Permissions Policies

Issue	01
Date	2022-09-21

HUAWEI TECHNOLOGIES CO., LTD.

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 System Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Scope: The projects for which permissions granted to a user group will take effect.

- Global service project: Services deployed without specifying physical regions, such as Object Storage Service (OBS) and Content Delivery Network (CDN), are called global services. Permissions for these services must be assigned in the global service project.
- Region-specific projects: Services deployed in specific regions, such as Elastic Cloud Server (ECS) and Bare Metal Server (BMS), are called project-level services. Permissions for these services need to be assigned in region-specific projects and take effect only for the corresponding regions.
  - All projects: Permissions take effect for both the global service project and region-specific projects, including projects created later.
  - Region-specific projects: Permissions take effect for the region-specific projects you select.

Type: You can grant users permissions by using roles and policies. Policies are a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. For details, see **Permission**.

- **For services that provide both policies and roles, preferentially use policies to assign permissions.**
- For services that support policy-based access control, you can **create custom policies** to supplement system-defined policies to allow or deny access to specific types of resources under certain conditions.

System-Defined Policies

Service	Scope	Role/Policy Name	Type	Description
BASE	Global service project	FullAccess	Policy	Full permissions for cloud services supporting policy-based authorization.
	All projects	Tenant Administrator	Role	Full permissions for all services except IAM. **NOTE** • If the permissions are granted for the global service project, they take effect for the global service project. • If the permissions are granted for all projects, they take effect for both the global service project and all region-specific projects, including projects created later. • If the permissions are granted for certain region-specific projects, they take effect only for these projects.
	All projects	Tenant Guest		Read-only permissions for all services except IAM. **NOTE** • If the permissions are granted for the global service project, they take effect for the global service project. • If the permissions are granted for all projects, they take effect for both the global service project and all region-specific projects, including projects created later. • If the permissions are granted for certain region-specific projects, they take effect only for these projects.
	Global service project	Agent Operator		Permissions for switching roles to access resources of delegating accounts.

Service	Scope	Role/Policy Name	Type	Description
Elastic Cloud Server (ECS) (Project-level service)	Region-specific projects	ECS FullAccess	Policy	Full permissions for ECS.
		ECS ReadOnlyAccess		Read-only permissions for ECS.
		ECS PartnerOperations		Partner permissions for ECS.
		ECS CommonOperations	Role	Permissions for starting, stopping, restarting, and querying ECSs.
Cloud Container Engine (CCE) (Project-level service)	Region-specific projects	CCE FullAccess	Policy	Common operation permissions for CCE cluster resources, including the permissions for creating, deleting, and updating clusters. This policy does not include namespace-level permissions for clusters that have Kubernetes RBAC enabled or administrator permissions for agency configuration and cluster certificate generation. **NOTE** You can grant IAM users namespace-level permissions for clusters that have Kubernetes RBAC enabled and administrator permissions for agency configuration and cluster certificate generation on the CCE console. For details, see **Permissions Overview**.
		CCE ReadOnlyAccess		Permissions to view CCE cluster resources, excluding namespace-level permissions for clusters that have Kubernetes RBAC enabled.

Service	Scope	Role/Policy Name	Type	Description
		CCE Administrator	Role	Read and write permissions for CCE clusters and all resources (including workloads, nodes, jobs, and Services) in the clusters. **This role depends on the following permissions:** **Global service project: OBS Buckets Viewer** **Region-specific projects (same projects): Tenant Guest, Server Administrator, ELB Administrator, SFS Administrator, SWR Admin, and APM FullAccess** **NOTE** Users also granted permissions with the **NAT Gateway Administrator** role can use NAT Gateway functions for clusters.
Object Storage Service (OBS)	Global service project	OBS OperateAccess	Policy	Users with this permission can perform all operations specified by **OBS ReadOnlyAccess** and perform basic object operations, such as uploading objects, downloading objects, deleting objects, and obtaining object ACLs.
		OBS ReadOnlyAccess		Users with this permission can list buckets, obtain basic bucket information, obtain bucket metadata, and list objects.
		OBS Buckets Viewer	Role	Users with this permission can list buckets, obtain basic bucket information, and obtain bucket metadata.

Service	Scope	Role/Policy Name	Type	Description
Content Delivery Network (CDN) (Global service)	Global service project	CDN DomainReadOnlyAccess	Policy	Read-only permissions for CDN acceleration domain names.
		CDN StatisticsReadOnlyAccess		Read-only permissions for CDN statistics.
		CDN LogsReadOnlyAccess		Read-only permissions for CDN logs.
		CDN Domain Configuration Operator		Permissions for configuring CDN acceleration domain names.
		CDN RefreshAndPreheatAccess		Permissions for cache refreshing and preheating.
		CDN Administrator	Role	Full permissions for CDN. **This role must be used together with the Tenant Guest role in the same project.**
Storage Disaster Recovery Service (SDRS) (Project-level service)	Region-specific projects	SDRS Administrator	Role	Full permissions for SDRS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
SSL Certificate Manager (SCM) (Global service) (SCM has been integrated into CCM.)	Global service project	SCM Administrator	Role	Full permissions for SCM. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
		SCM FullAccess	Policy	Full permissions for SCM.

Service	Scope	Role/Policy Name	Type	Description
		SCM ReadOnlyAccess		Read-only permissions for SCM. Users with these permissions can only query certificates but cannot add, delete, or modify certificates.
Situation Awareness (SA) (Global service)	Global service project	SA FullAccess	Policy	Full permissions for SA.
		SA ReadOnlyAccess		Read-only permissions for SA. Users with the read-only permission can only query SA information but cannot perform configuration in SA.
Cloud Bastion Host (CBH) (Project-level service)	Region-specific projects	CBH FullAccess	Policy	Full permissions for CBH instances.
		CBH ReadOnlyAccess		Read-only permissions for CBH instances. Users who have read-only permissions granted can only view CBH instances but cannot configure or perform operations on services.
Business Support System (BSS) (Project-level service) **NOTICE** These are the projects where permissions for this service can be assigned.	Region-specific projects	BSS Administrator	Role	Full permissions for Billing Center, Resource Center, and My Account.
		BSS Operator		Query permissions for Billing Center and management permissions for Resource Center and My Account.
		BSS Finance		Permissions for financial operations, including payment, consumption, and invoicing. This role does not have permissions for modifying cloud services.
		Enterprise Project BSS FullAccess	Policy	Permissions for accounting management of enterprise projects.

Service	Scope	Role/Policy Name	Type	Description
Elastic Cloud Server (ECS) Elastic Volume Service (EVS) Virtual Private Cloud (VPC) Image Management Service (IMS) (Project-level service)	Region-specific projects	Server Administrator	Role	• Full permissions for ECS. **This role must be used together with the Tenant Guest role in the same project.** If a user needs to create, delete, or change resources of other services, the user must also be granted **administrator permissions** of the corresponding services in the same project. For example, if a user needs to create a new VPC when creating an ECS, the user must also be granted permissions with the **VPC Administrator** role. • Full permissions for EVS. • Permissions for performing operations on EIPs, security groups, and ports. **This role must be used together with the Tenant Guest role in the same project.** • Permissions for creating, deleting, querying, modifying, and uploading images. **This role must be used together with the IMS Administrator role in the same project.**
Cloud Container Instance (CCI) (Project-level service)	Region-specific projects	CCI FullAccess	Policy	Full permissions for CCI. Users granted these permissions can create, delete, query, and update all CCI resources.

Service	Scope	Role/Policy Name	Type	Description
		CCI ReadOnlyAccess		Read-only permissions for CCI. Users granted these permissions can only view CCI resources.
		CCI CommonOperations		Common user permissions for CCI. Users granted these permissions can perform all operations except creating, deleting, and modifying role-based access control (RBAC) policies, networks, and namespaced resources.
		CCI Administrator	Role	Administrator permissions for CCI. Users granted these permissions can create, delete, query, and update all CCI resources.
Auto Scaling (AS) (Project-level service)	Region-specific projects	AutoScaling FullAccess	Policy	Full permissions for all AS resources.
		AutoScaling ReadOnlyAccess		Read-only permissions for all AS resources.
		AutoScaling Administrator	Role	Full permissions for all AS resources. **This role must be used together with the ELB Administrator, CES Administrator, Server Administrator, and Tenant Administrator roles in the same project.**
Image Management Service (IMS) (Project-level service)	Region-specific projects	IMS FullAccess	Policy	Full permissions for IMS.
		IMS ReadOnlyAccess		Read-only permissions for IMS.

Service	Scope	Role/Policy Name	Type	Description
		IMS Administrator	Role	Full permissions for IMS. **This role must be used together with the Tenant Administrator role in the global service project.**
Elastic Volume Service (EVS) (Project-level service)	Region-specific projects	EVS FullAccess	Policy	Full permissions for EVS. Users granted these permissions can create, mount, uninstall, query, and delete EVS resources, and expand capacity of EVS disks.
		EVS ReadOnlyAccess		Read-only permissions for EVS. Users granted these permissions can view EVS resource data only.
Cloud Server Backup Service (CSBS) (Project-level service)	Region-specific projects	CSBS Administrator	Role	Full permissions for CSBS. **This role must be used together with the Server Administrator role in the same project.**
Volume Backup Service (VBS) (Project-level service)	Region-specific projects	VBS Administrator	Role	Full permissions for VBS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
Dedicated Distributed Storage Service (DSS) (Project-level service)	Region-specific projects	DSS FullAccess	Policy	Full permissions for DSS.
		DSS ReadOnlyAccess		Read-only permissions for DSS.
Virtual Private Cloud (VPC)	Region-specific projects	VPC FullAccess	Policy	Full permissions for VPC.

Service	Scope	Role/Policy Name	Type	Description
(Project-level service)		VPC ReadOnlyAccess		Read-only permissions for VPC.
		VPC Administrator	Role	Permissions for VPC, excluding permissions for creating, modifying, deleting, and viewing security groups and security group rules. **This role must be used together with the Tenant Guest role in the same project.**
Cloud Container Engine (CCE) (Project-level service)	Region-specific projects	CCE FullAccess	Policy	Full permissions for CCE.
		CCE ReadOnlyAccess		Read-only permissions for CCE and all operations on Kubernetes resources.
		CCE Administrator	Role	Read and write permissions for CCE clusters and all resources (including workloads, nodes, jobs, and Services) in the clusters. **This role depends on the following permissions:** **Global service project: OBS Buckets Viewer** **Region-specific projects (same projects): Tenant Guest, Server Administrator, ELB Administrator, SFS Administrator, SWR Admin, and APM FullAccess** **NOTE** Users also granted permissions with the **NAT Gateway Administrator** role can use NAT Gateway functions for clusters.
Application Orchestrati	Region-specific projects	CDE Admin	Role	AOS administrator with full permissions.

Service	Scope	Role/Policy Name	Type	Description
on Service (AOS) (Project-level service)		CDE Developer		AOS developer.
Resource Formation (RF) (Project-level service)	Region-specific projects	RF FullAccess	Policy	Full permissions for RF.
		RF ReadOnlyAccess		Read-only permissions for RF.
		RF DeployByExecutionPlanOperations		Create, execute, and read permissions for execution plans and read permissions for stacks.
CloudTable Service (CloudTable) (Project-level service)	Region-specific projects	CloudTable Administrator	Role	Full permissions for CloudTable. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
Domain Name Service (DNS) (Project-level service)	Region-specific projects	DNS Administrator	Role	Full permissions for DNS. **This role must be used together with the Tenant Guest and VPC Administrator roles in the same project.**
		DNS FullAccess	Policy	Full permissions for DNS.
		DNS ReadOnlyAccess		Read-only permissions for DNS. Users granted these permissions can only view DNS resources.
VPC Endpoint (VPCEP) (Project-level service)	Region-specific projects	VPCEndpoint Administrator	Role	Full permissions for VPCEP. **This role must be used together with the Server Administrator, VPC Administrator, and DNS Administrator roles in the same project.**

Service	Scope	Role/Policy Name	Type	Description
Identity and Access Management (IAM) (Global service)	Global service project	Security Administrator	Role	Full permissions for IAM.
	Global service project	IAM ReadOnlyAccess	Policy	Read-only permissions for IAM.
Cloud Trace Service (CTS) (Project-level service)	Region-specific projects	CTS FullAccess	Policy	Full permissions for CTS. **NOTE** To enable CTS, a user must be granted permissions using the **CTS FullAccess** policy and the **Security Administrator** role.
		CTS ReadOnlyAccess		Read-only permissions for CTS.
		CTS Administrator	Role	Full permissions for CTS. **This role must be used together with the Tenant Guest and Tenant Administrator roles in the same project.**
Simple Message Notification (SMN) (Project-level service)	Region-specific projects	SMN Administrator	Role	Full permissions for SMN. **This role must be used together with the Tenant Guest role in the same project.**
		SMN FullAccess	Policy	Full permissions for SMN.
		SMN ReadOnlyAccess		Read-only permissions for SMN.
Relational Database Service (RDS) (Project-level service)	Region-specific projects	RDS FullAccess	Policy	Full permissions for RDS.
		RDS ReadOnlyAccess		Read-only permissions for RDS.
		RDS UserAccess		Database administrator permissions for all operations except deleting RDS resources.

Service	Scope	Role/Policy Name	Type	Description
		RDS Administrator	Role	Full permissions for RDS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
Distributed Message Service (DMS) (Project-level service)	Region-specific projects	DMS Administrator	Role	Full permissions for DMS.
DMS (DMS Kafka and DMS RabbitMQ) (Project-level service)	Region-specific projects	DMS UserAccess	Policy	Common user permissions for DMS (DMS for Kafka and DMS for RabbitMQ), excluding permissions for creating, modifying, deleting, scaling up instances and dumping.
		DMS ReadOnlyAccess		Read-only permissions for DMS (DMS for Kafka and DMS for RabbitMQ). Users granted these permissions can only view DMS data.
		DMS FullAccess		Administrator permissions for DMS (DMS for Kafka and DMS for RabbitMQ). Users granted these permissions can perform all operations on DMS.
Document Database Service (DDS) (Project-level service)	Region-specific projects	DDS FullAccess	Policy	Full permissions for DDS.
		DDS ReadOnlyAccess		Read-only permissions for DDS.
		DDS ManageAccess		Database administrator permissions for all operations except deleting DDS resources.

Service	Scope	Role/Policy Name	Type	Description
		DDS Administrator	Role	Full permissions for DDS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.** **If a DDS enterprise project is configured, you need to assign the DAS Admin role to users in the same project so that the users can log in to DAS from the DDS console.**
Data Replication Service (DRS) (Project-level service)	Region-specific projects	DRS Administrator	Role	Full permissions for DRS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
		DRS FullAccess	Policy	Full permissions for DRS.
		DRS ReadOnlyAccess		Read-only permissions for DRS.
Data Admin Service (DAS) (Project-level service)	Region-specific projects	DAS Administrator	Role	DAS administrator with full permissions. **This role must be used together with the Tenant Guest role in the same project.**
		DAS FullAccess	Policy	Full permissions for DAS.
GaussDB NoSQL (Project-level service)	Region-specific projects	GaussDB NoSQL FullAccess	Policy	Full permissions for GaussDB NoSQL.
		GaussDB NoSQL ReadOnlyAccess		Read-only permissions for GaussDB NoSQL.
GaussDB(for	Region-specific projects	GaussDB FullAccess	Policy	Full permissions for GaussDB.

Service	Scope	Role/Policy Name	Type	Description
openGauss) (Project-level service)		GaussDB ReadOnlyAccess		Read-only permissions for GaussDB.
GaussDB(for MySQL) (Project-level service)	Region-specific projects	GaussDB FullAccess	Policy	Full permissions for GaussDB.
		GaussDB ReadOnlyAccess		Read-only permissions for GaussDB.
Application Operations Management (AOM) (Project-level service)	Region-specific projects	AOM FullAccess	Policy	Full permissions for AOM.
		AOM ReadOnlyAccess		Read-only permissions for AOM.
Application Performance Management (APM) (Project-level service)	Region-specific projects	APM FullAccess	Policy	Full permissions for APM.
		APM ReadOnlyAccess		Read-only permissions for APM.
		APM Administrator	Role	Full permissions for APM.
Software Repository for Container (SWR) (Project-level service)	Region-specific projects	SWR Admin	Role	Full permissions for SWR.
		SWR FullAccess	Policy	Full permissions for SWR enterprise edition.
		SWR ReadOnlyAccess		Read-only permissions for SWR enterprise edition. Users with these permissions can query artifact repositories and charts, create temporary credentials, and download artifacts.

Service	Scope	Role/Policy Name	Type	Description
		SWR OperateAccess		Operation permissions for SWR enterprise edition. Users with these permissions can query enterprise edition instances, perform operations on artifact repositories and organizations, create temporary credentials, and upload and download artifacts.
Blockchain Service (BCS) (Project-level service)	Region-specific projects	BCS Administrator	Role	Administrator permissions for BCS.
		BCS FullAccess	Policy	Full permissions for BCS.
		BCS ReadOnlyAccess		Read-only permissions for BCS.
Gene Container Service (GCS) (Project-level service)	Region-specific projects	GCS Administrator	Role	GCS administrator.
		GCS FullAccess	Policy	Full permissions for GCS.
		GCS ReadOnlyAccess		Read-only permissions for GCS.
		GCS CommonOperations		Common operation permissions for GCS.
Cloud Eye (Project-level service)	Region-specific projects	CES Administrator	Role	Full permissions for Cloud Eye. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**

Service	Scope	Role/Policy Name	Type	Description
	Region-specific projects	CES FullAccess	Policy	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 policy-based authorization**.
	Region-specific projects	CES ReadOnlyAccess		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 policy-based authorization**.
Web Application Firewall (WAF) (Project-level service)	Region-specific projects	WAF Administrator	Role	Full permissions for WAF.
		WAF FullAccess	Policy	Full permissions for WAF.
		WAF ReadOnlyAccess		Read-only permissions for WAF.
Host Security Service (HSS) (Project-level service)	Region-specific projects	HSS Administrator	Role	Full permissions for HSS.
		HSS FullAccess	Policy	Full permissions for HSS.
		HSS ReadOnlyAccess		Read-only permissions for HSS.
Vulnerability Scan Service (VSS) (Project-level service)	Region-specific projects	VSS Administrator	Role	Full permissions for VSS.

Service	Scope	Role/Policy Name	Type	Description
Managed Detection and Response (MDR) (Project-level service)	Region-specific projects	SES Administrator	Role	MDR administrator with full permissions. **This role must be used together with the BSS Administrator role in the same project.**
Database Security Service (DBSS) (Project-level service)	Region-specific projects	DBSS System Administrator	Role	Full permissions for DBSS.
		DBSS Audit Administrator		Security auditing permissions for DBSS.
		DBSS Security Administrator		Security protection permissions for DBSS.
		DBSS FullAccess	Policy	Full permissions for DBSS.
		DBSS ReadOnlyAccess		Read-only permissions for DBSS. Users granted these permissions can only view this service and cannot configure resources in it.
Data Encryption Workshop (DEW) (Project-level service)	Region-specific projects	KMS Administrator	Role	DEW administrator with full permissions.
		KMS CMKFullAccess	Policy	Full permissions for encryption keys in DEW.
		DEW KeypairFullAccess		Full permissions for key pairs in DEW.
		DEW KeypairReadOnlyAccess		Permissions for viewing key pairs in DEW.

Service	Scope	Role/Policy Name	Type	Description
Anti-DDoS (Project-level service)	Region-specific projects	Anti-DDoS Administrator	Role	Full permissions for Anti-DDoS. **This role must be used together with the Tenant Guest role in the same project.**
Advanced Anti-DDoS (AAD) (Project-level service)	Region-specific projects	CAD Administrator	Role	AAD administrator with full permissions.
Scalable File Service (SFS) (Project-level service)	Region-specific projects	SFS FullAccess	Policy	Full permissions for SFS.
		SFS ReadOnlyAccess		Read-only permissions for SFS.
		SFS Turbo FullAccess		Full permissions for SFS Turbo.
		SFS Turbo ReadOnlyAccess		Read-only permissions for SFS Turbo.
		SFS Administrator	Role	Full permissions for SFS. **This role must be used together with the Tenant Guest role in the same project.**
Distributed Cache Service (DCS) (Project-level service)	Region-specific projects	DCS FullAccess	Policy	Full permissions for DCS.
		DCS UserAccess		Common user permissions for DCS operations except creating, modifying, deleting, and scaling instances.
		DCS ReadOnlyAccess		Read-only permissions for DCS.

Service	Scope	Role/Policy Name	Type	Description
		DCS Administrator	Role	Full permissions for DCS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
MapReduce Service (MRS) (Project-level service)	Region-specific projects	MRS FullAccess	Policy	Full permissions for MRS.
		MRS CommonOperations		Common user permissions for MRS operations except creating and deleting resources.
		MRS ReadOnlyAccess		Read-only permissions for MRS.
		MRS Administrator	Role	Full permissions for MRS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
ServiceStage Cloud Performance Test Service (CPTS) (Project-level service)	Region-specific projects	ServiceStage Administrator	Role	Permissions for performing operations on test resources of all users in CPTS, such as adding, deleting, modifying, and querying test resources.
		ServiceStage Developer		Permissions for performing operations only on a user's own test resources, such as adding, deleting, modifying, and querying test resources.
		ServiceStage Operator		Users can only read their own test resources.
		ServiceStage FullAccess	Policy	Full permissions for ServiceStage.
		ServiceStage ReadOnlyAccess		Read-only permissions for ServiceStage.

Service	Scope	Role/Policy Name	Type	Description
		ServiceStage Development		Developer permissions for ServiceStage, including permissions for performing operations on applications, components, and environments, but excluding approval permissions and permissions for creating infrastructure.
Cloud Service Engine (CSE)	Region-specific projects	CSE FullAccess	Policy	Full permissions for CSE.
		CSE ReadOnlyAccess		Read-only permissions for CSE.
Elastic Load Balance (ELB) (Project-level service)	Region-specific projects	ELB FullAccess	Policy	Full permissions for ELB.
		ELB ReadOnlyAccess		Read-only permissions for ELB.
		ELB Administrator	Role	Full permissions for ELB. **This role must be used together with the Tenant Guest role in the same project.**
NAT Gateway (Project-level service)	Region-specific projects	NAT FullAccess	Policy	Full permissions for NAT Gateway.
		NAT ReadOnlyAccess		Read-only permissions for NAT Gateway.
		NAT Gateway Administrator	Role	Full permissions for NAT Gateway. **This role must be used together with the Tenant Guest role in the same project.**
Direct Connect (Project-level service)	Region-specific projects	Direct Connect Administrator	Role	Full permissions for Direct Connect. **This role must be used together with the Tenant Guest role in the same project.**

Service	Scope	Role/Policy Name	Type	Description
Virtual Private Network (VPN) (Project-level service)	Region-specific projects	VPN Administrator	Policy	Administrator permissions for VPN. **This role must be used together with the Tenant Guest and VPC Administrator roles in the same project.**
		VPN FullAccess	Policy	Full permissions for VPN.
		VPN ReadOnlyAccess		Read-only permissions for VPN.
Cloud Backup and Recovery (CBR) (Project-level service)	Region-specific projects	CBR FullAccess	Policy	Administrator permissions for using all vaults and policies on CBR.
		CBR BackupsAndVaultsFullAccess	Policy	Common user permissions for creating, viewing, and deleting vaults on CBR.
		CBR ReadOnlyAccess	Policy	Read-only permissions for viewing data on CBR.
Graph Engine Service (GES) (Project-level service)	Region-specific projects	GES Administrator	Role	Full permissions for GES. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
		GES Manager		Advanced user of GES with permissions for performing any operations on GES resources except creating and deleting graphs. **This role must be used together with the Tenant Guest role in the same project.**

Service	Scope	Role/Policy Name	Type	Description
		GES Operator		Permissions for viewing and accessing graphs. **This role must be used together with the Tenant Guest role in the same project.**
	Region-specific projects	GES FullAccess	Policy	Administrator permissions for performing all operations (including creation, deletion, access, and upgrade operations) on GES.
		GES Development		Operator permissions for all operations except creating and deleting graphs.
		GES ReadOnlyAccess		Read-only permissions for viewing resources, such as graphs, metadata, and backup data.
ModelArts (Project-level service)	Region-specific projects	ModelArts FullAccess	Policy	Administrator permissions for performing all operations on ModelArts.
		ModelArts CommonOperations		Permissions for performing all operations except managing dedicated resource pools on ModelArts.
DataArts Studio (Project-level service)	Region-specific projects	DAYU Administrator	Role	Full permissions for DataArts Studio. Users with the **DAYU Administrator** role have all permissions for workspaces. Only DAYU Administrator has the permission to configure default items of DataArts Factory (including the periodic scheduling, multi-IF policy, hard and soft lock policy, and format of script variables). DAYU User does not have this permission.

Service	Scope	Role/Policy Name	Type	Description
		DAYU User		Common DataArts Studio user. Users with the **DAYU User** role have the permissions of the role assigned to them in a workspace.
		DAYU User		Common DataArts Studio user. Users with the **DAYU User** role have the permissions of the role assigned to them in a workspace.
		DWS ReadOnlyAccess		Read-only permissions for DWS.
		DWS Administrator	Role	Full permissions for DWS. **This role must be used together with the Tenant Guest and Server Administrator roles 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.
Data Lake Insight (DLI) (Project-level service)	Region-specific projects	DLI Service Admin	Role	Full permissions for DLI.
		DLI Service User		Permissions for using DLI, but not for creating resources.
Data Ingestion Service (DIS) (Project-level service)	Region-specific projects	DIS Administrator	Role	Full permissions for DIS.
		DIS Operator		Permissions for managing streams, such as creating and deleting streams, but not for uploading and downloading data.

Service	Scope	Role/Policy Name	Type	Description
		DIS User		Permissions for uploading and downloading data, but not for managing streams.
Conversational Bot Service (CBS) (Project-level service)	Region-specific projects	CBS Administrator	Role	Full permissions for CBS.
		CBS Guest		Read-only permissions for CBS.
Huawei HiLens (Project-level service)	Region-specific projects	HiLens FullAccess	Policy	Administrator permissions for Huawei HiLens. Users granted these permissions can operate and use all Huawei HiLens resources. **If you want to grant permissions for participating in OBT, receiving alarms, and setting skill messages, assign the SMN Administrator role in the same project.**
		HiLens CommonOperations		Operation permissions for Huawei HiLens. Users granted these permissions can perform operations on Huawei HiLens, except deregistering devices and suspending skills.
		HiLens ReadOnlyAccess		Read-only permissions for Huawei HiLens. Users granted these permissions can only view Huawei HiLens data. **If you want to grant permissions for participating in OBT, receiving alarms, and setting skill messages, assign the SMN Administrator role in the same project.**

Service	Scope	Role/Policy Name	Type	Description
Trusted Intelligent Computing Service (TICS) (Project-level service)	Region-specific projects	TICS FullAccess	Policy	Full permissions for TICS.
		TICS ReadOnlyAccess		Read-only permissions for TICS.
		TICS CommonOperations		Permissions for managing alliances, jobs, agents, notifications, and datasets in TICS.
Workspace (Project-level service)	Region-specific projects	Workspace Administrator	Role	Full permissions for Workspace. **This role must be used together with the Tenant Guest, Server Administrator, and VPC Administrator roles in the same project.**
ROMA Connect (Project-level service)	Region-specific projects	ROMA Administrator	Role	Administrator permissions for ROMA Connect. Users granted these permissions can use all ROMA Connect functions. **This role must be used together with the following dependence roles in the same project:** • To use VPC channels, the user must also be assigned the **VPC Administrator** role. • To use FunctionGraph as the backend service of APIs, the user must also be assigned the **FunctionGraph Administrator** role. • To use a rule engine to forward data to DIS, the user must also be assigned the **DIS Administrator** role.

Service	Scope	Role/Policy Name	Type	Description
		ROMA FullAccess	Policy	Full permissions for ROMA Connect. Users granted these permissions can use all ROMA Connect instances.
		ROMA CommonOperations		Common user permissions for ROMA Connect. This policy does not include permissions for creating, modifying, and deleting instances.
		ROMA ReadOnlyAccess		Read-only permissions for ROMA Connect. Users granted these permissions can only view ROMA Connect data.
Intelligent EdgeCloud (IEC) (Global service)	Global service project	IEC FullAccess	Policy	Full permissions for IEC. Users with these permissions can perform any operations on IEC resources.
		IEC ReadOnlyAccess		Read-only permissions for IEC. Users with these permissions can only view IEC data, for example, viewing the usage of IEC resources.
Professional Services (Global/project-level service)	All projects	PSDMFullAccess	Policy	Full permissions for the Professional Service Delivery Management (PSDM) platform.
		PSDMReadOnlyAccess		Read-only permissions for the PSDM platform.
ProjectMan (Project-level service)	Region-specific projects	ProjectManConfigOperations	Policy	Full permissions for ProjectMan.
Dedicated Host (DeH)	Region-specific projects	DeH FullAccess	Policy	Full permissions for DeH.
		DeH CommonOperations		Basic operation permissions for DeH.

Service	Scope	Role/Policy Name	Type	Description
(Project-level service)		DeH ReadOnlyAccess		Read-only permissions for DeH. Users with these permissions can only query DeHs.
Data Security Center (DSC) (Project-level service)	Region-specific projects	DSC FullAccess	Policy	Full permissions for DSC.
		DSC ReadOnlyAccess		Read-only permissions for DSC.
		DSC Dashboard ReadOnlyAccess		Read-only permissions for the overview page of DSC.
CloudSite (Project-level service)	Region-specific projects	CloudSite FullAccess	Policy	Full permissions for CloudSite.
		CloudSite ReadOnlyAccess		Read-only permissions for CloudSite.
		CloudSite CommonOperations		Basic operation permissions for CloudSite, including the permissions for viewing and modifying site information.
DevCloud (Project-level service)	Region-specific projects	DevCloud Console FullAccess	Policy	Full permissions for the DevCloud console.
		DevCloud Console ReadOnlyAccess		Read-only permissions for the DevCloud console.
ICP License Service (Global service)	Global service project	Beian Administrator	Role	ICP License Service administrator with full permissions.
Voice Call Message & SMS (Project-level service)	Region-specific projects	RTC Administrator	Role	Full permissions for Voice Call, Message & SMS, and Private Number.

Service	Scope	Role/Policy Name	Type	Description
Private Number (Project-level service)	Region-specific projects	RTC Administrator	Role	Full permissions for Voice Call, Message & SMS, and Private Number.
		PrivateNumber FullAccess	Policy	Full permissions for Private Number.
		PrivateNumber ReadOnlyAccess		Read-only permissions for Private Number.
Cloud Data Migration (CDM) (Project-level service)	Region-specific projects	CDM Administrator	Role	Full permissions for CDM. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
		CDM FullAccess	Policy	Administrator permissions for performing all operations on CDM.
		CDM FullAccessExceptUpdateEIP		Permissions for performing all operations except binding and unbinding EIPs on CDM.
		CDM CommonOperations		Permissions for performing operations on CDM jobs and links.
		CDM ReadOnlyAccess		Read-only permissions for CDM. Users granted these permissions can only view CDM clusters, links, and jobs.
Server Migration Service (SMS) (Global service)	Global service project	SMS FullAccess	Policy	Full permissions for SMS.
		SMS ReadOnlyAccess		Read-only permissions for SMS.

Service	Scope	Role/Policy Name	Type	Description
Object Storage Migration Service (OMS) (Project-level service)	Region-specific projects	OMS Administrator	Role	Full permissions for OMS. **To use OMS, an IAM user must also be assigned the OBS OperateAccess policy.**
Cloud Connect (CC) (Global service)	Global service project	Cross Connect Administrator	Role	CC administrator with full permissions. **This role must be used together with the Tenant Guest and VPC Administrator roles in the same project.**
		CC FullAccess	Policy	Full permissions for CC.
		CC ReadOnlyAccess		Read-only permissions for CC.
		CC Network Depend QueryAccess		Read-only permissions required to access dependency resources when using CC.
Huawei Cloud Real-Time Communication (CloudRTC) (Global service)	Global service project	RTC FullAccess	Policy	Full permissions for CloudRTC.
		RTC ReadOnlyAccess		Read-only permissions for CloudRTC.
Video on Demand (VOD) (Project-level service)	Region-specific projects	VOD Administrator	Role	Full permissions for operations on all media files.
		VOD Group Administrator		Permissions for operations (except global configuration and domain name management) on media files created by users in the current group.

Service	Scope	Role/Policy Name	Type	Description
		VOD Group Operator		Permissions for operations (except media review, media deletion, global configuration, and domain name management) on media files created by users in the current group.
		VOD Group Guest		Permissions for querying media files created by users in the current group.
		VOD Operator		Permissions for operations (except media review, global configuration, and domain name management) on video files created by users in the current group.
		VOD Guest		Read-only permissions for VOD.
		VOD FullAccess	Policy	Full permissions for VOD.
		VOD ReadOnlyAccess		Read-only permissions for VOD.
		VOD CommonOperations		Basic operation permissions for VOD, excluding permissions for global configuration, domain name management, permissions management, settings review, and audio and video hosting.
Live (Project-level service)	Region-specific projects	Live FullAccess	Policy	Full permissions for Live
		Live ReadOnlyAccess		Read-only permissions for Live
Face Recognition Service (FRS)	Region-specific projects	FRS FullAccess	Policy	Full permissions for FRS.

Service	Scope	Role/Policy Name	Type	Description
(Project-level service)		FRS ReadOnlyAccess		Read-only permissions for FRS.
Distributed Database Middleware (DDM) (Project-level service)	Region-specific projects	DDM FullAccess	Policy	Full permissions for DDM.
		DDM CommonOperations		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 ReadOnlyAccess		Read-only permissions for DDM.
Cloud Search Service (CSS) (Project-level service)	Region-specific projects	Elasticsearch Administrator	Role	Full permissions for CSS. **This role must be used together with the Tenant Guest and Server Administrator roles in the same project.**
API Gateway (Project-level service)	Region-specific projects	APIG Administrator	Role	Administrator permissions for API Gateway. Users granted these permissions can use all functions of the **shared** and **dedicated** gateways. **To use VPC channels, the user must also be assigned the VPC Administrator role.** **To use custom authentication, the user must also be assigned the FunctionGraph Administrator role.**

Service	Scope	Role/Policy Name	Type	Description
		APIG FullAccess	Policy	Full permissions for API Gateway. Users granted these permissions can use all functions of **dedicated** API gateways.
		APIG ReadOnlyAccess		Read-only permissions for API Gateway. Users granted these permissions can only view **dedicated** API gateways.
Cloud Firewall (CFW) (Project-level service)	Region-specific projects	CFW FullAccess	Policy	Full permissions for CFW.
		CFW ReadOnlyAccess		Read-only permissions for CFW.
Message Center (Global service)	Global service project	MessageCenter FullAccess	Policy	Full permissions for Message Center.
		MessageCenter ReadOnlyAccess		Read-only permissions for Message Center.
		MessageCenter RecipientManagement		Message receiving management permissions for Message Center, including permissions for configuring SMS messages, emails, and voice messages, viewing and modifying recipients.

