

Simple Message Notification

Service Overview

Issue 01
Date 2026-02-11



Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

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 Simple Message Notification.....	1
2 Service Advantages.....	2
3 Application Scenarios.....	4
4 Functions.....	5
5 Security.....	8
5.1 Identity Authentication and Access Control.....	8
5.2 Data Protection Technologies.....	9
5.3 Auditing and Logging.....	9
5.4 Resilience.....	9
5.5 Certificates.....	10
6 Notes and Constraints.....	12
7 Accessing and Using SMN.....	14
8 Billing.....	15
9 Permissions.....	17
10 SMN and Other Services.....	24
11 Concepts.....	26
12 Region and AZ.....	28

1 Simple Message Notification

Simple Message Notification (SMN) is a reliable and flexible large-scale message notification service. It enables you to efficiently send messages to various endpoints, such as phone numbers and email addresses.

SMN offers a publish/subscribe model to achieve one-to-multiple message subscriptions and notifications in a variety of message types. SMN involves two roles: publisher and subscriber. A publisher publishes messages to a topic, and SMN then delivers the messages to subscribers in the topic. The subscribers can be email addresses, phone numbers, and URLs.

A topic is a collection of messages and a logical access point, through which the publisher and the subscriber can interact with each other. Each topic has a unique name. The topic creator can configure topic policies to grant other users or cloud services permissions to perform certain operations to a topic, for example, querying subscriptions or publishing messages.

2 Service Advantages

SMN has the following advantages over other traditional messaging systems.

Table 2-1 SMN advantages

Item	SMN	Traditional Messaging System
Simplicity	SMN provides three basic APIs to create topics, add subscriptions, and publish messages. SMN can be quickly integrated with your services. It enables you to send messages in substantial quantity and does not require highly skilled development.	A self-developed messaging system is expensive and takes a long time to integrate with your services. Its APIs are complex and hard to use.
Stability and reliability	SMN is deployed across multiple data centers to ensure redundancy and high availability. If one service node is faulty, your requests are automatically processed by another available node.	A traditional messaging system cannot achieve the stability and reliability required by critical services and does not provide measures to ensure service continuity.
Multiple message types	You publish a message once, and SMN delivers it to endpoints in various message types.	You need to develop separate messaging systems in multiple types to send SMS message, FunctionGraph (function), email, HTTP, or HTTPS notifications.

Item	SMN	Traditional Messaging System
Security	SMN isolates data based on topics and prevents any unauthorized users from accessing message queues, thereby protecting your service data.	Service data is potentially exposed to unauthorized access due to lack of effective protection mechanisms.

3 Application Scenarios

- **System notifications**

After events or alarms are triggered, SMN can send notifications to specified users by email, SMS message, FunctionGraph (function), or HTTP/HTTPS message. For example, Cloud Trace Service (CTS) detects key cloud service operations and uses SMN to notify you and other users.

- **Off-peak traffic control**

If there is a discrepancy between processing capabilities of the upstream and downstream systems, SMN can cache data to reduce downstream pressure to reduce breakdowns, enhance availability, and mitigate complexity in the system.

4 Functions

This section describes main functions of SMN. You can check if a certain function is available in a region on the management console.

Billing

SMN is billed based on downstream Internet traffic and notification messages.

The billing modes for each notification type are as follows:

- SMS: The number of SMS notifications sent
- Email: The number of email notifications plus downstream Internet traffic
- HTTP or HTTPS: The number of HTTP or HTTPS requests plus downstream Internet traffic

Topics

A topic is a specified event to publish messages and subscribe to notifications. It serves as a message sending channel, where publishers and subscribers can interact with each other.

After a topic is created, the system generates a topic URN, which uniquely identifies the topic and cannot be changed. The topic you created is displayed in the topic list.

Subscriptions

A subscription is how you add endpoints to a topic. To deliver messages published to a topic to endpoints, you must add the subscription endpoints to the topic. Endpoints can be email addresses, phone numbers, and HTTP/HTTPS URLs. After you add endpoints to the topic and the subscribers confirm the subscription, they are able to receive messages published to the topic.

You can add multiple subscriptions to each topic. After you add a subscription, SMN sends a confirmation message to the subscription endpoint. The message contains a link for confirming the subscription. The subscription confirmation link is valid within 48 hours. Confirm the subscription on your mobile phone, mailbox, or other endpoints in time.

Subscribers

A subscription is how you add endpoints to a topic. On the **Subscribers** page, you can centrally manage subscriber information across regions. You can create multiple subscribers and batch subscribe them to a topic.

Currently, subscriber data can be stored and viewed only in regions in China.

Message Templates

Message templates contain fixed and changeable content and can be used to create and send messages more quickly. When you use a template to publish a message, you can specify values for different variables in the template.

Message templates are identified by name, but you can create different templates with the same name as long as they are configured for different protocols. You must create a **Default** template with the same name as each custom template. The **Default** template is used when no specific template has been set for a given protocol. If a template is configured for a specific protocol, any subscriber who chose that protocol during subscription will receive messages using that specific template. If you create a custom template but do not create a default template with the same name, you cannot use the custom template to publish messages.

Publishing a Message

SMN enables you to publish messages in the following formats:

- Text
- JSON
- Template

After you publish a message to a topic, SMN will deliver the message to all confirmed subscription endpoints in the topic.

If an SMS message exceeds 490 characters, the message may be intercepted by operators. Messages sent to SMS endpoints cannot contain square brackets ([]).

For HTTP or HTTPS endpoints, you must ensure that firewall policies have been enabled for them to allow SMN to send messages over the Internet. SMN automatically assembles messages. The message you receive consists of a message header and a body. For details about parameters, see [HTTP or HTTPS Message Format](#).

Receiving a Message

When you subscribe to a topic, you can specify a protocol. Messages received by each endpoint vary depending on the selected protocol. The available protocols are as follows:

- Email
The system sends notifications to the email address you provide. Email messages contain the message subject, content, and a link to unsubscribe.
- SMS
The system sends text messages to mobile phones. SMS messages only contain the message content.

Enterprise Project

SMN supports enterprise projects. An enterprise project facilitates project-level management and grouping of cloud resources and users.

Permissions

You can use Identity and Access Management (IAM) for fine-grained permissions control for your SMN resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing SMN resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or a cloud service to perform efficient O&M on your SMN resources.

Quota Adjustment

All cloud service resources have quotas to prevent unforeseen spikes in resource usage. Quotas can limit the number and capacity of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

You can also request for an increase in quota if the existing quota does not meet your service requirements.

Auditing Key Operations

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

Once CTS is enabled, it starts recording SMN operations. You can view the operation records of the last 7 days on the CTS management console.

APIs

SMN supports Representational State Transfer (REST) APIs that can be accessed over HTTPS, allowing you to publish messages to a topic.

SDKs

SMN provides Java, Python, Go, and .NET SDKs to facilitate your secondary development.

5 Security

[5.1 Identity Authentication and Access Control](#)

[5.2 Data Protection Technologies](#)

[5.3 Auditing and Logging](#)

[5.4 Resilience](#)

[5.5 Certificates](#)

5.1 Identity Authentication and Access Control

IAM Permission Policies

Identity and Access Management (IAM) is a basic service provided by Huawei Cloud for permissions management, access control, and identity authentication. You can use IAM to create and manage users and user groups, grant permissions to allow or deny their access to cloud services and resources, and configure policies to improve account and resource security. IAM also provides you with multiple secure access credentials.

You can use IAM to control access to your SMN resources. IAM permissions define which actions on your cloud resources are allowed or denied. With IAM, you can use your Huawei Cloud account to create IAM users and assign permissions to the users to control their access to specific resources.

After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by SMN to the user group. Then, all users in this group automatically inherit the granted permissions. For details about the system permissions and policies supported by SMN, see [Permissions Management](#).

Topic Policies

The topic creator has the right to configure topic policies. Using topic policies, you can specify which users and cloud services can perform a certain operation on a topic, for example, querying topic details and publishing messages. Topic creators always have permissions over a topic even if they grant topic permissions to other users.

For details, see [Configuring Topic Policies](#).

5.2 Data Protection Technologies

Static Data Protection

Subscription messages stored in SMN are encrypted using SHA256.

The subscription endpoints include:

- Phone numbers
- Email addresses
- HTTP/HTTPS addresses
- Webhook URLs of DingTalk, WeCom, or Lark group chatbot

Data Transmission Security

Data transmission security refers to the protection of data when it is transmitted between SMN and subscription endpoints.

When sending messages to SMN, you can call SMN APIs over HTTPS to ensure transmission security. SMN can also send HTTPS messages to external systems.

SMN can encrypt message content.

Data Destruction

Deleted data will be retained for 72 hours. After 72 hours, the system permanently deletes the data.

5.3 Auditing and Logging

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records for security analysis, audit compliance, resource tracking, and fault locating.

After CTS is enabled, SMN operations can be recorded for auditing.

- For details about how to enable and configure CTS, see [Overview](#).
- For details about SMN operations that can be audited, see [Key SMN Operations Recorded by CTS](#).
- For details about how to view CTS traces, see [CTS Traces](#).

5.4 Resilience

When individual customers send a large number of messages, the overall service experience of SMN will be affected. To solve this issue, SMN controls traffic from the following aspects:

- Topic

The number of messages that can be sent from a topic with any protocol type within one minute is limited. By default, 3,000 messages can be sent within 1 minute.

- SMS messages from a tenant

The number of SMS messages that a tenant can send to any phone number in a specified period is limited. By default, 10,000 messages can be sent within 10 minutes.

- Email messages from a tenant

The number of email messages that a tenant can send to any email address in a specified period is limited. By default, 1,000 messages can be sent within 10 minutes.

- SMS messages from a topic

For a specific topic, the number of SMS messages that can be sent to any phone number in a specified period is limited. By default, 100 messages can be sent within 10 minutes.

- Email messages from a topic

For a specific topic, the number of email messages that can be sent to any email address in a specified period is limited. By default, 100 messages can be sent within 10 minutes.

- SMS messages sent to a specific phone number

The number of SMS messages that a tenant can send to a specific phone number in a specified period is limited. By default, 100 messages can be sent within 10 minutes.

- Email messages sent to a specific email address

The number of email messages that a tenant can send to a specific email address in a specified period is limited. By default, 100 messages can be sent within 10 minutes.

 **NOTE**

The preceding limitations are for reference only and will be adjusted based on service requirements.

5.5 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

Figure 5-1 Downloading compliance certificates

Download Compliance Certificates

Please enter a keyword to search

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

ISO 27017:2015

ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 5-2 Resource center

Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

6 Notes and Constraints

⚠ CAUTION

When you use SMN to send emails or messages, ensure that the content complies with local laws and regulations.

SMN pushes messages asynchronously, which does not ensure the timeliness of message delivery. If your service requires messages need to be delivered in a quasi-real-time manner, exercise caution whether to use SMN.

The email addresses and phone numbers used by SMN to send emails, SMS messages, or voice calls can be changed. Do not whitelist such email addresses or phone numbers. Otherwise, SMN messages may fail to be received if they are changed.

The source IP address used by SMN to send messages is not fixed and may be changed at any time. Do not configure a whitelist for source IP addresses, or you may fail to receive SMN messages.

For network security purposes, SMN does not send messages to Huawei Cloud private networks by default.

SMN imposes restrictions on some items. Do not exceed their limits when using SMN. Otherwise, program exceptions may occur.

[Table 6-1](#) lists the restrictions on topics.

Table 6-1 Restrictions on topics

Item	Quota	Description
Number of topics	3,000	If the number of topics exceeds the quota, no more topics can be created.
Topic name	1 to 255 characters	If you enter 256 or more characters, the topic cannot be created.

Item	Quota	Description
Display name	192 bytes	If you enter 193 or more bytes, the topic cannot be created.
Tag	20	If you add 21 or more tags to a topic, the topic cannot be created.
Tag key length	128 characters	If you enter 129 or more characters, the tag cannot be created.
Tag value length	255 characters	If you enter 256 or more characters, the tag cannot be created.
Text message title	512 bytes	None
Text message content	256 KB	The maximum length of an SMS message is 490 characters, or the message may be intercepted. Messages sent to SMS endpoints cannot contain square brackets ([]).
JSON message content	256 KB	None
Template message content	256 KB	None

Table 6-2 lists restrictions on subscriptions.

Table 6-2 Restrictions on subscriptions

Item	Quota	Description
Endpoint	10,000	None
Validity of a subscription confirmation link	48 hours	Confirm the subscription on your mobile phone, mailbox, or other endpoints in time.

7 Accessing and Using SMN

You can access the SMN service using a web-based management console and HTTPS-based APIs.

- **Management console**

The management console is a web user interface for you to manage your computing, storage, and other cloud resources. You can access SMN using the management console.

- **APIs**

If you want to integrate SMN into a third-party system for secondary development, you can access SMN using APIs. For details, see *Simple Message Notification API Reference*.

8 Billing

You only pay for what you use with no minimum fees.

Billing Items

You pay based on the number of notification messages and downstream Internet traffic. For details, see [Product Pricing Details](#).

Table 8-1 SMN billing items

Billing Item	Description
Notification messages	<ul style="list-style-type: none"> SMS: You are billed based on the number of SMS messages sent under each topic in each region every month. For details about how to calculate the number of SMS messages, see section SMS Length Calculation in the "Message & SMS Service Overview". <p>NOTE</p> <ul style="list-style-type: none"> International SMS: All SMSs sent will be billed. Chinese mainland SMS: Only successfully sent SMSs will be billed. <ul style="list-style-type: none"> Email: You are billed based on the number of emails sent under each topic in each region every month. HTTP/HTTPS: You are billed based on the number of requests sent under each topic in each region every month. You are billed once for each 1 million requests every month. FunctionGraph: You are billed based on the number of function calls, but SMN messages to FunctionGraph are free. Subscription confirmation messages will be counted as messages sent and will be billed.
Downstream Internet traffic	When your notifications incur Internet traffic, the first 1 GB is free for each month, and extra traffic will be billed per GB according to the Huawei Cloud standard traffic fee.

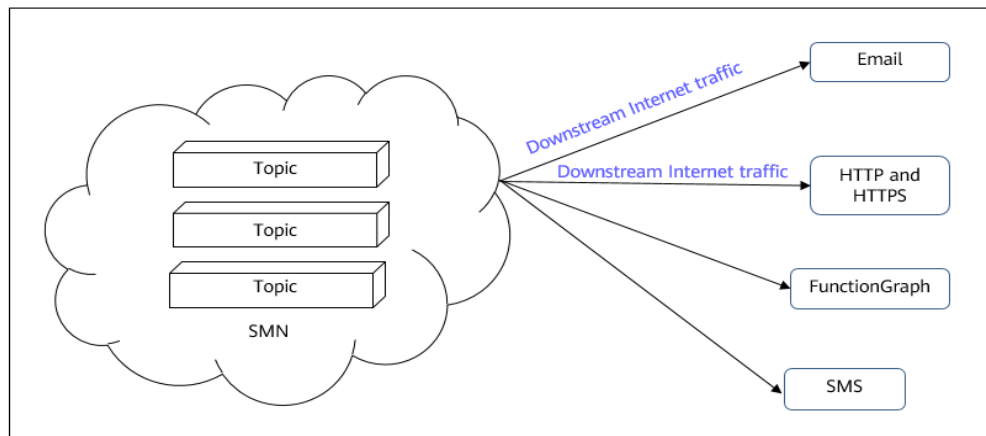
 NOTE

- All billing items are calculated based on a regular calendar month.
- Some cloud services send messages to email addresses or mobile numbers through SMN. In this case, the resource name column in the bill is empty.

Cost Elements in Different Scenarios

SMN is billed based on downstream Internet traffic and notification messages.

Figure 8-1 Billing components



The costs for sending different types of messages relate to different elements:

- SMS: number of SMS notifications
- Email: Email notifications+Downstream Internet traffic
- HTTP or HTTPS: HTTP or HTTPS notifications+Downstream Internet traffic

Renewal

For details, see [Renewal Management](#).

Expiration and Overdue Payment

For details, see [Service Suspension and Resource Release](#) and [Payment and Repayment](#).

9 Permissions

If you need to grant your enterprise personnel permission to access your SMN resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your Huawei Cloud resources. If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM is free. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, if you want some software developers in your enterprise to use SMN resources but do not want them to delete the resources or perform any other high-risk operations, you can grant permissions to use the resources but not permissions to delete them.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

Table 9-1 Differences between role/policy-based authorization and identity policy-based authorization

Authorization Model	Core Relationship	Permissions	Authorization Method	Description
Role/Policy	User-permission-authorization scope	<ul style="list-style-type: none"> System-defined roles System-defined policies Custom policies 	Assigning roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity policy	User-policy	<ul style="list-style-type: none"> System-defined identity policies Custom identity policies 	<ul style="list-style-type: none"> Assigning identity policies to principals Attaching identity policies to principals 	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users the permissions needed to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the users or grant the users the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization models are not interoperable. You are advised to use the identity policy-based authorization model. For details about system-defined permissions, see [Role/Policy-based Authorization](#) and [Identity Policy-based Authorization](#).

For more information about IAM, see [IAM Service Overview](#).

Role/Policy-based Authorization

SMN supports authorization with roles and policies. By default, new IAM users do not have any permissions assigned. You need to add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

SMN is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for VPC Endpoint resources in the selected projects. If you set **Scope** to **All resources**, the users have permissions for VPC Endpoint resources in all region-specific projects. When accessing SMN, the users need to switch to a region where they have been authorized to use this service.

Table 9-2 lists all the system-defined permissions for SMN. System-defined policies and system-defined identity policies in the two authorization models are not interoperable.

Table 9-2 SMN system-defined permissions

Role/Policy	Description	Type	Dependency
SMN Administrator	Administrator permissions for SMN. Users with these permissions can perform all operations on SMN.	System-defined roles	The Tenant Guest and SMN Administrator roles need to be assigned in the same project.
SMN FullAccess	Administrator permissions for SMN. Users with these permissions can perform all operations on SMN.	System-defined policies	None
SMN ReadOnlyAccesses	Read-only permissions for SMN. Users granted these permissions can only view SMN data.	System-defined policies	None

Table 9-3 lists the common operations supported by SMN system-defined permissions.

Table 9-3 Common operations supported by each system-defined policy

Operation	SMN Administrator	SMN FullAccess	SMN ReadOnlyAccess
Creating a topic	√	√	×
Updating a topic	√	√	×
Deleting a topic	√	√	×
Querying topics	√	√	√
Adding a subscription to a topic	√	√	×
Adding a tag to a topic	√	√	×
Configuring a topic policy	√	√	×
Publishing a message	√	√	×
Adding a subscription	√	√	×
Requesting subscription confirmation	√	√	×
Canceling a subscription	√	√	×
Deleting a subscription	√	√	×
Querying subscriptions	√	√	√
Creating a message template	√	√	×
Modifying a message template	√	√	×
Deleting a message template	√	√	×

Operation	SMN Administrator	SMN FullAccess	SMN ReadOnlyAccess
Querying a message template	√	√	√

Identity Policy-based Authorization

SMN supports authorization with identity policies. [Table 9-4](#) lists all the system-defined identity policies for SMN. System-defined identity policies and system-defined policies in the two authorization models are not interoperable.

Table 9-4 System-defined identity policies for SMN

Identity Policy Name	Description	Type
SMNFullAccessPolicy	Full permissions for SMN	System-defined identity policies
SMNReadOnlyPolicy	Read-only permissions for SMN	System-defined identity policies

[Table 9-5](#) lists common operations supported by system-defined identity policies for SMN.

Table 9-5 Common operations supported by system-defined identity policies of SMN

Operation	SMNFullAccessPolicy	SMNReadOnlyPolicy
Querying topics	√	√
Creating a topic	√	x
Querying details of a topic	√	√
Updating a topic	√	x
Deleting a topic	√	x
Querying a topic policy	√	√
Deleting all topic policies	√	x
Updating a topic policy	√	x
Deleting a topic policy	√	x
Querying subscriptions	√	√

Operation	SMNFullAccessPolicy	SMNReadOnlyPolicy
Querying subscriptions of a topic	√	√
Adding a subscription	√	x
Canceling a subscription	√	x
Updating a subscription	√	x
Importing subscribers	√	x
Querying message templates	√	√
Creating a message template	√	x
Querying details of a message template	√	√
Modifying a message template	√	x
Deleting a message template	√	x
Publishing a message	√	x
Publishing a detection message	√	x
Obtaining the HTTP detection result	√	√
Querying resources by tag	√	x
Batch adding or deleting resource tags	√	x
Querying resource tags	√	√
Adding a resource tag	√	x
Query project tags	√	√
Deleting tags from a resource	√	x
Querying all SMN API versions	√	√
Querying the version of SMN API v2	√	√

Operation	SMNFullAccessPolicy	SMNReadOnlyPolicy
Binding a cloud log to a topic	√	x
Querying a cloud log	√	√
Updating a cloud log	√	x
Unbinding a cloud log from a topic	√	x
Creating message filter policies for a subscriber	√	x
Updating message filter policies of subscribers	√	x
Deleting message filter policies of subscribers	√	x

Helpful Links

- [IAM Service Overview](#)

10 SMN and Other Services

SMN can be interconnected with other cloud services to provide them with messaging capabilities so that these services can send notifications to tenants or their message processing systems. For details about how to use SMN in other cloud services, see user guides of the related services.

The following are examples of some services using SMN.

Figure 10-1 SMN and other services

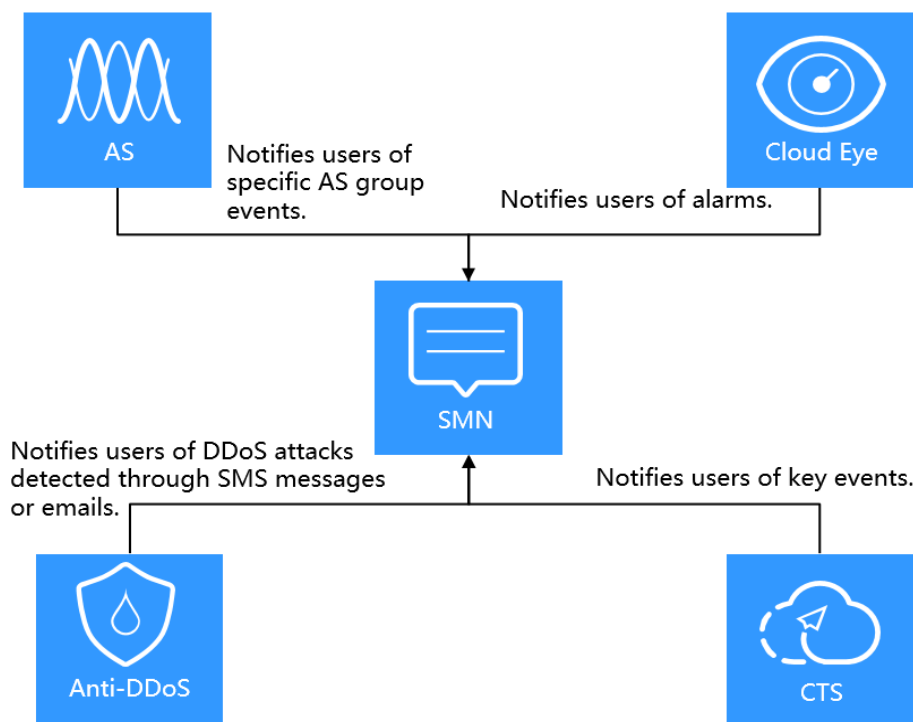


Table 10-1 Services related to SMN

Description	Related Service	Reference
Send notifications using SMN.	Auto Scaling	Configuring Notifications for an AS Group
	Cloud Eye	Introduction to the Alarm Function
	Anti-DDoS	Enabling Alarm Notifications
	CTS	Configuring Key Event Notifications

11 Concepts

Project

Projects are used to group and isolate OpenStack resources, including compute, storage, and networking resources. A project can be either a department or a project team. Multiple projects can be created in one account.

Protocol

A protocol is a message type. SMN supports the following protocols: SMS, Email, HTTP, and HTTPS.

Publisher

A publisher publishes messages to a topic.

Subscriber

A subscriber receives messages published to a topic.

When adding a subscription, you can choose protocols as required:

- Email: The endpoint can be one or more email addresses.
- SMS: The endpoint can be one or more phone numbers.
- HTTP or HTTPS: The endpoint can be one or more URLs.
- FunctionGraph (function): The endpoint can be one function.

Topic

A topic is a specified event to publish messages and subscribe to notifications. It can be used to isolate messages. A topic serves as a message sending channel, where publishers and subscribers can interact with each other.

URN

Uniform Resource Names (URNs) are used to identify SMN resources.

- Topic URN

After a topic is created, SMN generates a topic URN composed of the service name, region name, project ID, and topic name to uniquely identify the topic, for example, **urn:smn:region:cffe4fc4c9a54219b60dbaf7b586e132:Mytopic**. When you call an API to create a topic, a topic URN will be returned. The topic URN will be used whenever a publisher or subscriber performs operations relating to the topic.

- **Subscription URN**

After a user subscribes to a topic, SMN will generate a subscription URN composed of the service name, region name, project ID, topic name, and subscription ID, for example,

urn:smn:region:cffe4fc4c9a54219b60dbaf7b586e132:Mytopic:5293b436967f450abc51e0c36347b27a. The URN is displayed on the **Subscriptions** page for subscribers to confirm or cancel a subscription.

Message Template

Message templates contain fixed and changeable content and can be used to send messages quickly. Changeable content is represented with variables. When you publish template messages, the system replaces the variables with the message content you specify.

Template Variable

A message template contains fixed and changeable content. Changeable content is represented with variables. You can specify values for variables when publishing messages using a template.

For example, the template content is **The Arts and Crafts Exposition will be held from {startdate} through {enddate}. We sincerely invite you to join us..** In the content, *{startdate}* and *{enddate}* are variables.

12 Region and AZ

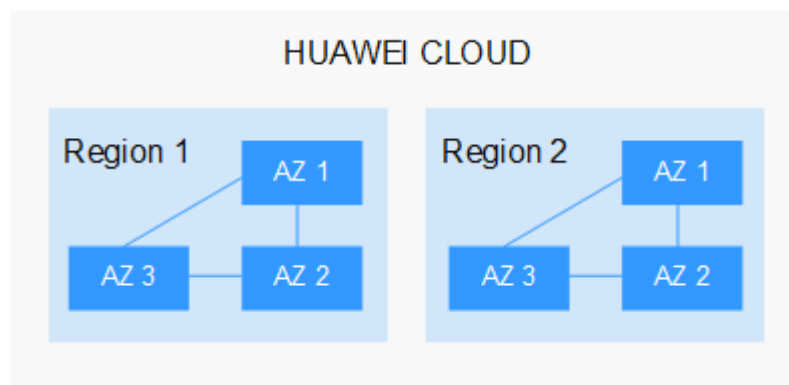
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters.

Figure 12-1 shows the relationship between regions and AZs.

Figure 12-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see [Huawei Cloud Global Products and Services](#).

Selecting a Region

When selecting a region, consider the following factors:

- Location

It is recommended that you select the closest region for lower network latency and quick access.

- If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
- If your target users are in Africa, select the **AF-Johannesburg** region.
- If your target users are in Latin America, select the **LA-Santiago** region.

 **NOTE**

The **LA-Santiago** region is located in Chile.

- Resource price

Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).