Simple Message Notification

Service Overview

Issue	06
Date	2022-11-10

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.

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

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 any 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 and can be quickly integrated with your services. It enables you to send messages in substantial quantity and do not require highly skilled development.	A self-developed messaging system is expensive and takes long time to be integrated with your services. Its APIs are complicated and hard to use.
Stability and reliability	SMN stores messages in multiple data centers and supports transparent topic migration. Once a message fails to deliver, SMN saves it in a message queue and tries to deliver it again. 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, email, HTTP, or HTTPS notifications.

Item	SMN	Traditional Messaging System
Security	SMN isolates data based on topics and does not allow any unauthorized users to access 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, or HTTP/HTTPS message. For example, Cloud Trace Service (CTS) detects key cloud service operations and uses SMN to notify you and other users.

- **Integrating with cloud services**

  SMN can function as a message middleware to directly connect cloud services, improving service efficiency. For example, Cloud Eye does not have to be integrated with Object Storage Service (OBS) to interact with each other. Instead, they can be connected by SMN, so faults in one service will not affect the other.

- **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 Security

4.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

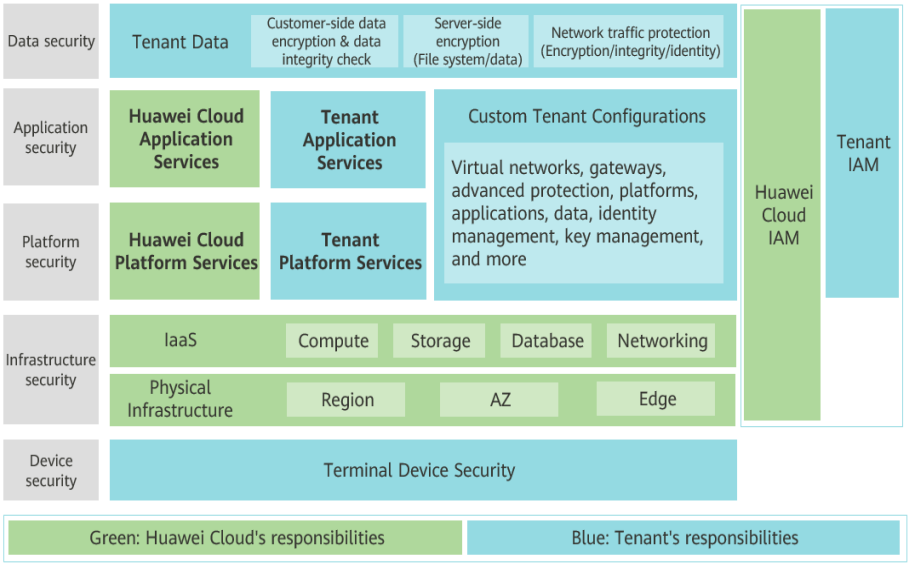
Figure 4-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared

responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 4-1 Huawei Cloud shared security responsibility model



4.2 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**.

4.3 Data Protection Technologies

4.3.1 Static Data Protection

Subscription messages stored in SMN are encrypted using SHA256 encryption.

The subscription endpoints include:

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

4.3.2 Data Transmission Security

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

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

4.3.3 Data Destruction

After a customer deletes data, the data will be retained for 72 hours before being permanently deleted.

4.4 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 **Enabling CTS**.
- 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**.

4.5 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 send 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 send 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

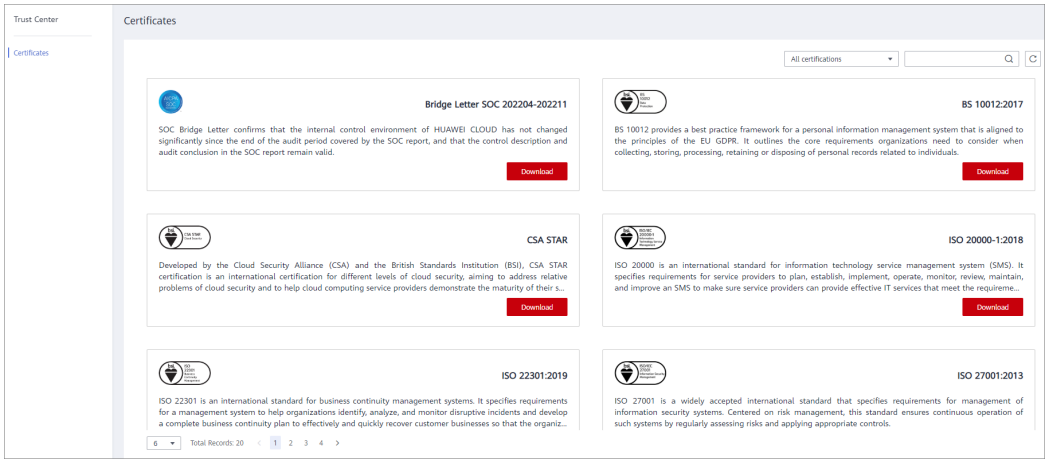
The preceding limitations are for reference only and will be adjusted based on service requirements.

4.6 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.

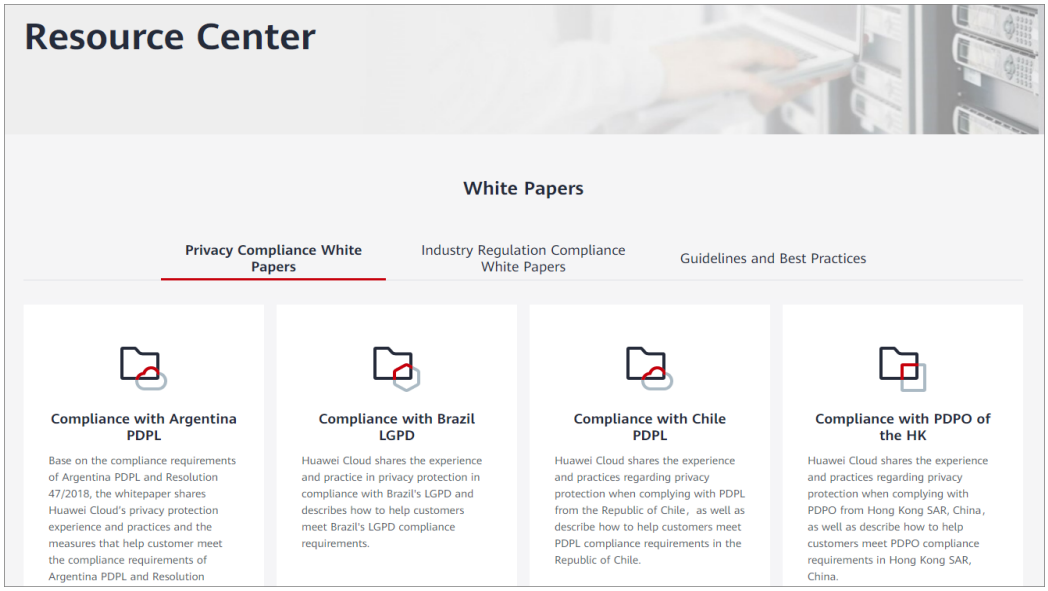
Figure 4-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 4-3 Resource center



5 Notes and Constraints

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 for receiving emails or SMS messages or voice calls from SMN 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 through private networks by default. If you use a Huawei Cloud private IP address to receive SMN messages, contact SMN O&M personnel to configure resolution records for the private IP address and configure firewalls in advance.

6 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 log in the management console and select **Simple Message Notification** on the homepage to switch to the SMN 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*.

7 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 7-1 SMN billing items

Billing Item	Description
Notification messages	• SMS: You are billed based on the number of SMS messages sent 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". **NOTE** • International SMS: All SMSs sent will be billed. • Chinese mainland SMS: Only successfully sent SMSs will be billed. • Email: You are billed based on the number of emails sent in each region every month. • HTTP/HTTPS: You are billed based on the number of requests sent in each region every month. You are billed once for each 1 million requests every month. • FunctionGraph: Notifications sent to FunctionGraph endpoints 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.

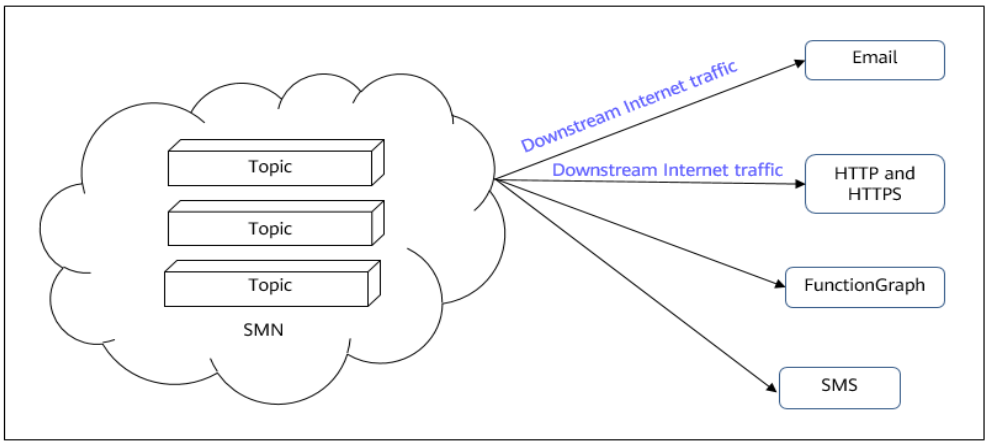
NOTE

All items are calculated based on a regular calendar month.

Cost Elements in Different Scenarios

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

Figure 7-1 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**.

8 Permissions

You can use Identity and Access Management (IAM) to manage SMN permissions and control access to your resources. IAM provides identity authentication, permissions management, and access control.

You can create IAM users for your employees, and assign permissions to these users on a principle of least privilege (PoLP) basis to control their access to specific resource types. For example, you can create IAM users for software developers and assign specific permissions to allow them to use SMN resources but prevent them from being able to delete resources or perform any high-risk operations.

If your Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account.

For more information about IAM, see **IAM Service Overview**.

SMN Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, add them to one or more groups, and attach permissions policies or roles to these groups.

SMN is a project-level service deployed and accessed in specific physical regions. When assigning SMN permissions to a user group, specify region-specific projects where the permissions will take effect. If you select **All projects**, the permissions will be granted for all region-specific projects. When accessing SMN, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: a type of coarse-grained authorization mechanism that provides only a limited number of service-level roles When using roles to grant permissions, you also need to assign dependency roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions This mechanism allows for more flexible policy-based authorization for secure access control. For example, you can grant SMN users only the permissions for managing a certain type of ECSs. Most policies define

permissions based on APIs. For the API actions supported by SMN, see section "Permissions Policies and Supported Actions" in the *Simple Message Notification API Reference*.

Table 8-1 lists all system-defined policies supported by SMN.

Table 8-1 System-defined policies supported by SMN

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

Table 8-2 lists the common operations supported by each SMN system policy or role. Select the policies or roles as needed.

Table 8-2 Common operations supported by each system-defined policy or role of SMN

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 tags to a topic	√	√	×

Operation	SMN Administrator	SMN FullAccess	SMN ReadOnlyAccess
Configuring topic policies	√	√	×
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	√	√	×
Querying a message template	√	√	√

Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting SMN Permissions**
- Supported actions: **Permissions Policies and Supported Actions** in the *Simple Message Notification API Reference*

9 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.

Figure 9-1 lists services related with SMN.

Figure 9-1 SMN and other services

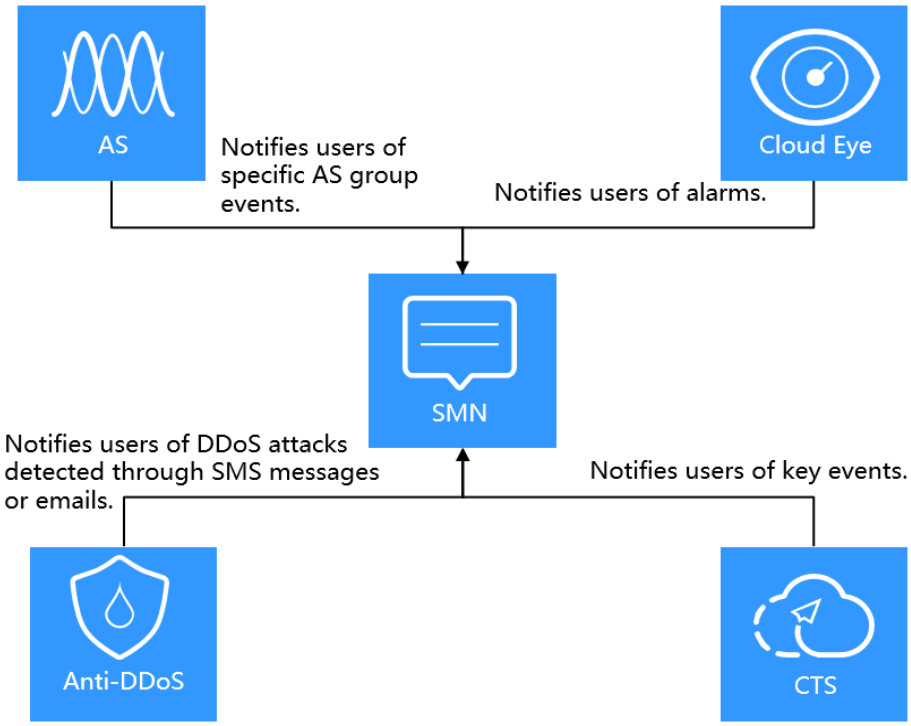


Table 9-1 Services related to SMN

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**
	Cloud Trace Service (CTS)	**Configuring Key Event Notifications**

10 Concepts

Project

Projects are used to group and isolate OpenStack resources, including compute, storage, and network 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, FunctionGraph (function), Email, HTTP, and HTTPS.

Publisher

A publisher sends messages to a topic.

Subscriber

A subscriber receives messages delivered from 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.

11 Region and AZ

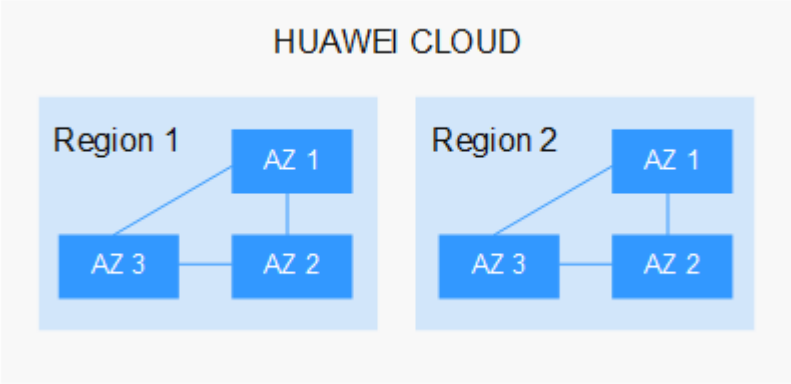
Concept

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. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 11-1 shows the relationship between regions and AZs.

Figure 11-1 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 Regions**.

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**.

12 Change History

Released On	Description
2022-11-10	This issue is the sixth official release, which incorporates the following change: Added section "Security".
2022-03-30	This issue is the fifth official release, which incorporates the following changes: ● Removed **Application** from the supported subscription protocols. ● Removed **DMS** from the supported subscription protocols.
2019-07-05	This issue is the fourth official release, which incorporates the following change: Added Regions and AZs.
2019-02-28	This issue is the third official release, which incorporates the following change: Added the Application subscription protocol.
2018-08-30	This issue is the second official release, which incorporates the following changes: ● Added the SMS subscription protocol. ● Added the DMS subscription protocol.
2017-12-31	This issue is the first official release.

