Domain Name Service

Service Overview

Issue 01

Date 2025-08-01

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is DNS?

Domain Name Service (DNS) is a highly available and scalable authoritative Domain Name System (DNS) web service that translates domain names (such as www.example.com) into IP addresses (such as 192.1.2.3) required for network connection. The DNS service allows end users to visit your websites or web applications using domain names.

The DNS service is free and is enabled by default.

Basic Functions

The DNS service provides the following functions:

- **Public DNS Resolution**

  Maps domain names to public IP addresses so that end users can access your website or web applications over the Internet.
- **Private DNS Resolution**

  Translates private domain names into private IP addresses to facilitate access to cloud resources within VPCs.
- **Reverse resolution**

  Obtains a domain name based on an IP address. Reverse resolution, or reverse DNS lookup, is typically used to affirm the credibility of email servers.
- **Intelligent resolution**

  Returns different IP addresses for the same domain name based on the carrier networks or geographic locations. This significantly reduces network latency for end users from different carrier networks and geographic locations.

Product Advantages

The DNS service has the following advantages:

- High performance

  A single DNS node can handle millions of concurrent queries, allowing end users to access your website or application much faster.
- Easy access to cloud resources

Your ECSs can communicate with each other and with other resources within VPCs using private domain names. Traffic is kept within your internal network, which reduces network latency and improves security.

For more details, see **Configuring Private Domain Names for ECSs**.

- Smooth service migration

  You can transfer the record sets configured for an in-use website domain to the Huawei Cloud DNS service. You can create a public zone and add record sets on the DNS console before the migration. In this way, your website services are not interrupted during the migration.

- Isolation of core data

  A private DNS server provides domain name resolution for ECSs carrying core data, enabling secure, controlled access to such data. You do not need to bind EIPs to these ECSs.

Accessing the DNS Service

The cloud platform provides a web-based management console as well as REST APIs through which you can access the DNS service.

- Management console

  A web-based management console is provided for you to perform operations on the DNS service.

  - If you already have an account, log in to the management console, click **Service List** and choose **Networking** > **Domain Name Service**.
  - If you do not have an account, create one by following the instructions in **Before You Start** and perform the preceding step.

  With a few steps, you can start using the DNS service for domain name resolution.

- APIs

  REST APIs are provided for accessing the DNS service. You can also use the provided APIs to integrate DNS into a third-party system for secondary development. For details, see the **Domain Name Service API Reference**.

2 Public DNS Resolution

What Is Public DNS Resolution?

Public DNS translates domain names and their subdomains into IP addresses for routing traffic over the Internet so that end users to access your website or application over the Internet using your domain name.

Accessing a Website Using a Domain Name

To make your website accessible on the Internet through a domain name, take the following steps:

1. Register your domain name with a domain name registrar.
2. Set up your website.

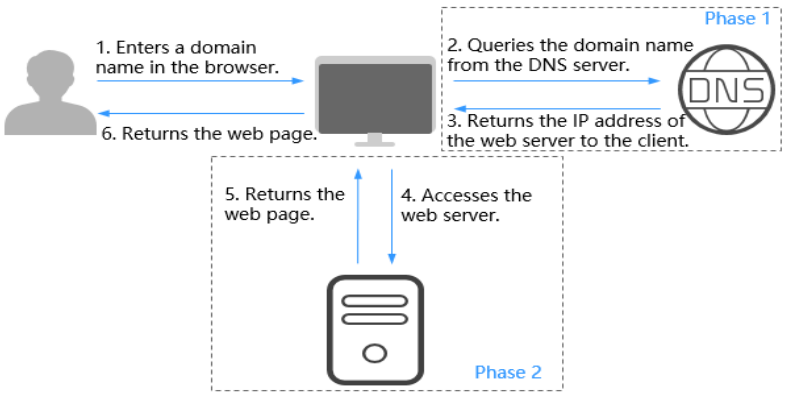
   Purchase cloud resources from Huawei Cloud or other cloud service providers.
3. Configure the DNS service to route Internet traffic for your domain name.

   Create a public zone to host the domain name on the DNS service and add a record set to map the domain name to the EIP of the server where the website is set up.

   For detailed operations, see **Routing Internet Traffic to a Website**.

After you have completed the above steps, end users will be able to access your website on the Internet using the registered domain name or its subdomains.

Figure 2-1 How DNS routes Internet traffic to a website



- Phase 1 shows how DNS resolves your domain name.
- Phase 2 shows how the web page is returned to the user.

Public domain name resolution depends on the DNS hierarchy. The following describes the hierarchy and how domain names are resolved.

DNS Hierarchy

Domain names are hierarchical, and domain name resolution is a recursive lookup process. The following uses example.com to describe the different types of DNS servers at each level.

- Root domain

  A period (.) is the designation for the root domain.

  A fully qualified domain name (FQDN) ends with a period (example.com.). When you enter a domain name (example.com) in the browser, the DNS system will automatically add a period in the end.

  Root domain names are resolved by root DNS servers that hold the addresses of top-level DNS servers.
- Top-level domain

  Below the root domain are top-level domains, which are categorized into two types:

  – Generic top-level domain (gTLD), such as .com, .net, .org, and .top

  – Country code top-level domain (ccTLD), such as .cn, .uk, and .de

  Top-level domains are resolved by top-level DNS servers that hold the addresses of second-level DNS servers. For example, the top-level DNS server of .com saves the addresses of all DNS servers of second-level domain names that end with .com.
- Second-level domain

  Second-level domains (such as example.com) are subdomains of top-level domains and are resolved by second-level DNS servers, which provide authoritative domain name resolution services.

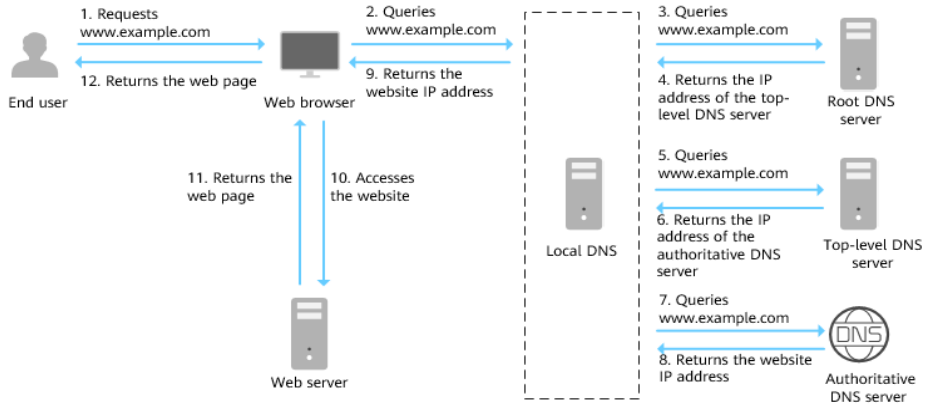
  For example, if you purchase example.com from a domain name registrar and set a DNS server for the domain name, the DNS server will provide authoritative resolution for example.com, and its address will be recorded by all top-level DNS servers.

  If you host domain names on the Huawei Cloud DNS service, authoritative DNS servers will be provided for the domain names.

Process of Domain Name Resolution

Figure 2-2 shows the process for accessing a website using the domain name www.example.com.

Figure 2-2 Domain name resolution



1. An end user enters **www.example.com** in the address box of a browser.
2. The DNS query for www.example.com is routed to the local DNS server.

   Local DNS servers are usually provided by the Internet service provider to cache domain name information and perform recursive lookup.
3. If the local DNS server does not find any records in the cache, it routes the request for www.example.com to the root DNS server.
4. The root DNS server returns the DNS server address of .com (because the domain name suffix is .com) to the local DNS server.
5. The local DNS server sends the request to the top-level DNS server of .com.
6. The top-level DNS server of .com returns the address of the authoritative DNS server which provides authoritative records for example.com.
7. The local DNS server sends the request to the authoritative DNS server of example.com.

   If you have hosted www.example.com on the DNS service and configured **Huawei Cloud DNS name servers**, these name servers will provide authoritative DNS for the domain name.
8. The authoritative DNS server returns the IP address mapped to www.example.com to the local DNS server.
9. The local DNS server returns the IP address to the web browser.
10. The web browser accesses the web server with the IP address.
11. The web server returns the web page to the browser.
12. The end user views the web page using the browser.

For details, see **Routing Internet Traffic to a Website**.

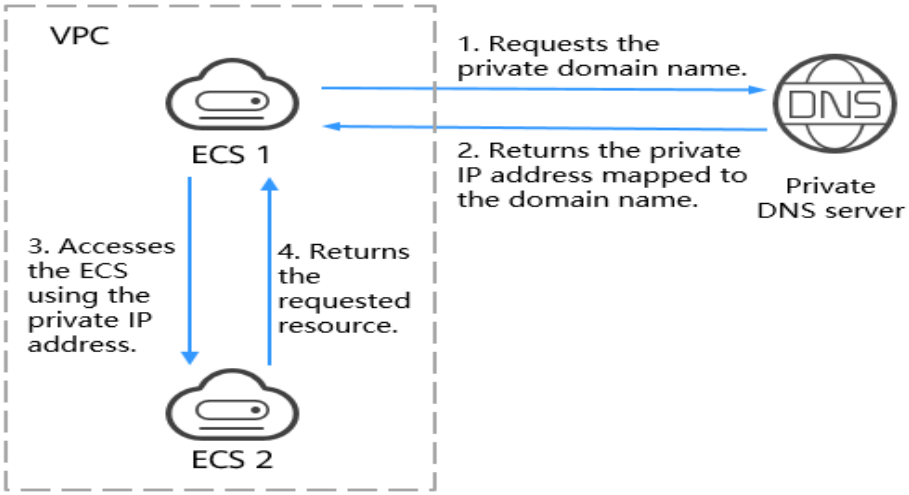
3 Private DNS Resolution

What Is Private DNS Resolution?

Private DNS resolution translates domain names like ecs.com and their subdomains used within one or more VPCs to private IP addresses (such as 192.168.1.1). With private DNS resolution, ECSs within a VPC can communicate with each other using private domain names and access cloud services, such as OBS and SMN, over a private network.

Figure 3-1 shows how a private domain name is resolved by a private DNS server.

Figure 3-1 Process for resolving a private domain name



When an ECS in the VPC requests to access a private domain name, the private DNS server directly returns a private IP address mapped to the domain name.

Private zones allow you to:

- Create custom private domain names in your VPCs.
- Associate one or more VPCs with a private zone.
- Use private domain names to access ECSs as well as OBS and SMN resources in the VPCs more quickly, preventing DNS spoofing.

You can use private domain names in the following scenarios:

- **Managing ECS Host Names**
- **Keeping Your Website Up and Running Even While Your Server Is Being Replaced**
- **Accessing Cloud Resources**

Managing ECS Host Names

You can plan host names based on the locations, usages, and account information of ECSs, and map the host names to private IP addresses, helping you manage ECSs more easily.

For example, if you have deployed 20 ECSs in an AZ, 10 for website A and 10 for website B, you can plan their host names (private domain names) as follows:

- ECSs for website A: weba01.region1.az1.com – weba10.region1.az1.com
- ECSs for website B: webb01.region1.az1.com – webb10.region1.az1.com

After you configure the host names, you will be able to quickly determine the locations and usages of ECSs during routine management and maintenance.

For detailed operations, see **Routing Traffic Within VPCs**.

Keeping Your Website Up and Running Even While Your Server Is Being Replaced

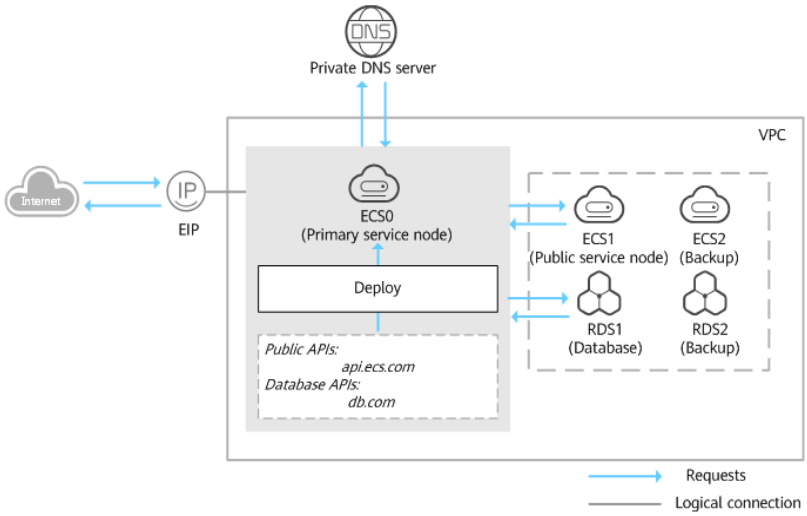
As the number of Internet users is continuously increasing, a website or web application deployed on a single server can hardly handle concurrent requests during peak hours. A common practice is to deploy the website or application on multiple servers and distribute the load across the servers.

These servers are in the same VPC and communicate with each other using private IP addresses that are coded into internal APIs called among the servers. If one of these servers is replaced, its private IP address changes. As a result, you need to change this IP address in the APIs and re-publish the website. This poses challenges for system maintenance.

If you create a private zone for each server and configure record sets to map their private domain names to the private IP addresses, they will be able to communicate using private domain names. When you replace any of the servers, you only need to change the private IP address in the record set, instead of modifying the code.

Figure 3-2 illustrates such use of private domain name resolution.

Figure 3-2 Configuring private DNS for cloud servers



The ECSs and RDS instances are in the same VPC.

- ECS0: primary service node
- ECS1: public service node
- RDS1: service database
- ECS2 and RDS2: backup service node and backup database

When ECS1 becomes faulty, ECS2 must take over. However, if no private zones are configured for the two ECSs, you need to change the private IP addresses in the code for ECS0. This will interrupt services, and you will need to publish the website again.

Now assume that you have configured private zones for the ECSs and have included their private names in the code. If ECS1 becomes faulty, you only need to change the DNS records to direct traffic to ECS2. Services are not interrupted, and you do not need to publish the website again.

For more details, see **Configuring a Private Domain Name for an ECS**.

Accessing Cloud Resources

Configure private domain names for ECSs so that they can access other cloud services, such as SMN and OBS, without connecting to the Internet.

When you create an ECS, note the following:

- If public DNS servers are configured for the VPC subnet where the ECS is running, requests to access cloud services will be routed over the Internet.

  Figure 3-3 shows the process for resolving a domain name when an ECS accesses Huawei cloud services such as OBS and SMN.

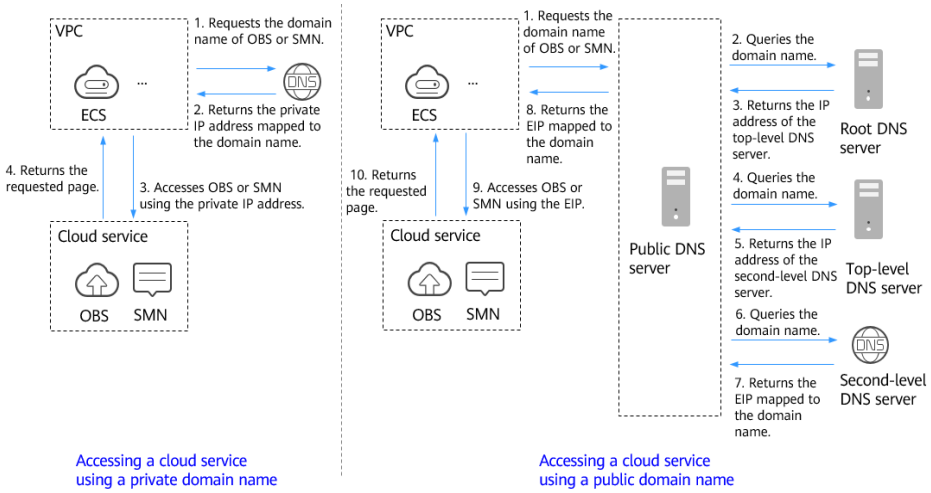
  Requests are routed over the Internet, resulting in high network latency and poor user experience.
- If a private DNS server is configured for the subnet, the private DNS server directly processes the requests to access cloud services.

  When the ECS accesses the Huawei cloud services, the private DNS server returns their private IP addresses, instead of routing requests over the

Internet. This reduces network latency and improves access speed. Steps 1 to 4 on the left of **Figure 3-3** shows the process.

To make your ECS accessible within the private network, change the default DNS servers of the ECS to private DNS servers, see **How Do I Change Default DNS Servers of an ECS to Private DNS Servers Provided by the DNS Service?**

Figure 3-3 Accessing cloud services



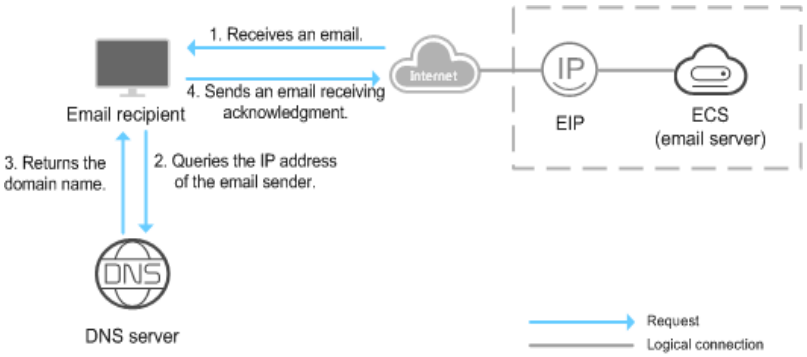
4 Reverse Resolution

Reverse resolution, also called reverse DNS lookup, resolves an IP address back to a host name. This is typically used to affirm the credibility of email servers.

After a recipient server receives an email, it checks whether the IP address and domain name of the sender server are trustworthy and determines whether the email is spam. If the recipient server cannot obtain the domain name mapped to the IP address of the sender server, it concludes that the email is sent by a malicious host and rejects it. It is necessary to configure pointer records (PTR) to point the IP addresses of your email servers to domain names.

In the following figure, an ECS serves as an email server, and a PTR record is configured to map the EIP of the ECS to the domain name configured for accessing the email server.

Figure 4-1 Reverse resolution



NOTE

Figure 4-1 shows only the process for reverse resolution. Information about how an email server checks the credibility of the sender's IP address and whether domain name is available on the Internet is not provided here.

If no PTR records are configured, the recipient server will treat emails from the email server as spam or malicious and discard them.

For detailed operations, see **Translating an IP Address to a Domain Name**.

5 Intelligent Resolution

If end users access a domain name, DNS servers return the same IP address to the end users regardless of their networks or geographic locations. However, in cross-network or cross-region access, this would lead to an increase in network latency and poor user experience.

With configurable resolution lines, you can specify different IP addresses for the same domain name based on visitors' carrier networks or geographic locations.

You can create more fine-grained resolution lines based on source IP addresses.

Huawei Cloud DNS supports the following types of routing policies:

- **ISP lines**
- **Region lines**
- **Custom lines**
- **Weighted routing**

NOTE

Intelligent resolution is not available for private zones and PTR records.

6 Notes and Constraints

Quotas

You can **log in to the console** to view the default quotas for each resource. To increase the quotas, you can **submit a service ticket**.

Table 6-1 DNS resource quotas

Resource Type	Default Quota	How to Increase
Public zone	50	**Submit a service ticket**.
Private zone	50	**Submit a service ticket**.
Record set	500	**Submit a service ticket**.
PTR record	50	**Submit a service ticket**.
Custom line	50	**Submit a service ticket**.

Specifications

Table 6-2 DNS specifications

Resource Type	Specifications	Description
Maximum number of IP addresses that can be bound to an endpoint	6	**Submit a service ticket** to increase the quota.
Maximum number of VPCs that can be associated with a private zone	No limit	-
Maximum number of VPCs that can be associated with an endpoint rule	No limit	-

Resource Type	Specifications	Description
Maximum number of requests for a single ECS in a VPC	2,000 per second	For a single ECS in a VPC, the maximum number of resolution requests is 2,000 per second. If the number of requests exceeds this, extra requests may not be handled. To avoid this, enable DNS caching to improve lookup efficiency.
Total number of requests for all ECSs in a VPC	No limit	-
Maximum number of recursive resolution requests for a single ECS in a VPC	600 per second	For a single ECS in a VPC, the maximum number of external recursive requests is 600 per second. If the number of requests exceeds this, extra requests may not be handled. If your services initiate an enormous volume of concurrent requests, enable DNS caching to improve lookup efficiency.
Total number of recursive requests for all ECSs in a VPC	5,000 per second	For all ECSs in a VPC, the maximum number of external recursive requests is 5,000 per second. If the number of requests exceeds this, extra requests may not be handled. If access to a large number of Internet domain names is required, some domain names may not be accessible due to traffic limiting. To avoid this, **submit a service ticket**.
Maximum number of recursive resolution requests for a single domain name in a VPC	50 requests per second	For a single domain name (for example, example.com) and its subdomains in a VPC, the maximum number of external recursive requests is 50 per second. If the number of requests exceeds this, extra requests may not be handled.

Resource Type	Specifications	Description
Bandwidth for handling requests to a public zone	5 Gbit/s	If your public domain name has abnormal requests evaluated by Huawei, such as attacks, and more than 5 Gbit/s of bandwidth is required for handling the requests, the domain name may be blocked. To address this issue, you should select an appropriate security protection product.

7 Permissions

If you need to assign different permissions to personnel in your enterprise to access your DNS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely access your resources.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, if you want some software developers in your enterprise to use DNS resources but do not want them to delete DNS resources or perform any other high-risk operations, you can create IAM users and grant permission to use DNS resources but not permission to delete them.

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

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

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

DNS Permissions

New IAM users do not have any permissions assigned by default. You need to first 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.

DNS resources include the following:

- Public zones: global-level resources
- Private zones: project-level resources
- PTR records: project-level resources

DNS permissions for global-level resources cannot be set in the global service project and must be granted for each project.

When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **eu-west-101**) in the specified regions (for example, **EU-Dublin**), the users only have permissions for DNS in the selected projects. If you set **Scope** to **All resources**, the users have permissions for DNS in all region-specific projects. When accessing DNS, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services depend on each other. When you grant permissions using roles, you also need to attach dependent roles. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only permissions to manage DNS resources of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by DNS, see **Permissions and Supported Actions**.

Table 7-1 lists all system-defined permissions supported by DNS.

Table 7-1 System-defined permissions for DNS

Role/Policy Name	Description	Type	Dependencies
DNS FullAccess	Full permissions for DNS	System-defined policy	None
DNS ReadOnlyAccess	Read-only permissions for DNS. Users granted with these permissions can only view DNS resources.	System-defined policy	None
DNS Administrator	Full permissions for DNS	System-defined role	**Tenant Guest** and **VPC Administrator**, which must be attached in the same project as the **DNS Administrator** role

Table 7-2 lists common operations supported by system-defined permissions for DNS.

Table 7-2 Common operations supported by system-defined permissions

Operation	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Creating a public zone	Supported	Not supported	Supported
Viewing a public zone	Supported	Supported	Supported

Operation	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Modifying a public zone	Supported	Not supported	Supported
Deleting a public zone	Supported	Not supported	Supported
Deleting public zones in batches	Supported	Not supported	Supported
Disabling or enabling a public zone	Supported	Not supported	Supported
Creating a private zone	Supported	Not supported	Supported
Viewing a private zone	Supported	Supported	Supported
Modifying a private zone	Supported	Not supported	Supported
Deleting a private zone	Supported	Not supported	Supported
Deleting private zones in batches	Supported	Not supported	Supported
Associating a VPC with a private zone	Supported	Not supported	Supported
Disassociating a VPC from a private zone	Supported	Not supported	Supported
Adding a record set	Supported	Not supported	Supported
Viewing a record set	Supported	Supported	Supported
Modify a record set	Supported	Not supported	Supported
Deleting a record set	Supported	Not supported	Supported
Delete record sets in batches	Supported	Not supported	Supported
Disabling or enabling a record set	Supported	Not supported	Supported
Exporting record sets in batches	Supported	Not supported	Supported
Importing record sets in batches	Supported	Not supported	Supported
Creating a PTR record	Supported	Not supported	Supported
Viewing a PTR record	Supported	Supported	Supported
Modifying a PTR record	Supported	Not supported	Supported
Deleting a PTR record	Supported	Not supported	Supported

Operation	DNS FullAccess	DNS ReadOnlyAccess	DNS Administrator
Deleting PTR records in batches	Supported	Not supported	Supported

Helpful Links

- What Is IAM?
- Creating a User and Granting DNS Permissions
- Permissions Policies and Supported Actions

8 Integration with Other Services

Figure 8-1 shows the relationships between DNS and other services.

Figure 8-1 Related services

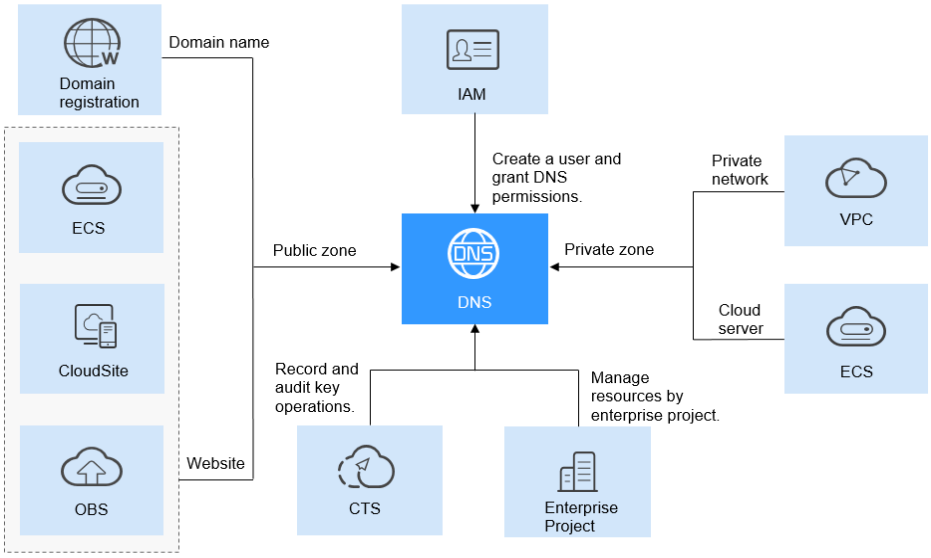


Table 8-1 shows the relationships between DNS and other services.

Table 8-1 DNS and other services

Related Service	Description	Reference
Elastic Cloud Server (ECS)	DNS can resolve the domain names to IP addresses of ECSs where a website or application is deployed so that end users can use domain name to access the website or application.	Routing Internet Traffic to a Website

Related Service	Description	Reference
Virtual Private Cloud (VPC)	DNS can resolve private domain names that are used for network connections within VPCs.	**Routing Traffic in a VPC**
Object Storage Service (OBS)	DNS maps your domain name to a bucket's access domain name for you to access the static websites hosted in the bucket.	**Static Website Hosting**
Cloud Trace Service (CTS)	CTS can record the operations performed on the DNS service.	**DNS Operations Recorded by CTS**
Enterprise Management	You can create different enterprise projects to manage public zones, private zones, and PTR records.	**Creating a Public Zone** **Creating a Private Zone** **Creating a PTR Record**

9 Product Concepts

9.1 Domain Name Format and DNS Hierarchy

A valid domain name meets the following requirements:

- A domain name is segmented using periods (.) into multiple labels.
- A domain name label can contain specified characters in different languages, letters, digits, and hyphens (-) and cannot start or end with a hyphen.
- A label cannot exceed 63 characters.
- The total length of a domain name, including the period at the end, cannot exceed 254 characters.

A domain name is divided into the following levels based on its structure:

- Root domain: . (a period)
- Top-level domain: for example, .com, .net, .org, and .cn
- Second-level domain: subdomains of the top-level domain names, such as example.com, example.net, and example.org
- Third-level domain: subdomains of the second-level domain names, such as abc.example.com, abc.example.net, and abc.example.org
- The next-level domain names are similarly expanded by adding prefixes to the previous-level domain names, such as def.abc.example.com, def.abc.example.net, and def.abc.example.org.

9.2 Record Set

Overview

A record set provides information about a domain name, including the IP addresses associated with and how to handle requests for the domain name and its subdomains.

If you have created a zone on the DNS console, you can add record sets to define how you want to route traffic for the domain name or its subdomains.

Table 9-1 describes the record set types and their application scenarios.

Table 9-1 Record set usages

Record Set Type	Where to Use	Description
A	Public and private zones	Maps domains to IPv4 addresses.
CNAME	Public and private zones	Maps one domain name to another domain name or multiple domain names to one domain name.
Mail exchanger (MX)	Public and private zones	Maps domain names to email servers.
AAAA	Public and private zones	Maps domain names to IPv6 addresses.
Text (TXT)	Public and private zones	TXT record sets are usually used to record the following: • DKIM public keys to prevent email fraud • To record the identity of domain name owners to facilitate domain name retrieval.
Service (SRV)	Public and private zones	Records servers providing specific services.
Nameserver (NS)	Public and private zones	Delegates subdomains to other name servers. • For public zones, an NS record set is automatically created, and you can add NS record sets for subdomains. • For private zones, an NS record set is automatically created, and you cannot add other NS record sets.
Start of authority (SOA)	Public and private zones	Identifies the base information about a domain name. The SOA record set is automatically generated by the DNS service and cannot be added manually.
Certification Authority Authorization (CAA)	Public zone	Grants certificate issuing permissions to CAs. CAA record sets can prevent the issuance of unauthorized HTTPS certificates.
Pointer (PTR)	Public and private zones	Maps IP addresses to domain names.

Usage

Record sets are used in following scenarios:

- Routing Internet traffic to a website

  A and AAAA record sets are usually used to map domain names used by websites to IPv4 or IPv6 addresses of web servers where the websites are deployed.

  Figure 9-1 Accessing a website over the Internet using domain name

- Private domain name resolution

  On a private network, A and AAAA record sets translate private domain names into private IP addresses.

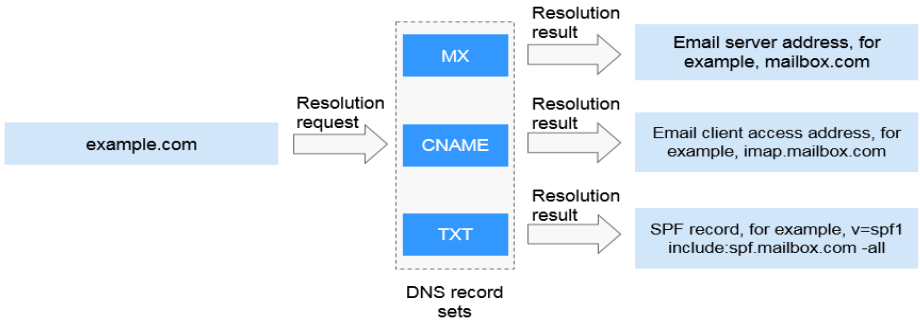
  Figure 9-2 Private domain name resolution

- Email domain name resolution

  MX, CNAME, and TXT record sets are usually used for email services.

  Figure 9-3 Email domain name resolution

- Reverse resolution on a private network

  PTR records translate private IP addresses into private domain names.

  Figure 9-4 Reverse resolution on a private network

Helpful Links

For details about how to add and manage record sets, see **Record Set**.

9.3 Project

Projects are used to group and isolate cloud resources, including computing, storage, and network resources. Multiple projects can be created for one account. A project can be a department or a project team.

Public zones are global-level resources, while private zones and PTR records are resources at the region level. Private zones and PTR records are isolated and managed based on projects. You need to create, query, and configure private zones or PTR records in specific regions and projects.

9.4 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.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

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.

