ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Apsara Stack DNS

User Guide

Product Version: v3.16.2

Document Version: 20220916

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is Apsara Stack DNS?

Apsara Stack DNS is a service that runs on Apsara Stack to resolve domain names. You can configure rules to map domain names to IP addresses. Then, Apsara Stack DNS distributes domain name requests from clients to cloud resources, business systems on your internal networks, or the business resources of Internet service providers (ISPs).

Apsara Stack DNS provides DNS resolution in virtual private clouds (VPCs). You can perform the following operations in your VPC by using Apsara Stack DNS:

- Access other ECS instances deployed in your VPC.
- Access cloud service instances provided by Apsara Stack.
- Access custom enterprise business systems.
- Access Internet services and businesses.
- Establish network connections between DNS and user-created DNS over a leased line.
- Manage internal domain names.
- Manage DNS records of internal domain names.
- Manage forwarding configurations.
- Manage recursive resolution configurations.

2.User roles and permissions

Role	Permission
System administrator	A user of this role has read, write, and execute permissions on all level-1 organization resources, global resources, and system configurations.
Level-1 organization administrator	A user of this role has read, write, and execute permissions on level-1 organization resources to which the user belongs, but does not have permissions on level-1 organization resources, global resources, or system configurations to which other users belong.
Lower-level organization administrator	A user of this role does not have permissions on Apsara Stack DNS. The user does not have permissions on level-1 organization resources to which the user belongs, and does not have permissions on level-1 organization resources, global resources, or system configurations to which other users belong.
Resource user	A user of this role does not have permissions on Apsara Stack DNS. The user does not have permissions on level-1 organization resources to which the user belongs, and does not have permissions on level-1 organization resources, global resources, or system configurations to which other users belong.
Other roles	A user of this role does not have permissions on Apsara Stack DNS. The user does not have permissions on level-1 organization resources to which the user belongs, and does not have permissions on level-1 organization resources, global resources, or system configurations to which other users belong.

3.Log on to the Apsara Stack DNS console

This topic describes how to log on to the Apsara Stack DNS console by using Google Chrome.

Prerequisites

- Before you log on to the Apsara Uni-manager Management Console, the endpoint of the console is obtained from the deployment staff.
- We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press the Enter key.
2. Enter your username and password.

   Obtain the username and password that you use to log on to the Apsara Uni-manager Management Console from the operations administrator.

   > **Note** The first time that you log on to the Apsara Uni-manager Management Console, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters
   > - Digits
   > - Special characters, including exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%)

3. Click **Log On**.
4. If multi-factor authentication (MFA) is enabled for your account, perform the corresponding operations in the following scenarios:
   - You log on to the Apsara Uni-manager Management Console for the first time after MFA is enabled by the administrator.
     a. On the Bind Virtual MFA Device page, bind an MFA device.
     b. Enter the username and password again as in Step 2 and click **Log On**.
     c. Enter a six-digit MFA verification code and click **Authenticate**.
   - You have enabled MFA and bound an MFA device.

     Enter a six-digit MFA verification code and click **Authenticate**.

     > **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Management Console User Guide*.

5. In the top navigation bar, choose **Products > Networking > DNS within Cloud**.

4.Global internal domain names in Apsara Stack

Apsara Stack DNS allows you to manage global internal domain names, global forwarding configurations, and global recursive resolution configurations on the Global Domain Names page.

4.1. Global internal domain names

4.1.1. Overview

All the operations of this feature require administrator privileges.

4.1.2. View a global internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, enter a keyword of the domain name that you want to view in the search box next to **Add Domain Name**.
4. Click **Search**.

   In the search result that is returned, find and view the required domain name.

4.1.3. Create a global internal domain name

This topic describes how to create a global internal domain name in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, click **Add Domain Name**.
4. In the Add Global Internal Domain Name dialog box, enter the domain name that you want to create in the **Global Internal Domain Name** field and specify a domain name type.
5. Click **OK**.

4.1.4. Add a description for a global internal domain name

This topic describes how to add a description for a global internal domain name in the Apsara Uni-manager Management Console.

Context

You can add a description for a domain name to help you identify the domain name. For example, you can specify a hostname or internal system information to describe a domain name.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, find the domain name for which you want to add a description and click **Add Description** in the Actions column.
4. In the Add Description dialog box, enter a description in the Add Description field.
5. Click **OK**.

4.1.5. Delete a global internal domain name

This topic describes how to delete a global internal domain name in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, find the domain name that you want to delete and click **Delete** in the **Actions** column.
4. In the message that appears, click **Delete**.

4.1.6. Delete multiple global internal domain names at a time

This topic describes how to delete multiple global internal domain names at a time in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, select one or more domain names that you want to delete and click **Batch Delete** in the lower-left corner.
4. In the message that appears, click **Delete**.

4.1.7. Configure DNS records for a global internal domain name

This topic describes how to configure DNS records for a global internal domain name in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane.
3. On the Global Internet Domain Name tab, find the domain name for which you want to configure DNS records and click **Configure DNS Records** in the Actions column.
4. On the **DNS Settings** page, click **Add DNS Record** in the upper-right corner.

4.2. Global forwarding configurations

4.2.1. Global forwarding domain names

4.2.1.1. Overview

All operations on global forwarding domain names require system administrator permissions.

Apsara Stack DNS forwards specific domain names to other DNS servers for resolution.

Apsara Stack DNS can forward requests with or without recursion.

- In the mode of forwarding without recursion, only the specified DNS server is used to resolve domain names. If the resolution fails or times out, a message is returned to the DNS client to indicate that the current request fails.
- In the mode of forwarding with recursion, the specified DNS server is preferentially used to resolve domain names. If the resolution fails, the local DNS server is used.

4.2.1.2. View a global forwarding domain name

This topic describes how to view a global forwarding domain name in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, enter a keyword of the domain name that you want to view in the search box next to **Add Domain Name** and click **Search**.

4.2.1.3. Create a global forwarding domain name

This topic describes how to create a global forwarding domain name in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.

2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, click **Add Domain Name**.
4. In the Add Global Forwarding Domain Name dialog box, set the required parameters, including *Global Forwarding Domain Name*, *Forwarding Mode*, and *Destination IP Address*, and click **OK**.

4.2.1.4. Add a description for a global forwarding domain name

This topic describes how to add a description for a global forwarding domain name in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Context

You can add a description for a domain name to help you identify the domain name. For example, you can specify a hostname or internal system information to describe a domain name.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, find the domain name for which you want to add a description and click **Add Description** in the Actions column.
4. In the Add Description dialog box, enter a description in the Add Description field, and click **OK**.

4.2.1.5. Modify the configurations of a global forwarding domain name

This topic describes how to modify the configurations of a global forwarding domain name in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, find the domain name whose configurations you want to modify and click **Modify** in the Actions column.
4. In the dialog box that appears, modify the *Global Forwarding Domain Name, Forwarding Mode, and Destination IP Address* parameters based on your business requirements and click **OK**.

4.2.1.6. Delete a global forwarding domain name

This topic describes how to delete a global forwarding domain name in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, find the domain name that you want to delete and click **Delete** in the Actions column.
4. In the message that appears, click **Delete**.

4.2.1.7. Delete multiple global forwarding domain names at a time

This topic describes how to delete multiple global forwarding domain names at a time in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab.
3. On the Global Forwarding Domain Names subtab, select one or more domain names that you want to delete and click **Batch Delete** in the lower-left corner.
4. In the message that appears, click **Delete**.

4.2.2. Global default forwarding configurations

4.2.2.1. Enable default forwarding

This topic describes how to enable default forwarding in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab. Then, click the Global Default Forwarding Configurations subtab.
3. Turn on Default Forwarding.
4. Set the **Default Forwarding Mode** and **Destination IP Address** parameters and click **Save**.

   You must make sure that the Default Forwarding switch is turned on.

4.2.2.2. Modify default forwarding configurations

This topic describes how to modify default forwarding configurations in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab. Then, click the Global Default Forwarding Configurations subtab.
3. Modify the *Default Forwarding Mode* and *Destination IP Address* parameters and click **Save**.

4.2.2.3. Disable default forwarding

This topic describes how to disable default forwarding in the Apsara Uni-manager Management Console. This operation requires system administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **DNS within Cloud > Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Forwarding Configurations** tab. Then, click the Global Default Forwarding Configurations subtab.
3. Turn off Default Forwarding.
4. Click **Save**.

4.3. Global recursive resolution

4.3.1. Enable global recursive resolution

Prerequisites

System administrator permissions are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose DNS within Cloud > **Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Recursive Resolution** tab. Then, click the Global Default Recursion subtab.
3. Turn on **Global Recursive Resolution**.
4. Click **Save**.

4.3.2. Disable global recursive resolution

Prerequisites

System administrator permissions are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose DNS within Cloud > **Global Domain Name within Cloud** in the left-side navigation pane. On the Global Domain Names page, click the **Global Recursive Resolution** tab. Then, click the

Global Default Recursion subtab.

3. Turn off **Global Recursive Resolution**.
4. Click **Save**.

5.Private domain names for VPCs

Apsara Stack DNS allows you to create VPC-specific tenant internal domain names. You can associate the domain names with VPCs based on your business requirements to achieve tenant isolation.

5.1. Tenant internal domain name

5.1.1. View a tenant internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab of the Private Domain Names for VPC page. Enter a keyword of the domain name that you want to view in the field next to **Add Domain Name**.
4. Click Search.

   In the **search result** that is returned, find and view the required domain name.

5.1.2. Create a tenant internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab of the Private Domain Names for VPC page, click **Add Domain Name**.
4. In the Add Tenant Internal Domain Name dialog box, set the required parameters such as *Tenant Internal Domain Name*.
5. Click **OK**.

5.1.3. Configure DNS records for a tenant internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. Find the domain name for which you want to configure DNS records and click **Configure DNS Records** in the Actions column.
4. On the **DNS Settings** page, click **Add DNS Record** in the upper-left corner.
5. In the **Add DNS Record** dialog box, set the parameters including *Record Name*, *Record Type*, TTL (Seconds), Load Balancing Policy, Resolution Line, and *Record Values*. Then, click **OK**.

The following tables describe the settings of the Load Balancing Policy parameter that correspond to different types of DNS records.

- A record

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique IPv4 addresses. Each address must be in a separate row. Make sure that the IPv4 addresses are valid. Examples: ■ 192.168.1.1 ■ 192.168.1.2 ■ 192.168.1.3
Weight	You can specify up to 100 unique IPv4 addresses. Each address must be in a separate row. Requirements: ■ Use the format of [IPv4 address] [Weight] to specify each IPv4 address. Separate the IPv4 address and weight with a space. ■ Make sure that the IPv4 address is valid. ■ The weight value must be an integer ranging from 0 to 999. A larger value indicates a greater weight. Examples: ■ 192.168.1.1 20 ■ 192.168.1.1 30 ■ 192.168.1.1 50

- AAAA record

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique IPv6 addresses. Each address must be in a separate row. Make sure that the IPv6 addresses are valid. Examples: ■ 2400:3200::6666 ■ 2400:3200::6688 ■ 2400:3200::8888

Load Balancing Policy	Description
Weight	You can specify up to 100 unique IPv6 addresses. Each address must be in a separate row. Requirements: ■ Use the format of [IPv6 address] [Weight] to specify each IPv6 address. Separate the IPv6 address and weight with a space. ■ Make sure that the IPv6 address is valid. ■ The weight value must be an integer ranging from 0 to 999. A larger value indicates a greater weight. Examples: ■ 2400:3200::6666 20 ■ 2400:3200::6688 20 ■ 2400:3200::8888 60

- CNAME record

Load Balancing Policy	Description
Round-robin Scheduling	You can enter only one domain name. The domain name must be a fully qualified domain name (FQDN) that ends with a period (.). The domain name can be up to 255 characters in length. Example: www.example.com.
Weight	You can specify up to 100 unique domain names. Each domain name must be in a separate row. Requirements: ■ Use the format of [Domain name] [Weight] to specify each domain name. Separate the domain name and weight with a space. ■ The domain name must be an FQDN that ends with a period (.) and can be up to 255 characters in length. ■ The weight value must be an integer ranging from 0 to 999. A larger value indicates a greater weight. Examples: ■ www1.example.com. 20 ■ www2.example.com. 20 ■ www3.example.com. 60

- MX record

Load Balancing Policy	Description

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique email server hostnames. Each hostname must be in a separate row. Requirements: ■ Use the format of [Priority] [Email server hostname] to specify each hostname. Separate the priority and hostname with a space. ■ The priority value must be an integer ranging from 0 to 999. A smaller value indicates a higher priority. ■ The email server hostname must be an FQDN that ends with a period (.) and can be up to 255 characters in length. Examples: ■ 10 mailserver1.example.com. ■ 20 mailserver2.example.com.

- TXT record

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique character strings. Each string must be in a separate row. A string must be 1 to 255 characters in length. No row can be left empty. Example: "v=spf1 ip4:192.168.0.1/16 ip6:2001::1/96 ~all"

- PTR record

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique domain names. Each domain name must be in a separate row. Each domain name must be an FQDN that ends with a period (.) and can be up to 255 characters in length. Examples: ■ www1.example.com. ■ www2.example.com. ■ www3.example.com.

- SRV record

Load Balancing Policy	Formatting rule

Load Balancing Policy	Formatting rule
Round-robin Scheduling	You can specify up to 100 unique application server hostnames. Each hostname must be in a separate row. Requirements: ■ Use the format of [Priority] [Weight] [Port number] [Application server hostname] to specify each hostname. Separate every two consecutive items with a space. ■ The priority value must be an integer ranging from 0 to 999. A smaller value indicates a higher priority. ■ The weight value must be an integer ranging from 0 to 999. A larger value indicates a greater weight. ■ The port number must be an integer ranging from 0 to 65535. The value indicates the TCP or UDP port used for network communications. ■ The application server hostname must be an FQDN that ends with a period (.) and can be up to 255 characters in length. Examples: ■ 1 10 8080 www1.example.com. ■ 2 20 8081 www2.example.com.

- NAPTR record

Load Balancing Policy	Description

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique NAPTR records. Each record must be in a separate row. Requirements: ■ Use the format of [Serial number] [Priority] [Flag] [Service information] [Regular expression] [Substitute domain name] to specify each record. Separate every two consecutive items with a space. ■ The serial number must be an integer ranging from 0 to 999. A smaller value indicates a higher priority. ■ The priority value must be an integer ranging from 0 to 999. A smaller value indicates a higher priority. If two records have the same serial number, the one with a higher priority takes effect first. ■ The flag value can be left empty or be a character from A to Z, a to z, or 0 to 9. The flag value is not case-sensitive and must be enclosed in double quotation marks (""). ■ The service information can be left empty or be a string of 1 to 32 characters. The value must start with a letter and be enclosed in double quotation marks (""). ■ The regular expression can be left empty or be a string of 1 to 255 characters enclosed in double quotation marks (""). ■ The substitute domain name must be an FQDN that ends with a period (.) and can be up to 255 characters in length. Examples: ■ 100 50 "S" "Z3950+I2L+I2C" "" _z3950._tcp.example.com. ■ 100 50 "S" "RCDS+I2C" "" _rcds._udp.example.com. ■ 100 50 "S" "HTTP+I2L+I2C+I2R" "" _http._tcp.example.com.

- CAA record

Load Balancing Policy	Description

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique CAA records. Each record must be in a separate row. Requirements: ■ Use the format of [Certificate authority flag] [Certificate property tag] [Authorization information] to specify each record. Separate every two consecutive items with a space. ■ The certification authority flag must be an integer ranging from 0 to 255. ■ The certificate property tag can be issue, issuewild, or iodef. ■ The authorization information must be 1 to 255 characters in length and enclosed in double quotation marks (""). Examples: ■ 0 issue "caa.example.com" ■ 0 issuewild ";" ■ 0 iodef "mailto:example@example.com"

- NS record

Load Balancing Policy	Description
Round-robin Scheduling	You can specify up to 100 unique DNS server addresses. Each address must be in a separate row. Each DNS server address must be an FQDN that ends with a period (.) and can be up to 255 characters in length. It cannot be a wildcard domain name. Examples: ■ ns1.example.com. ■ ns2.example.com.

6. After you add DNS records, perform the following operations on the DNS Settings page based on your business requirements.
   - Add a description for a DNS record

     Find the DNS record for which you want to add a description and click **Add Description** in the Actions column. In the dialog box that appears, enter a description in the Add Description and click **OK**.
   - Delete a DNS record

     Find the DNS record that you want to delete and click **Delete** in the Actions column. In the message that appears, click **Delete**.
   - Modify a DNS record

     Find the DNS record that you want to modify and click **Modify** in the Actions column. In the Modify DNS Record dialog box, modify the parameters based on your business requirements and click **OK**.

- Delete multiple DNS records at a time

  Select the DNS records that you want to delete at a time and click **Batch Delete** in the lower-left corner of the page. In the message that appears, click **Delete**.

5.1.4. Associate a tenant internal domain name with a VPC

Tenant internal domain names are isolated based on VPCs. To ensure that the DNS forwarding configurations take effect, you must associate a tenant internal domain name with a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, find the domain name with which you want to associate a VPC and click **Associate VPC** in the Actions column.
4. In the Associate VPC dialog box, select a **region** from the Region drop-down list, select a VPC that you want to associate with the domain name from the **Associate VPC** drop-down list, and then click **OK**.

5.1.5. Disassociate a tenant internal domain name from a VPC

This topic describes how to disassociate a tenant internal domain name from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, find the domain name that you want to disassociate from a VPC and click the number in the **Associated VPCs** column.
4. On the **VPCs** page, find the VPC from which you want to disassociate the domain name and click **Disassociate** in the **Actions** column.

   The VPC from which you dissociate the domain name is no longer displayed on the VPCs page.

5.1.6. Add a description for a tenant internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, find the domain name for which you want to add a description and click **Add Description** in the Actions column.

4. In the Add Description dialog box, enter a description in the Add Description field.
5. Click **OK**.

5.1.7. Delete a tenant internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, find the domain name that you want to delete and click **Delete** in the Actions column.
4. In the message that appears, click **Delete**.

5.1.8. Delete multiple tenant internal domain names at a time

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, select one or more domain names that you want to delete and click **Batch Delete** in the lower-left corner of the tab.
4. In the message that appears, click **Delete**.

5.1.9. View the load balancing policy configured for a tenant internal domain name

This topic describes how to view the load balancing policy that you configure for a tenant internal domain name.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane.
3. On the Tenant Internal Domain Name tab, find the domain name whose load balancing policy settings you want to view and click **Configure DNS Records** in the Actions column.
4. On the DNS Settings page, view the load balancing policy that you configure for the domain name.

5.2. Tenant forwarding configurations

5.2.1. Tenant forwarding domain names

5.2.1.1. View a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab.
3. On the **Tenant Forwarding Domain Names** subtab, enter a keyword of the domain name that you want to view in the field next to Add Domain Name.
4. Click **Search**.

   In the search result that is returned, find and view the required domain name.

5.2.1.2. Create a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Private DNS > Private Domain Name for VPC** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, click **Add Domain Name**.
4. In the Add Tenant Forwarding Domain Name dialog box, set the required parameters, including Organization, Resource Set, *Tenant Forwarding Domain Name*, *Forwarding Mode*, and *Destination IP Address*. The following table describes some of the parameters.

Parameter	Description
Tenant Forwarding Domain Name	The *tenant forwarding domain name* that you want to create. Take note of the following rules: ◦ The domain name must be 1 to 254 characters in length. This includes the period (.) at the end. ◦ The domain name can contain multiple domain name segments that are separated by periods (.). A domain name segment must be 1 to 63 characters in length. The domain name cannot contain consecutive periods (.). ◦ The domain name can contain only letters, digits, hyphens (-), and underscores (_). ◦ ◦ The domain name is not case-sensitive. ◦ The domain name must end with a period (.).

Parameter	Description
Forwarding Mode	The forwarding mode of the domain name. For both domain name-based forwarding and default forwarding, the following two forwarding modes are supported: ○ Forward All Mode: forwards DNS requests to the destination DNS server. If the destination DNS server cannot resolve a domain name, a message is returned to the DNS client indicating that the request failed. ○ Forward First Mode: A specified DNS server is preferentially used to resolve domain names. If the specified DNS server cannot resolve a domain name, the local DNS is used. If you enter internal IP addresses in the Destination IP Address field, unexpected results may occur during recursive resolution. For example, a domain name used for internal network services may be resolved to a public IP address.
Destination IP Address	The destination IP addresses. **Note** You can specify up to five unique IPv4 or IPv6 addresses. Each address must be in a separate row.

5. Click **OK**.

5.2.1.3. Associate a tenant forwarding domain name with a VPC

Tenant forwarding domain names are isolated based on VPCs. To ensure that the DNS forwarding configurations take effect, you must associate a tenant forwarding domain name with a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, find the domain name with which you want to associate a VPC and click **Associate VPC** in the Actions column.
4. Select one or more VPCs from the Associate VPC drop-down list and click **OK**.

5.2.1.3.1. Modify the forwarding configurations of a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.

3. On the Tenant Forwarding Domain Names subtab, find the domain name for which you want to modify the forwarding configurations and click Modify in the Actions column.
4. In the dialog box that appears, modify the **Forwarding Mode** or **Destination IP Address** parameter based on your business requirements.
5. Click **OK**.

5.2.1.4. Disassociate a tenant forwarding domain name from a VPC

This topic describes how to disassociate a tenant forwarding domain name from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, find the domain name that you want to disassociate from a VPC and click the number in the **Associated VPCs** column.
4. On the VPCs page, find the VPC from which you want to disassociate the domain name and click **Disassociate** in the Actions column.

   The VPC from which you dissociate the domain name is no longer displayed on the VPCs page.

5.2.1.5. Add a description for a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, find the domain name for which you want to add a description and click Add Description in the Actions column.
4. In the Add Description dialog box, enter a description in the Add Description field.
5. Click **OK**.

5.2.1.6. Delete a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, find the domain name that you want o delete and click **Delete** in the Actions column.

4. In the message that appears, click **Delete**.

5.2.1.7. Delete multiple tenant forwarding domain names at a time

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the **Private Domain Names for VPC** page, click the **Tenant Forwarding Configurations** tab.
3. On the Tenant Forwarding Domain Names subtab, select one or more domain names that you want to delete and click **Batch Delete** in the lower-left corner of the tab.
4. In the message that appears, click **Delete**.

5.2.2. Tenant default forwarding configurations

5.2.2.1. View default forwarding configurations

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab. You can view the created default forwarding configurations on this subtab.

5.2.2.2. Create a default forwarding configuration

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab.
3. Click **Add Configuration**.
4. Set the required parameters, including Organization, Resource Set, Forwarding Mode, and *Destination IP Address*. The following table describes the Forwarding Mode and Destination IP Address

parameters.

Parameter	Description
Forwarding Mode	The forwarding mode to be used. For both domain name-based forwarding and default forwarding, the following two forwarding modes are supported: ○ Forward All Mode: forwards DNS requests to the destination DNS server. If the destination DNS server cannot resolve a domain name, a message is returned to the DNS client indicating that the request failed. ○ Forward First Mode: A specified DNS server is preferentially used to resolve domain names. If the specified DNS server cannot resolve a domain name, the local DNS server is used. If you enter internal IP addresses in the Destination IP Address field, unexpected results may occur during recursive resolution. For example, a domain name used for internal network services may be resolved to a public IP address.
Destination IP Address	The destination IP addresses. **Note** You can specify up to five unique IPv4 or IPv6 addresses. Each address must be in a separate row.

5. Click **OK**.

5.2.2.3. Associate a default forwarding configuration with a VPC

Tenant resources are isolated based on VPCs. To ensure that the DNS forwarding configurations take effect, you must associate a default forwarding configuration with a VPC.

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab.
3. Find the default forwarding configuration with which you want to associate a VPC and click **Associate VPC** in the Actions column.
4. Select one or more VPCs from the Associate VPC drop-down list and click **OK**.

5.2.2.4. Disassociate a default forwarding configuration from a VPC

This topic describes how to disassociate a default forwarding configuration from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab
3. Find the default forwarding configuration that you want to disassociate from a VPC and click the number in the **Associated VPCs** column.
4. On the VPCs page, find the VPC from which you want to disassociate the default forwarding configuration and click **Disassociate** in the Actions column.

   The VPC from which you dissociate the default forwarding configuration is no longer displayed on the VPCs page.

5.2.2.5. Modify a default forwarding configuration

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab
3. Find the default forwarding configuration that you want to modify and click **Modify** in the Actions column.
4. In the dialog box that appears, modify the **Forwarding Mode** or **Destination IP Address** parameter based on your business requirements.
5. Click **OK**.

5.2.2.6. Add a description to a default forwarding configuration

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab
3. Find the default forwarding configuration for which you want to add a description and click **Add Description** in the Actions column.
4. In the Add Description dialog box, enter a description in the **Add Description** field.
5. Click **OK**.

5.2.2.7. Delete a default forwarding configuration

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab
3. Find the default forwarding configuration that you want to delete and click **Delete** in the Actions column.
4. In the message that appears, click **Delete**.

5.2.2.8. Delete multiple default forwarding configurations at a time

Prerequisites

The permissions of a system administrator or level-1 organization administrator are granted to your account.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Click **VPCs** in the left-side navigation pane. On the Private Domain Names for VPC page, click the **Tenant Forwarding Configurations** tab. Then, click the **Tenant Default Forwarding Configurations** subtab
3. Select one or more default forwarding configurations and click **Batch Delete** in the lower-left corner.
4. In the message that appears, click **Delete**.

6.Scheduling instances

A scheduling instance is a unit for global traffic management. Apsara Stack DNS schedules the traffic of specific domain names based on scheduling instances.

6.1. Scheduling instances

The Scheduling Instance page displays all existing scheduling instances. You can create, delete, modify, and configure scheduling instances on this page. You must associate an address pool and a scheduling domain with the instance.

6.1.1. Create a scheduling instance

You must associate a scheduling instance with a scheduling domain and an address pool.

1. In the left-side navigation pane, click **Scheduling Instances.**

2. On the Scheduling Instance tab, click **Create Scheduling Instance** in the upper-left corner.

3. In the Create Scheduling Instance dialog box, set parameters such as Scheduling Instance Name, Scheduling Domain Name, Scheduling Domain, and Global TTL, and click **OK**.

6.1.2. Modify a scheduling instance

1. In the left-side navigation pane, click **Scheduling Instances.**

2. On the Scheduling Instance tab, find the scheduling instance that you want to modify and click **Modify** in the Actions column.

3. In the Modify Scheduling Instance dialog box, modify the configurations of the scheduling instance based on your business requirements and click **OK**.

6.1.3. Configure a scheduling instance

You can create, delete, modify, and query access policies for scheduling instances.

1. In the left-side navigation pane, click **Scheduling Instances**.
2. On the Scheduling Instance tab, find the scheduling instance that you want to configure and click **Edit** in the **Actions** column.
3. The Access Policy page appears, which displays information about the access policies that you have created for the scheduling instance in the **Name**, **DNS Query Sources**, **Address Pool in Use, Switchover Policy, and Address Pool** columns.
4. Click the plus icon (**+**) next to an access policy to view its details, including information about the **primary and secondary address pools**.
5. Open the **Edit Access Policy** dialog box and set the **Address Pool Switchover Policy** parameter. The default value is **Automatic**. You can change the value to **Manual**. If you set the Address Pool Switchover Policy parameter to **Automatic**, the system automatically selects an available address pool. If you set the Address Pool Switchover Policy parameter to **Manual**, you must manually specify whether to use the **primary address pool** or **secondary address pool**.

> **Note**
>
> Whether an address pool is available is determined based on the number of normal addresses in the address pool and the minimum number of available addresses in an address pool that you specify when you configure the access policy. If the number of normal addresses in the address pool is less than the specified minimum number of available addresses in an address pool, the address pool is considered unavailable. You can perform a health check to obtain the number of normal addresses in the address pool.

Processing logic for automatic switchover

State of the primary address pool	State of the secondary address pool	Comparison between the numbers of normal addresses in the primary and secondary address pools	Effective address pool (list of available addresses)
Available	Available	N/A	Primary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)
Available	Unavailable	N/A	Primary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)
Unavailable	Available	N/A	Secondary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)

Unavailable	Unavailable	Number of normal addresses in the primary address pool > Number of normal addresses in the secondary address pool	Primary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)
Unavailable	Unavailable	Number of normal addresses in the primary address pool < Number of normal addresses in the secondary address pool	Secondary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)
Unavailable	Unavailable	Number of normal addresses in the primary address pool = Number of normal addresses in the secondary address pool > 0	Primary address pool (including the normal addresses that are automatically returned and the addresses that are always online. Abnormal addresses that are automatically returned are deleted, or their weight values are set to 0.)

Unavailable	Unavailable	Number of normal addresses in the primary address pool = Number of normal addresses in the secondary address pool = 0	If the DNS request source is a custom line, the system clears the DNS configurations of the line instead of selecting an address pool. The configurations of the custom line are deleted. If the DNS request source is the global default line, the system selects the primary address pool. The system returns all the configured addresses without considering their return mode.

When the system compares the numbers of normal addresses between the primary and secondary address pools, normal addresses include the normal addresses that are automatically returned and all addresses that are always online (with the health status ignored). The abnormal addresses that are automatically returned and all addresses that are always offline (with the health status ignored) are not normal addresses.

The following table describes the processing logic for address types if a line is selected in two access policies.

Scenario	Address type for the effective address pool in two access policies		Processing logic
Same DNS request source: Scenario 1	IPv4	IPv6	IPv4 and IPv6 addresses take effect at the same time.
Same DNS request source: Scenario 2	IPv4	Domain name	Addresses of the domain name type take effect.
Same DNS request source: Scenario 3	IPv6	Domain name	Addresses of the domain name type take effect.

6.1.3.1. Create an access policy

You can create multiple access policies to resolve different address pools based on different DNS request sources.

1. On the Access Policy page, click **Create Access Policy** in the upper-left corner.

2. In the Create Access Policy dialog box, set the **Access Policy**, **DNS Query Source**, **Primary Address Pool**, and Secondary Address Pool parameters. If you turn on Whether Source of DNS Queries Is Global Default, you cannot set the DNS Query Source parameter to configure multiple lines. You can leave the Secondary Address Pool parameter empty, but the Primary Address Pool parameter is required.
3. The address types of the primary and secondary address pools are automatically identified based on the address pools that you specify. For example, you can specify address pools of the IPv4, IPv6, or domain name address type. Then, set the **Minimum Number of Available Primary Address Pools** parameter. If the number of healthy addresses in an address pool is less than the value of this parameter, the address pool is determined to be unavailable. The value of the Minimum Number of Available Primary Address Pools parameter must be an integer ranging from 1 to 100.
4. Set the **Address Pool Switchover Policy** parameter. The default value is **Automatic**. You can change the value to **Manual**. If you set the Address Pool Switchover Policy parameter to **Automatic**, the system automatically selects an available address pool. If you set the Address Pool Switchover Policy parameter to **Manual**, you must manually specify whether to use the **primary address pool** or **secondary address pool**.
5. Click **OK**.

The following table describes the limits on address types of the primary and secondary address pools for two access policies that have the same DNS request source.

Scenario	Address type of the primary address pool (access policy 1)	Address type of the secondary address pool (access policy 2)	Processing logic
Same DNS request source: Scenario 1	IPv4	IPv4	The address pools are allowed to be added.
Same DNS request source: Scenario 2	IPv4	IPv6	The address pools are not allowed to be added.
Same DNS request source: Scenario 3	IPv4	Domain name	The address pools are allowed to be added.
Same DNS request source: Scenario 4	IPv6	IPv4	The address pools are not allowed to be added.
Same DNS request source: Scenario 5	IPv6	IPv6	The address pools are allowed to be added.
Same DNS request source: Scenario 6	IPv6	Domain name	The address pools are allowed to be added.

Same DNS request source: Scenario 7	Domain name	IPv6	The address pools are allowed to be added.
Same DNS request source: Scenario 8	Domain name	IPv4	The address pools are allowed to be added.
Same DNS request source: Scenario 9	Domain name	Domain name	The address pools are allowed to be added.

The following tables describe the limits on address types of primary address pools and those of the secondary address pools for two access policies that have the same DNS request source.

Scenario	Address type of the primary address pool (access policy 1)	Address type of the primary address pool (access policy 2)	Processing logic
Same DNS request source: Scenario 1	IPv4	IPv6	The address pools are allowed to be added, and they can coexist.
Same DNS request source: Scenario 2	IPv4	IPv4	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 3	IPv4	Domain name	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 4	IPv6	IPv6	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 5	Domain name	IPv6	The address pools are not allowed to be added, and they cannot coexist.

Same DNS request source: Scenario 6	Domain name	Domain name	The address pools are allowed to be added, and they can coexist. However, the following conditions must be met: 1. The two primary address pools are the same. 2. Both of the secondary address pools exist. In addition, one secondary address pool is of the IPv4 address type, and the other is of the IPv6 address type.

Scenario	Address type of the secondary address pool (access policy 1)	Address type of the secondary address pool (access policy 2)	Processing logic
Same DNS request source: Scenario 1	IPv4	IPv6	The address pools are allowed to be added, and they can coexist.
Same DNS request source: Scenario 2	IPv4	IPv4	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 3	IPv4	Domain name	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 4	IPv6	IPv6	The address pools are not allowed to be added, and they cannot coexist.
Same DNS request source: Scenario 5	Domain name	IPv6	The address pools are not allowed to be added, and they cannot coexist.

Same DNS request source: Scenario 6	Domain name	Domain name	The address pools are allowed to be added, and they can coexist. However, the following conditions must be met: 1. The two secondary address pools are the same. 2. Both of the two primary address pools exist. In addition, one primary address pool is of the IPv4 address type, and the other is of the IPv6 address type.

6.1.3.2. Modify an access policy

Notice

If you do not change the primary or secondary address pool when you modify an access policy, no primary/secondary switchover is triggered. If you change one of the address pools, the system applies the following processing rules:

1. Manual switchover mode: If the secondary address pool is deleted, the system forcibly switches services to the primary address pool. If the secondary address pool is not deleted, the effective address pool does not change.
2. Automatic switchover mode: The system determines the address pool that takes effect based on the status of the newly selected address pools. Exercise caution when you change the address pools.

1. On the Access Policy page, find the access policy that you want to modify and click **Edit** in the Actions column.
2. In the Edit Access Policy dialog box, modify the **Access Policy**, **DNS Query Source**, **Primary Address Pool**, and Secondary Address Pool parameters. If you turn on Whether Source of DNS Queries Is Global Default, you cannot set the DNS Query Source parameter to configure multiple lines. You can leave the Secondary Address Pool parameter empty, but the Primary Address Pool parameter is required.
3. The address types of the primary and secondary address pools are automatically identified based on the address pools that you specify. For example, you can specify address pools of the IPv4, IPv6, or domain name address type. Then, modify the **Minimum Number of Available Primary Address Pools** parameter. If the number of healthy addresses in an address pool is less than the value of this parameter, the address pool is determined to be unavailable. The value of the Minimum Number of Available Primary Address Pools parameter must be an integer ranging from 1 to 100.

4. Modify the **Address Pool Switchover Policy** parameter. The default value is **Automatic**. You can change the value to **Manual**. If you set the Address Pool Switchover Policy parameter to **Automatic**, the system automatically selects an available address pool. If you set the Address Pool Switchover Policy parameter to **Manual**, you must manually specify whether to use the **primary address pool** or **secondary address pool**.
5. Click **OK**.

6.1.3.3. Delete an access policy

On the Access Policy page, find the access policy that you want to delete and click **Delete** in the Actions column.

In the message that appears, verify the information and click **Delete**.

6.1.4. Delete a scheduling instance

1. **Click Scheduling Instances in the left-side navigation pane.**

2. On the Scheduling Instance tab, find the scheduling instance that you want to delete and click **Delete** in the Actions column.

3. In the message that appears, click **Delete**.

Note: After you delete the instance, its configuration data is also deleted.

6.2. Address pools

You can manage address pools on the Address Pool page. For example, you can associate address pools with the access policies of scheduling instances. Address pools are classified into three types: IPv4 address pools, IPv6 address pools, and domain name address pools. The load balancing policy of an address pool can be set to Round-robin Scheduling or Weight.

1. Log on to the Apsara Stack DNS console.
2. Click **Scheduling Instances** in the left-side navigation pane. On the Scheduling Instance page, click the **Address Pool** tab.
3. The Address Pool tab displays information about the created address pools in the Address Pool Name/ID, Address Type, Load Balancing Policy, Addresses, Created At, and Last Modified At columns. You can also click the buttons in the Actions column to perform specific operations on an address pool.
4. Click the plus icon (+) to the left of an address pool. In the section that appears, you can view the addresses in the address pool and the return mode and health status of the addresses.

6.2.1. Create an address pool

You can define a list of addresses that form an address pool, which can be associated with the access policies of scheduling instances when you configure the access policies.

1. Log on to the Apsara Stack DNS console.
2. Click **Scheduling Instances** in the left-side navigation pane. On the Scheduling Instance page, click the Address Pool tab.
3. On the Address Pool tab, click **Create Address Pool**.

4. In the Create Address Pool dialog box, set the **Address Pool Name**, **Address Type**, and **Load Balancing Policy (Among Addresses)** parameters, add addresses one by one in the **Addresses** section, and then click **OK**. The following table describes some of the required parameters.

Parameter	Description
Address Pool Name	The name of the address pool. The name can contain a maximum of 20 characters.
Address Type	The address type of the address pool. You can select IPv4, IPv6, or Domain Name from the drop-down list. You cannot modify this parameter after you create the address pool.
Load Balancing Policy (Among Addresses)	The load balancing policy of the address pool. You can select Round-robin Scheduling or Weight from the drop-down list. You cannot modify this parameter after you create the address pool.
Mode	The mode of the added address. Valid values: • Automatically Returned: The system determines whether the address is available based on the health check result of the address. • Always Online: The system ignores the health check result of the address and sets the address to be always available. The health check task is still running. • Always Online: The system ignores the health check result of the address and sets the address to be always unavailable. The health check task is still running.

6.2.2. Modify an address pool

> **Notice**
>
> After you modify an address pool, the health check results of all addresses in the address pool are reset to normal if health check is enabled. If the address pool has been associated with specific access policies and automatic switchover is enabled, a primary/secondary switchover may be triggered. Proceed with caution when you modify an address pool.

1. Log on to the Apsara Stack DNS console.
2. Click **Scheduling Instances** in the left-side navigation pane. On the Scheduling Instance page, click the **Address Pool** tab.
3. On the Address Pool tab, find the address pool that you want to modify and click **Modify** in the Actions column.
4. In the Modify Address Pool dialog box, modify the **Address Pool Name** parameter and the addresses specified in the **Addresses** section.
5. Click **OK**.

6.2.3. Delete an address pool

1. **In the left-side navigation pane, click Scheduling Instances. On the Scheduling Instance page, click the Address Pool tab.**

2. On the Address Pool tab, find the address pool that you want to delete and click **Delete** in the Actions column.

3. In the message that appears, click **Delete**.

6.2.4. Create a health check task for an address pool

You can enable health check to check the status of the addresses in an address pool. Only the addresses whose health check result is normal can be returned.

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, click **Scheduling Instances**. On the Scheduling Instance page, click the **Address Pool** tab.
3. On the Address Pool tab, find the address pool for which you want to create a health check task and click **Health Check** in the Actions column.
4. On the Health Check page, click **Create Health Check Task** in the upper-left corner. In the Create Health Check Task dialog box, turn on or off **Health Check** based on your business requirements, set the remaining parameters, and then click **OK**. The following table describes the parameters.

Configuration category or parameter	Parameter	Description	Supported protocols
	Port	The port number that is used for health checks on the address pool. The value must be an integer in the range of 1 to 65535. This parameter cannot be empty.	HTTP, HTTPS, TCP, and UDP
	URL	The HTTP or HTTPS path that is used for health checks on the address pool. This path is used to check whether the HTTP or HTTPS service of an address in the address pool is normal. If the HTTP status code returned from this path is 2xx or 3xx, the HTTP or HTTPS service is normal. The system automatically adds a forward slash (/) before the path. The path can be empty. The default value is /. The path can be up to 255 characters in length.	HTTP and HTTPS

Configuration category or parameter	Parameter	Description	Supported protocols
Protocol Settings	Host Settings	The host configuration that is used for health checks. If you do not set this parameter, the primary domain name is used.	HTTP and HTTPS
	Returned Code Greater Than	The minimum value of the HTTP status code when the health check result is abnormal. The system considers the result of a health check to be abnormal if the HTTP status code returned is greater than or equal to the value of this parameter.	HTTP and HTTPS
Health check settings	Interval	The time interval at which health checks are performed on the address pool.	
	Timeout Period	The timeout period for which the system waits after an exception occurs.	
	Number of Retries	The minimum number of consecutive health check failures that must occur before the status of an address is considered abnormal.	

7.Global lines

Apsara Stack DNS allows you to define lines based on IP addresses on the Global Line page. The lines are used to group request sources to achieve intelligent load balancing. The lines can be referenced by global domain names in Apsara Stack.

7.1. Create a global line

1. Click **Query Source** in the left-side navigation pane.
2. Click **Add Line** in the upper-left corner of the Global Line page.
3. In the Add Line dialog box, set the required parameters and click **OK**.

7.2. Change the priority of a global line

1. Click **Query Source** in the left-side navigation pane.
2. On the Global Line page, find the line whose priority you want to change and click **Sort** in the Actions column.
3. In the Sort Line dialog box, specify a sorting method and click **OK**.

7.3. Modify a global line

1. Click **Query Source** in the left-side navigation pane.
2. On the Global Line page, find the line that you want to modify and click **Modify** in the Actions column.
3. In the Modify Line dialog box, modify the parameters based on your business requirements and click **OK**.

7.4. Delete a global line

1. Click **Query Source** in the left-side navigation pane.
2. On the Global Line page, find the line that you want to delete and click **Delete** in the Actions column.
3. In the message that appears, click **Delete**.

8.Private lines

Apsara Stack DNS allows you to define lines based on IP addresses on the Private Line page. The lines are used to group request sources to achieve intelligent load balancing. The lines can be referenced by private domain names for VPCs.

8.1. Create a private line

1. Click **Query Source (Private Zone)** in the left-side navigation pane.
2. Click **Add Line** in the upper-left corner of the Private Line page.
3. In the Add Line dialog box, set the required parameters and click **OK**.

8.2. Change the priority of a private line

1. Click **Query Source (Private Zone)** in the left-side navigation pane.
2. On the Private Line page, find the line whose priority you want to change and click **Sort** in the Actions column.
3. In the Sort Line dialog box, specify a sorting method and click **OK**.

8.3. Modify a private line

1. Click **Query Source (Private Zone)** in the left-side navigation pane.
2. On the Private Line page, find the line that you want to modify and click **Modify** in the Actions column.
3. In the Modify Line dialog box, modify the parameters based on your business requirements and click **OK**.

8.4. Delete a private line

1. Click **Query Source (Private Zone)** in the left-side navigation pane.
2. On the Private Line page, find the line that you want to delete and click **Delete** in the Actions column.
3. In the message that appears, click **Delete**.

9.Nodes

The Nodes page displays the DNS servers that serve as nodes. On this page, you can monitor the role and status of each node and check data consistency after synchronization.

9.1. Configure the emergency group feature

1. Click **Nodes** in the left-side navigation pane.

2. Click **Create Emergency Group** in the upper-left corner of the Nodes page.

3. In the Create Emergency Group dialog box, turn on or off **Emergency Group** based on your business requirements. If you turn on the switch, you need to set the Service Instance parameter.

9.2. Add a description for a node

1. Click **Nodes** in the left-side navigation pane.

2. Find the node for which you want to add a description based on IP addresses and click **Add Description** in the Actions column. In the Add Description dialog box, enter a description in the Add Description field and click OK.

9.3. Set a follower node as the leader node

1. Click **Nodes** in the left-side navigation pane.

2. Find the follower node that you want to set as the leader node based on IP addresses and click **Switch Primary Node** in the Actions column. In the message that appears, click **OK**. Then, the system sets the selected node as the new leader of the cluster for data synchronization.

10.View a node

1. Click **Nodes** in the left-side navigation pane.

2. On the Nodes page, find the node that you want to view and check the information displayed in the **Service Instance IP Address**, **Service Instance Role**, **Working Mode**, **Working Status**, **Latest Synchronization Log ID**, **Service Address**, and **Description** columns. You can also view the operations that you can perform on the node in the **Actions** column.

11.Logs

The Logs page displays the alert information about the DNS server cluster.

11.1. Query alert logs

1. Click **Logs** in the left-side navigation pane.

2. On the Logs page, select the type of alert log that you want to query from the drop-down list in the upper-left corner. You can select **All, Primary/Secondary Address Pool Switchover, Address Pool Unavailable, The address pool becomes available, Address Unavailable, or Address Restored to Available**. Then, enter a keyword in the search box, specify the start and end time for the query, and then click **Search**.

3. Check the information displayed in the **Time**, **Object**, **Behavior**, and **Content** columns.