Permissions Policies

Issue 01

Date 2024-10-21

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 System-defined 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 be applied.

- Global services: 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 globally.
- 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 must be assigned in region-specific projects and will be applied only for specific regions.
  - All resources: Permissions will be applied for both global services and region-specific projects, including projects created later.
  - Region-specific projects: Permissions will be applied 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 Permissions

Service	Scope	Policy/Role Name	Type	Description
BASE	Global services	FullAccess	Policy	Full permissions for cloud services supporting policy-based authorization.
	All resources	Tenant Administrator	Role	Full permissions for all services except IAM. **NOTE** ● If the permission scope is **Global services**, they will be applied for global services. ● If the permission scope is **All resources**, they will be applied for both global services and all region-specific projects, including projects created later. ● If the permission scope is **Region-specific projects**, they will be applied only for specific projects.
	All resources	Tenant Guest		Read-only permissions for all services except IAM. **NOTE** ● If the permission scope is **Global services**, they will be applied for global services. ● If the permission scope is **All resources**, they will be applied for both global services and all region-specific projects, including projects created later. ● If the permission scope is **Region-specific projects**, they will be applied only for specific projects.
	Global services	Agent Operator		Permissions for switching roles to access resources of delegating accounts.

Service	Scope	Policy/Role Name	Type	Description
Elastic Cloud Server (ECS) (Project-level service)	Region-specific projects	ECSFullAccess	Policy	Full permissions for ECS.
		ECSReadOnlyAccess		Read-only permissions for ECS.
		ECSCommonOperations	Role	Permissions for starting, stopping, restarting, and querying ECSs.
Cloud Container Engine (CCE) (Project-level service)	Region-specific projects	CCEFullAccess	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**.
		CCEReadOnlyAccess		Permissions to view CCE cluster resources, excluding namespace-level permissions for clusters that have Kubernetes RBAC enabled.

Service	Scope	Policy/Role 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 services: **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 services	OBSOperateAccess	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.
		OBSReadOnlyAccess		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	Policy/Role Name	Type	Description
Content Delivery Network (CDN) (Global service)	Global services	CDNDomainReadOnlyAccess	Policy	Read-only permissions for CDN acceleration domain names.
		CDNStatisticsReadOnlyAccess		Read-only permissions for CDN statistics.
		CDNLogsReadOnlyAccess		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 services	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.
		SCMFullAccess	Policy	Full permissions for SCM.

Service	Scope	Policy/Role Name	Type	Description
		SCMReadOnlyAccess		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 services	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 ReadonlyAccess	Policy	Read-only permissions for Billing Center, Cost Center, and Message Center.
		BSS FinanceAccess		Financial administrator of Business Support System (BSS) in Billing Center, who has full permissions for financial operations.
		Enterprise Project BSS FullAccess		All operations permissions supported by Enterprise Project

Service	Scope	Policy/Role 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	Policy/Role 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	AutoScalingFullAccess	Policy	Full permissions for all AS resources.
		AutoScalingReadOnlyAccess		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	IMSFullAccess	Policy	Full permissions for IMS.
		IMS ReadOnlyAccess		Read-only permissions for IMS.
		IMS Administrator	Role	Full permissions for IMS. This role must be used together with the **Tenant Administrator** role in global services.

Service	Scope	Policy/Role Name	Type	Description
Elastic Volume Service (EVS) (Project-level service)	Region-specific projects	EVSFullAccess	Policy	Full permissions for EVS. Users granted these permissions can create, mount, uninstall, query, and delete EVS resources, and expand capacity of EVS disks.
		EVSReadOnlyAccess		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	DSSFullAccess	Policy	Full permissions for DSS.
		DSSReadOnlyAccess		Read-only permissions for DSS.
Virtual Private Cloud (VPC) (Project-level service)	Region-specific projects	VPCFullAccess	Policy	Full permissions for VPC.
		VPCReadOnlyAccess		Read-only permissions for VPC.

Service	Scope	Policy/Role Name	Type	Description
		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	CCEFullAccess	Policy	Full permissions for CCE.
		CCEReadOnlyAccess		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 services: **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.

Service	Scope	Policy/Role Name	Type	Description
Application Orchestration Service (AOS) (Project-level service)	Region-specific projects	CDE Admin	Role	AOS administrator with full permissions.
		CDE Developer		AOS developer.
		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	Policy/Role Name	Type	Description
Identity and Access Management (IAM) (Global service)	Global services	Security Administrator	Role	Full permissions for IAM.
	Global services	IAM ReadOnlyAccess	Policy	Read-only permissions for IAM.
Tag Management Service (TMS) (Global service)	Global services	TMS FullAccess	Policy	Full permissions for TMS.
		TMS ReadOnlyAccess		Read-only permissions for TMS.

Service	Scope	Policy/Role Name	Type	Description
		TMS Administrator	Role	Full permissions for TMS. Users with these permissions can query, create, delete, import, or export predefined tags, and create, delete, modify, or query resource tags. The permissions depend on the following policies: ● **Tenant Guest**: a global/project-level policy that grants read-only permissions for all cloud services (except IAM). ● **Server Administrator**: a project-level policy, which must be assigned in the same project as **TMS Administrator**. ● **Tenant Administrator**: A global/project-level policy that grants administrator permissions for all cloud services (except IAM). ● **IMS Administrator**: a project-level policy, which must be assigned in the same project as **TMS Administrator**. ● **AutoScaling Administrator**: a project-level policy, which must be assigned in the same project as **TMS Administrator**. ● **VPC Administrator**: a project-level policy, which must be assigned in the same project as **TMS Administrator**.

Service	Scope	Policy/Role Name	Type	Description
				- **VBS Administrator**: a project-level policy, which must be assigned in the same project as **TMS Administrator**.
Config (Global service)	Global services	Config ConsoleFullAccess	Policy	Permissions for all operations on the Config console.
		Config FullAccess		Full permissions for Config.
		Config ReadOnlyAccess		Read-only permissions for Config.
Resource Access Manager (RAM) (Global service)	Global services	RAM FullAccess	Policy	Full permissions for RAM.
		RAM ReadOnlyAccess		Read-only permissions for RAM.
		RAM ResourceShareParticipantAccess		Permissions for accepting or reject a resource sharing invitation.
Organizations (Global service)	Global services	Organizations FullAccess	Policy	Full permissions for Organizations.
		Organizations ReadOnlyAccess		Read-only permissions for Organizations.
Enterprise Project Management Service (EPS) (Global service)	Global services	EPS FullAccess	Policy	Full permissions for EPS.
		EPS ReadOnlyAccess		Read-only permissions for EPS.

Service	Scope	Policy/Role Name	Type	Description
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.
		SMNFullAccess	Policy	Full permissions for SMN.
		SMNReadOnlyAccess		Read-only permissions for SMN.
Relational Database Service (RDS) (Project-level service)	Region-specific projects	RDSFullAccess	Policy	Full permissions for RDS.
		RDSReadOnlyAccess		Read-only permissions for RDS.
		RDSUserAccess		Database administrator permissions for all operations except deleting RDS resources.
		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.

Service	Scope	Policy/Role Name	Type	Description
Distributed Message Service (DMS for Kafka and DMS for RabbitMQ) (Project-level service)	Region-specific projects	DMSUserAccess	Policy	Common user permissions for DMS (DMS for Kafka and DMS for RabbitMQ), excluding permissions for creating, modifying, deleting, scaling up instances and dumping.
		DMSReadOnlyAccess		Read-only permissions for DMS (DMS for Kafka and DMS for RabbitMQ). Users granted these permissions can only view DMS data.
		DMSFullAccess		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	DDSFullAccess	Policy	Full permissions for DDS.
		DDSReadOnlyAccess		Read-only permissions for DDS.
		DDSManageAccess		Database administrator permissions for all operations except deleting DDS resources.
		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.

Service	Scope	Policy/Role Name	Type	Description
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.
		DASFullAccess	Policy	Full permissions for DAS.
GeminiDB (Project-level service)	Region-specific projects	GaussDB NoSQL FullAccess	Policy	Full permissions for GeminiDB.
		GaussDB NoSQL ReadOnlyAccess		Read-only permissions for GeminiDB.
GaussDB (Project-level service)	Region-specific projects	GaussDB FullAccess	Policy	Full permissions for GaussDB.
		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.

Service	Scope	Policy/Role Name	Type	Description
Application Operations Management (AOM) (Project-level service)	Region-specific projects	AOMFullAccess	Policy	Full permissions for AOM.
		AOMReadOnlyAccess		Read-only permissions for AOM.
Application Performance Management (APM) (Project-level service)	Region-specific projects	APMFullAccess	Policy	Full permissions for APM.
		APMReadOnlyAccess		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.
		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.

Service	Scope	Policy/Role Name	Type	Description
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.
	Region-specific projects	CESFullAccess	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.

Service	Scope	Policy/Role Name	Type	Description
	Region-specific projects	CESReadOnlyAccess		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.
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.

Service	Scope	Policy/Role Name	Type	Description
		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.
		CSMS FullAccess		Full permissions for Cloud Secret Management Service (CSMS).
		CSMS ReadOnlyAccess		Read-only permissions for CSMS.
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.

Service	Scope	Policy/Role Name	Type	Description
Scalable File Service (SFS) (Project-level service)	Region-specific projects	SFSFullAccess	Policy	Full permissions for SFS.
		SFSReadOnlyAccess		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	DCSFullAccess	Policy	Full permissions for DCS.
		DCSUserAccess		Common user permissions for DCS operations except creating, modifying, deleting, and scaling instances.
		DCSReadOnlyAccess		Read-only permissions for DCS.
		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	MRSFullAccess	Policy	Full permissions for MRS.
		MRSCommonOperations		Common user permissions for MRS operations except creating and deleting resources.
		MRSReadOnlyAccess		Read-only permissions for MRS.

Service	Scope	Policy/Role Name	Type	Description
		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.
		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.

Service	Scope	Policy/Role Name	Type	Description
Elastic Load Balance (ELB) (Project-level service)	Region-specific projects	ELBFullAccess	Policy	Full permissions for ELB.
		ELBReadOnlyAccess		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	NATFullAccess	Policy	Full permissions for NAT Gateway.
		NATReadOnlyAccess		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.
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.

Service	Scope	Policy/Role Name	Type	Description
Cloud Backup and Recovery (CBR) (Project-level service)	Region-specific projects	CBRFullAccess	Policy	Administrator permissions for using all vaults and policies on CBR.
		CBRBackupsAndVaultsFullAccess	Policy	Common user permissions for creating, viewing, and deleting vaults on CBR.
		CBRReadOnlyAccess	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.
		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	GESFullAccess	Policy	Administrator permissions for performing all operations (including creation, deletion, access, and upgrade operations) on GES.
		GESDevelopment		Operator permissions for all operations except creating and deleting graphs.

Service	Scope	Policy/Role Name	Type	Description
		GESReadOnlyAccess		Read-only permissions for viewing resources, such as graphs, metadata, and backup data.
ModelArts (Project-level service)	Region-specific projects	ModelArtsFullAccess	Policy	Administrator permissions for performing all operations on ModelArts.
		ModelArtsCommonOperations		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.
		DAYU User		Common DataArts Studio user. Users with the **DAYU User** role have the permissions of the role assigned to them in a workspace.
GaussDB(DWS)	Region-specific projects	DWS FullAccess	Policy	Database administrator permissions for GaussDB(DWS). Users granted these permissions can perform all operations on GaussDB(DWS).
		DWSReadOnlyAccess		Read-only permissions for DWS.

Service	Scope	Policy/Role Name	Type	Description
		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.
		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.

Service	Scope	Policy/Role Name	Type	Description
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 permission to participate in OBT, receive alarms, and set 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 permission to participate in OBT, receive alarms, and set skill messages, assign the **SMN Administrator** role in the same project.
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 FullAccess	Policy	Full permissions for Workspace.

Service	Scope	Policy/Role Name	Type	Description
		Workspace DesktopsManager		Desktop administrator permissions for Workspace.
		Workspace UserManager		User administrator permissions for Workspace.
		Workspace SecurityManager		Security administrator permissions for Workspace.
		Workspace TenantManager		Tenant administrator permissions for Workspace.
		Workspace ReadOnlyAccess		Read-only permissions for Workspace.
ROMA Connect (Project-level service)	Region-specific projects	ROMA Administrator	Role	Administrator permissions for ROMA Connect. Users with these permissions can perform all operations on ROMA Connect. 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	Policy/Role 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.
CloudLake (IEC) (Global service)	Global services	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 resources	PSDMFullAccess	Policy	Full permissions for the Professional Service Delivery Management (PSDM) platform.
		PSDMReadOnlyAccess		Read-only permissions for the PSDM platform.
CodeArts Req (Project-level service)	Region-specific projects	ProjectManConfigOperations	Policy	Full permissions for ProjectMan.

Service	Scope	Policy/Role Name	Type	Description
Dedicated Host (DeH) (Project-level service)	Region-specific projects	DeH FullAccess	Policy	Full permissions for DeH.
		DeH CommonOperations		Basic operation permissions for DeH.
		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.
CodeArts (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 services	Beian Administrator	Role	ICP License Service administrator with full permissions.

Service	Scope	Policy/Role Name	Type	Description
Voice Call (Project-level service)	Region-specific projects	RTC Administrator	Role	Full permissions for Voice Call, Message & SMS, and Private Number.
Message & SMS (Project-level service)	Region-specific projects	RTC Administrator	Role	Full permissions for Voice Call, Message & SMS, and Private Number.
		MSGSMS FullAccess	Policy	Common user permissions for Message & SMS. Users granted these permissions can perform all operations supported by Message & SMS, including creation, deletion, and viewing, and modifying specifications.
		MSGSMS ReadOnlyAccess		Read-only permissions for Message & SMS. Users granted these permissions can only view Message & SMS statistics.
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.
		CDMFullAccess	Policy	Administrator permissions for performing all operations on CDM.

Service	Scope	Policy/Role Name	Type	Description
		CDMFullAccessExceptUpdateEIP		Permissions for performing all operations except binding and unbinding EIPs on CDM.
		CDMCommonOperations		Permissions for performing operations on CDM jobs and links.
		CDMReadOnlyAccess		Read-only permissions for CDM. Users granted these permissions can only view CDM clusters, links, and jobs.
Server Migration Service (SMS) (Global service)	Global services	SMS FullAccess	Policy	Full permissions for SMS.
		SMS ReadOnlyAccess		Read-only permissions for SMS.
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 services	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.

Service	Scope	Policy/Role Name	Type	Description
Huawei Cloud Real-Time Communication (CloudRTC) (Global service)	Global services	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.
		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.

Service	**Scope**	**Policy/Role Name**	**Type**	**Description**
		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) (Project-level service)	Region-specific projects	FRS FullAccess	Policy	Full permissions for FRS.
		FRS ReadOnlyAccess		Read-only permissions for FRS.
Distributed Database Middleware (DDM) (Project-level service)	Region-specific projects	DDMFullAccess	Policy	Full permissions for DDM.
		DDMCommonOperations		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
		DDMReadOnlyAccess		Read-only permissions for DDM.

Service	Scope	Policy/Role Name	Type	Description
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.
		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 services	MessageCenter FullAccess	Policy	Full permissions for Message Center.

Service	Scope	Policy/Role Name	Type	Description
		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.
Ubiquitous Cloud Native Service (UCS) (Global service)	Global services	UCS FullAccess	Policy	UCS administrator permissions, including creating permissions policies and security policies.
		UCS CommonOperations		Common UCS user permissions for creating workloads, distributing traffic, and other operations.
		UCS CIAOperations		UCS Container Intelligent Analysis (CIA) administrator with full permissions.
		UCS ReadOnlyAccess		Read-only permissions on UCS (except for CIA).
Service Ticket (Global service)	Global services	Ticket Administrator	Role	Full permissions for Service Ticket.
		Ticket Group Operator		Permissions for processing service tickets of other users in the same group.