CCI Administrator	RBAC	Full permissions for CCI
		CCI Admin	**Fine-grained**	Full permissions for CCI
		CCI Viewer		Read-only permissions for CCI
Data Ingestion Service (DIS) (Project-level service)	Specific regions	DIS Administrator	RBAC	Full permissions for DIS
		DIS Operator		Permissions for managing streams, such as creating and deleting streams, but not for uploading and downloading data

Service	Region	System-Defined Policies	Policy Type	Permissions
		DIS User		Permissions for uploading and downloading data, but not for managing streams
Data Warehouse Service (DWS) (Project-level service)	Specific regions	DWS Admin	Fine-grained	Full permissions for DWS
		DWS Viewer		Read-only permissions for DWS
		DWS Administrator	RBAC	Full permissions for DWS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
		DWS Database Access		Permissions for accessing DWS. Users granted these permissions can generate temporary tokens for connecting to DWS cluster databases.
CloudTable Service (CloudTable) (Project-level service)	Specific regions	CloudTable Administrator	RBAC	Full permissions for CloudTable **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Data Lake Factory (DLF) (Project-level service)	Specific regions	DLF Administrator	RBAC	Full permissions for DLF **This policy depends on the Tenant Administrator policy in the same project.**
		DLF Admin	Fine-grained	Full permissions for DLF

Service	Region	System-Defined Policies	Policy Type	Permissions
		DLF Developer		Developer permissions for DLF. Users granted these permissions can use DLF to develop scripts and orchestrate jobs, but cannot create, delete, or modify workspaces.
		DLF Operator		O&M permissions for DLF. Users granted these permissions can maintain scripts, jobs, and other resources, but cannot create, delete, or modify any resources.
		DLF Viewer		Read-only permissions for DLF. Users granted these permissions can only view DLF resources.
Data Lake Insight (DLI) (Project-level service)	Specific regions	DLI Service Admin	RBAC	Full permissions for DLI
		DLI Service User		Permissions for using DLI, but not for creating resources
Graph Engine Service (GES) (Project-level service)	Specific regions	GES Administrator	RBAC	Full permissions for GES **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**

Service	Region	System-Defined Policies	Policy Type	Permissions
		GES Operator		Permissions for viewing and accessing graphs **This policy depends on the Tenant Guest policy in the same project.**
	Specific regions	GES Admin	**Fine-grained**	Administrator permissions for performing all operations (including creation, deletion, access, and upgrade operations) on GES
		GES User		Operator permissions for all operations except creating and deleting graphs
		GES Viewer		Read-only permissions for viewing resources, such as graphs, metadata, and backup data
Cloud Data Migration (CDM) (Project-level service)	Specific regions	CDM Administrator	RBAC	Full permissions for CDM **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
		CDM Admin	**Fine-grained**	Administrator permissions for performing all operations on CDM.
		CDM Operator		Permissions for performing all operations except binding and unbinding EIPs on CDM

Service	Region	System-Defined Policies	Policy Type	Permissions
		CDM User		Permissions for performing operations on CDM jobs and links
		CDM Viewer		Read-only permissions for CDM. Users granted these permissions can only view CDM clusters, links, and jobs.
Cloud Search Service (CSS) (Project-level service)	Specific regions	Elasticsearch Administrator	RBAC	Full permissions for CSS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Log Tank Service (LTS) (Project-level service)	Specific regions	LTS Admin	Fine-grained	Full permissions for LTS
		LTS Viewer		Read-only permissions for LTS
		LTS Administrator	RBAC	Full permissions for LTS **This policy depends on the Tenant Guest policy in the same project and the Tenant Administrator policy in the OBS project.**
Domain Name Service (DNS) (Project-level service)	Specific regions	DNS Administrator	RBAC	Full permissions for DNS

Service	Region	System-Defined Policies	Policy Type	Permissions
Cloud Trace Service (CTS) (Project-level service)	Specific regions	CTS Administrator	RBAC	Full permissions for CTS **This policy depends on the Tenant Guest policy in the same project and the Tenant Administrator policy in the OBS project.**
Simple Message Notification (SMN) (Project-level service)	Specific regions	SMN Administrator	RBAC	Full permissions for SMN
Cloud Phone (CPH) (Project-level service)	Specific regions	CPH Administrator	RBAC	Full permissions for CPH
		CPH User		Read-only permissions for CPH
Resource Template Service (RTS) (Project-level service)	Specific regions	RTS Administrator	RBAC	Full permissions for RTS **This policy depends on the Server Administrator, ELB Administrator, and CES Administrator policies in the same project.**
Relational Database Service (RDS) (Project-level service)	Specific regions	RDS Admin	**Fine-grained**	Full permissions for RDS
		RDS Viewer		Read-only permissions for RDS
		RDS DBA		DBA permissions for all operations except deleting RDS resources

Service	Region	System-Defined Policies	Policy Type	Permissions
		RDS Administrator	RBAC	Full permissions for RDS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Distributed Message Service (DMS) (Project-level service)	Specific regions	DMS Administrator	RBAC	Full permissions for DMS
Document Database Service (DDS) (Project-level service)	Specific regions	DDS Admin	**Fine-grained**	Full permissions for DDS
		DDS Viewer		Read-only permissions for DDS
		DDS DBA		DBA permissions for all operations except deleting DDS resources
		DDS Administrator	RBAC	Full permissions for DDS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.** **If a DDS enterprise project is configured, you need to select the DAS Admin policy in the same project so that you can log in to DAS from the DDS console.**

Service	Region	System-Defined Policies	Policy Type	Permissions
Data Replication Service (DRS) (Project-level service)	Specific regions	DRS Administrator	RBAC	Full permissions for DRS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
Data Admin Service (DAS) (Project-level service)	Specific regions	DAS Administrator	RBAC	Full permissions for DAS **This policy depends on the Tenant Guest policy in the same project.**
Distributed Database Middleware (DDM) (Project-level service)	Specific regions	DDM Admin	**Fine-grained**	Full permissions for DDM
		DDM User		Common permissions for DDM Users with common permissions cannot perform the following operations: ● Buying DDM instances ● Deleting DDM instances ● Scaling up instances ● Rolling back instances or clearing data when scale-up fails
		DDM Viewer		Read-only permissions for DDM
Application Operations Management (AOM)	Specific regions	AOM Admin	**Fine-grained**	Full permissions for AOM

Service	Region	System-Defined Policies	Policy Type	Permissions
(Project-level service)		AOM Viewer		Read-only permissions for AOM
Application Performance Management (APM) (Project-level service)	Specific regions	APM Admin	Fine-grained	Full permissions for APM
		APM Viewer		Read-only permissions for APM
API Gateway (Project-level service)	Specific regions	APIG Administrator	RBAC	Full permissions for API Gateway
Software Repository for Container (SWR) (Project-level service)	Specific regions	SWR Admin	RBAC	Full permissions for SWR
Cloud Eye (Project-level service)	Specific regions	CES Administrator	RBAC	Full permissions for Cloud Eye **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
	Specific regions	CES Admin	Fine-grained	Administrator permissions for performing all operations on Cloud Eye The monitoring function of Cloud Eye involves the query of cloud resources, which requires the relevant cloud services to support fine-grained authorization. For details, see **Supported Cloud Services**.

Service	Region	System-Defined Policies	Policy Type	Permissions
	Specific regions	CES Viewer		Read-only permissions for viewing data on Cloud Eye The monitoring function of Cloud Eye involves the query of cloud resources, which requires the relevant cloud services to support fine-grained authorization. For details, see **Supported Cloud Services**.
Web Application Firewall (WAF) (Project-level service)	Specific regions	WAF Administrator	RBAC	Full permissions for WAF
Host Security Service (HSS) (Project-level service)	Specific regions	HSS Administrator	RBAC	Full permissions for HSS
Vulnerability Scan Service (VSS) (Project-level service)	Specific regions	VSS Administrator	RBAC	Full permissions for VSS
Container Guard Service (CGS) (Project-level service)	Specific regions	CGS Administrator	RBAC	Full permissions for CGS
Security Expert Service (SES) (Project-level service)	Specific regions	SES Administrator	RBAC	Full permissions for SES

Service	Region	System-Defined Policies	Policy Type	Permissions
Database Security Service (DBSS) (Project-level service)	Specific regions	DBSS System Administrator	RBAC	Full permissions for DBSS
		DBSS Audit Administrator		Security auditing permissions for DBSS
		DBSS Security Administrator		Security protection permissions for DBSS
Data Encryption Workshop (DEW) (Project-level service)	Specific regions	KMS Administrator	RBAC	Full permissions for DEW
Anti-DDoS (Project-level service)	Specific regions	Anti-DDoS Administrator	RBAC	Full permissions for Anti-DDoS **This policy depends on the Tenant Guest policy in the same project.**
Advanced Anti-DDoS (AAD) (Project-level service)	Specific regions	CAD Administrator	RBAC	Full permissions for AAD
Video on Demand (VOD) (Project-level service)	Specific regions	VOD Administrator	RBAC	Full permissions for VOD. The operation object is all video content.
		VOD Group Administrator		Permissions for VOD operations except global configuration. The operation object is the video content created by users in the current group.

Service	Region	System-Defined Policies	Policy Type	Permissions
		VOD Group Operator		Permissions for VOD operations except content release, cancellation of content release, content deletion, and global configuration. The operation object is the video content created by users in the current group.
		VOD Group Guest		Permissions only for querying video content. The operation object is the video content created by users in the current group.
Media Processing Center (MPC) (Project-level service)	Specific regions	MPC Administrator	RBAC	Full permissions for MPC
Scalable File Service (SFS) (Project-level service)	Specific regions	SFS Admin	**Fine-grained**	Full permissions for SFS
		SFS Viewer		Read-only permissions for SFS
		SFS Administrator	RBAC	Full permissions for SFS **This policy depends on the Tenant Guest policy in the same project.**
Cloud Stream Service (CS) (Project-level service)	Specific regions	CS Admin	**Fine-grained**	Full permissions for CS
		CS User		Common user permissions for CS. Users granted these permissions can create, delete, and modify jobs and templates.

Service	Region	System-Defined Policies	Policy Type	Permissions
		CS Viewer		Read-only permissions for CS. Users granted these permissions can only view CS jobs, templates, and exclusive clusters.
		CS Tenant User	RBAC	Common user permissions for CS. Users granted these permissions can create, delete, and modify jobs and templates.
		CS Tenant Admin		Administrator permissions for all operations on CS, including: ● Creating, deleting, and modifying CS jobs, templates, and exclusive clusters ● Allocating available clusters and quotas to users with permissions of the **CS User** policy ● Viewing all user jobs in exclusive clusters
Distributed Cache Service (DCS) (Project-level service)	Specific regions	DCS Admin	**Fine-grained**	Full permissions for DCS
		DCS User		Common user permissions for DCS operations except creating, modifying, deleting, and scaling instances
		DCS Viewer		Read-only permissions for DCS

Service	Region	System-Defined Policies	Policy Type	Permissions
		DCS Administrator	RBAC	Full permissions for DCS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
MapReduce Service (MRS) (Project-level service)	Specific regions	MRS Admin	**Fine-grained**	Full permissions for MRS
		MRS User		Common user permissions for MRS operations except creating and deleting resources
		MRS Viewer		Read-only permissions for MRS
		MRS Administrator	RBAC	Full permissions for MRS **This policy depends on the Tenant Guest and Server Administrator policies in the same project.**
FunctionGraph (Project-level service)	Specific regions	FunctionGraph Administrator	RBAC	Permissions for managing FunctionGraph functions, workflows, and triggers **This policy depends on the Tenant Guest policy in the same project.**
		FunctionGraph Invoker		Permissions for querying FunctionGraph functions, workflows, and triggers

Service	Region	System-Defined Policies	Policy Type	Permissions
ServiceStage Cloud Performance Test Service (CPTS) (Project-level service)	Specific regions	SvcStg Admin	RBAC	● Full permissions for ServiceStage, including service, application, node, stack, and pipeline management. ● Permissions for performing operations on test resources of all users in CPTS, such as adding, deleting, modifying, and querying test resources
		SvcStg Developer		● Common user permissions for ServiceStage except node management ● Permissions for performing operations only on a user's own test resources, such as adding, deleting, modifying, and querying test resources
		SvcStg Operator		● Read-only permissions for ServiceStage ● Read-only permissions only for a user's own test resources

Service	Region	System-Defined Policies	Policy Type	Permissions
Workspace (Project-level service)	Specific regions	Workspace Administrator	RBAC	Full permissions for Workspace **This policy depends on the Tenant Guest, Server Administrator, and VPC Administrator policies in the same project.**
Voice Call Message & SMS Private Number (Project-level service)	Specific regions	RTC Administrator	RBAC	Full permissions for Voice Call, Message & SMS, and Private Number
Elastic Load Balance (ELB) (Project-level service)	Specific regions	ELB Admin	**Fine-grained**	Full permissions for ELB
		ELB Viewer		Read-only permissions for ELB
		ELB Service Administrator	RBAC	Full permissions for ELB **This policy depends on the Tenant Guest policy in the same project.**
NAT Gateway (Project-level service)	Specific regions	NAT Admin	Fine-grained	Full permissions for NAT Gateway
		NAT Viewer		Read-only permission for NAT Gateway
		NAT Gateway Administrator	RBAC	Full permissions for NAT Gateway **This policy depends on the Tenant Guest policy in the same project.**
Recommender System (RES) (Project-level service)	Specific regions	RES Admin	**Fine-grained**	Full permissions for RES

Service	Region	System-Defined Policies	Policy Type	Permissions
		RES Viewer		Read-only permissions for RES
Direct Connect (Project-level service)	Specific regions	Direct Connect Administrator	RBAC	Full permissions for Direct Connect **This policy depends on the Tenant Guest policy in the same project.**
VPC Endpoint (VPCEP) (Project-level service)	Specific regions	VPCEndpoint Administrator	RBAC	Full permissions for VPCEP **This policy depends on the Server Administrator, VPC Administrator, and DNS Administrator policies in the same project.**
Cloud Backup and Recovery (CBR) (Project-level service)	Specific regions	CBR Admin	Fine-grained	Administrator permissions for using all vaults and policies on CBR
		CBR User	Fine-grained	Common user permissions for creating, viewing, and deleting vaults on CBR
		CBR Viewer	Fine-grained	Read-only permissions for viewing data on CBR
DAYU (Project-level service)	Specific regions	DAYU Administrator	RBAC	Full permissions for DAYU
		DAYU User		Read-only permissions for DAYU
ModelArts (Project-level service)	Specific regions	ModelArts Admin	Fine-grained	Administrator permissions for performing all operations on ModelArts

Service	Region	System-Defined Policies	Policy Type	Permissions
		ModelArts User		Permissions for performing all operations except managing dedicated resource pools on ModelArts

