

Private DNS

Product Introduction

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Product Introduction

Overview

Strengths

Use Limits

Use Cases

Product Introduction

Overview

Last updated : 2024-07-04 15:31:04

Overview

Private DNS is a private DNS management service based on Tencent Cloud Virtual Private Cloud (VPC). It allows you to quickly build a DNS system in one or more VPCs and easily use private domain name records to manage Tencent Cloud resources (such as CVM, CLB, CDN, and COS) associated with the VPCs. These private domain names are inaccessible beyond the VPC.

Features

Private Domain Management

Private DNS

The private domain list contains the private domain name resource records that you need to manage. You can create multiple private domain names and add the following types of DNS records for them:

Record Type	Description
A	It is used to specify the IPv4 address (such as <code>8.8.8.8</code>) of a domain. If you want to point a domain to an IP address, you need to add an A record.
AAAA	It is used to specify the IPv6 address (such as <code>ff06:0:0:0:0:0:0:c3</code>) of a domain. If you want to point a domain to an IPv6 address, you need to add an AAAA record.
CNAME	Alias record, used to point a domain to another domain.
MX	If you want to set up a mailbox so that it can receive emails, you need to add an MX record.
TXT	You can enter anything in this record with a length limit of 255 characters. Most TXT records are used as SPF records (for anti-spam).
PTR	It reversely maps an IP address to a domain.

Associated VPCs

You can associate a private domain name with one or more VPCs that need to be configured so as to map it to IP addresses.

Note:

Private domain names with the same name cannot be associated with the same VPC. For example, if there are two instances of `tencent.com` at the same time, you cannot associate both of them with the same VPC.

Reverse DNS

Reverse DNS refers to mapping an IP address to a domain name, that is, the private domain name pointed to by the IP address is obtained by querying the PTR record of the IP address.

Subdomain Recursive DNS

With the aid of Private DNS, you can implement private network hijacking in VPCs without relying on the authoritative DNS. In certain scenarios, some domain names need to be opened to access public IPs in private environments. Private DNS can achieve dual DNS for one single domain name by working with the authoritative DNS and thus achieve interconnection in hybrid clouds, that is, you can use `nslookup` in CMD to resolve the same domain name and get different IP addresses.

Custom Private Domain

CVM instance name management can be well planned to make the instance purposes and information easier to understand and more user-friendly.

Internal Domain Name Security Isolation

The core system privacy protection feature ensures that the domain names of internal core systems are not exposed to the internet and thus improves their security.

Recursive Resolution

The recursive resolution capability of the Private DNS private domain resolution service primarily provides public network domain name recursive resolution services for various terminals (such as CVMs and Lighthouse) in the enterprise intranet VPC environment. This service is the default free service provided for Tencent Cloud VPC intranet resolution scenarios, but it does not guarantee service SLA. If you don't use Tencent Cloud's default DNS servers 183.60.83.19 and 183.60.82.98, you will be unable to use the Private DNS service.

Note:

Private DNS Service Product Rules **Effective only for requests initiated by DNS server addresses in the enterprise intranet VPC configured as 183.60.83.19 / 183.60.82.98** (If the DNS settings of the CVM endpoints are changed to other IP addresses, the product rules of Tencent DNS intranet resolution service will not be effective on that CVM).

Strengths

Last updated : 2022-01-28 12:11:12

Security and Reliability

- Private DNS is a Tencent Cloud strategic product based on DNSPod's 14 years of DNS technology accumulation and provides more professional private domain name DNS capabilities.
- It provides Tencent Cloud VPC-dedicated private network DNS to directly respond to VPC domain name DNS requests, which is fast, efficient, and effective in preventing hijacking.

Wide Applicability

The core network infrastructure component of Private DNS in VPC scenarios helps you easily deploy integrated VPC solutions.

Ease of Use

You can customize IP mappings for private domain names and quickly tag them for easier OPS management.

Flexibility and Elasticity

You can create custom public networks and register private domain names that comply with the IANA specifications, which makes the configuration of private domain names more flexible and elastic.

Unified Management

One private domain name can be associated with multiple VPCs to facilitate unified management and deployment.

Comprehensive Records

6 types of records are supported: A, CNAME, MX, AAAA, TXT, and PTR, covering multiple application scenarios of DNS.

Reverse DNS

You can set reverse DNS by creating a fixed private domain ending with `in-addr.arpa` and adding a PTR record.

Subdomain Recursive DNS

After subdomain recursive DNS is enabled, subdomains that have no DNS records configured will be automatically forwarded to the public authoritative DNS for resolution.

Use Limits

Last updated : 2024-07-04 15:29:28

Private DNS Use Limits

Currently, use of Private DNS has the following limits and restrictions:

Note:

Finance regions are only visible to group cloud users and financial users.

If you don't use Tencent Cloud's default DNS servers `183.60.83.19` and `183.60.82.98`, you will be unable to use the Private DNS service. If you need to modify the DNS server, see [Getting Private IP Addresses and Setting DNS](#).

For more scenario requirements, provide your feedback via your rep or [submit a ticket](#).

Item	Limit	Description
Number of DNS records	100,000	Up to 100,000 DNS records can be added under each UIN account.
Number of domains	500	Up to 500 private domains can be created under each UIN account.
TTL	1 - 86400s	TTL is the retention time of a DNS record on the DNS server and can be customized. There is a cache TTL mechanism for DNS queries. The DNS queries in Private DNS are counted based on the actual origin-pull requests and billed. You need to set the local NSCD cache to reduce origin pulls.
Available regions	Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, Wuhan, Jinan, Shijiazhuang, Nanjing, Hefei, Shenyang, Changsha, Zhengzhou, Xi'an, Fuzhou, Hangzhou, Hong Kong (China), Silicon Valley, Singapore, Frankfurt, Jakarta, Bangkok, Mumbai, Virginia, Tokyo, Seoul, Toronto, Beijing Finance, Shanghai Finance, and Shenzhen Finance	An available region is a VPC region that can be associated with a private domain.
Private domain creation	The system supports creating TLDs conforming to IANA by default. To	Reference: Root Zone Database .

	create custom TLDs, purchase Value-Added Service – Non-Standard TLDs first.	
Total resolution requests per instance within the VPC	5,000 times/second	<p>The maximum DNS request threshold per instance within the VPC is 5,000 times/sec (including private domain resolution and external recursive resolution). If the DNS query peak per second exceeds the threshold, a risk of speed limit will be there, and the availability SLA (99.99%) of the paid version for private domain resolution cannot be guaranteed.</p> <p>Note: This instance includes both CVM and Lighthouse.</p>
Number of External Recursive Resolution Requests per Instance within VPC	100 times/second	<p>The threshold for external recursive resolution requests per instance within the VPC is 100 times/second. If the speed limit threshold is exceeded, a risk of speed limit will be there.</p> <p>Note: This instance includes both CVM and Lighthouse.</p>
Total external recursive resolution requests for all instances within the VPC	1,000 times/second	<p>The overall external recursive request threshold within a single VPC is 1,000 times/second. If the speed limit threshold is exceeded, a risk of speed limit will be there.</p>
Volume of External Recursive Resolution Requests for a Single Domain within the VPC	30 times/second	<p>The external recursive resolution request threshold for a single domain (such as example.com) within a single VPC is 30 times/second. If the speed limit threshold is exceeded, a risk of speed limit will be there.</p>
DNS request protocol	-	<p>The DNS request protocol through private domain resolution within the VPC supports the UDP Protocol, and each request packet must be less than 512 bytes.</p> <p>Note: This instance includes both CVM and Lighthouse.</p>

Recursive subdomain resolution	-	After the Recursive Subdomain Resolution feature of Private DNS is enabled, queries for a subdomain for which no records are set will be forwarded to the public DNS. If this feature is not enabled, such queries cannot be properly resolved.
CNAME flattening	-	If you have set a CNAME record, the target IP of the CNAME record will be synchronously returned after the CNAME flattening feature is enabled. We recommend you enable the Recursive Subdomain Resolution feature before using this feature. Otherwise, no final result can be returned if the target IP of the CNAME record requires query in the public DNS.

Round-Robin DNS Record Limits

Note:

Number of "Round-Robin DNS Records" refers to the number of records that can be added under the same host and the same record type.

Those out of the limit cannot be properly added. To add the number of round-robin DNS records, purchase [Value-Added Service Packages](#) first.

Record Type	Number of "Round-Robin DNS Records"	Remarks
A	10	-
AAAA	10	-
TXT	20	Weight setting is unavailable for round-robin DNS of TXT records.
CNAME	5	-
MX	50	-
PTR	The PTR record does not support round-robin DNS.	-

Use Cases

Last updated : 2022-01-28 12:11:12

This document describes the common use cases of Private DNS.

Private Network Access Hijacking

You can use Private DNS to create a private domain name, associate it with a VPC, add a DNS record for it, and set resource mapping to implement the private network hijacking feature. Then, when you access the private domain in the VPC, the mapped resource that you set in advance will be returned.

Tencent Cloud Service Resource Management

You can use private DNS records to manage Tencent Cloud resources such as CVM, CLB, CDN, and COS in VPCs. For example, you can plan the hosts of CVM instances according to the region, business scenario, server information, etc. and use the host information to add private domain names and DNS records for such instances. These private domain names are inaccessible outside the VPCs, which makes it easier for you to manage CVM resources.

Mutual Access Between Tencent Cloud Service Resources

You can connect VPCs with traditional IDCs through Direct Connect or VPN so that they can access each other's resources at private domain names, facilitating the intuitive use of Tencent Cloud service resources.

Tencent Cloud Service Resource Switching

Generally, in order to ensure the stable operation of a high-concurrency business, the business is distributed on multiple CVM instances for them to share the pressure, and the same VPC can be established for such instances to enable mutual access between them at private IPs. However, when an instance is switched, its private IP will also change accordingly. Therefore, it is necessary to modify the business code and release the change, which is extremely inconvenient.

In this case, you can create a private domain name for each instance in your VPC through Private DNS and add DNS records pointing to the corresponding private IPs. The instances can access each other at the private domain names, and when an instance is switched, you do not need to modify the code. Instead, you can simply modify the DNS record of its domain name.