ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Alibaba Cloud DNS

User Guide

Product Version: V3.14.0

Document Version: 20220928

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. Apsara Stack DNS then 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 VPCs. You can perform the following operations on 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. In the top navigation bar, choose **Products > Networking > Apsara Stack DNS**.

4.Internal DNS resolution management

Internal DNS resolution management allows you to manage global internal domain names, global forwarding configurations, and global recursive resolution configurations that you have created in Apsara Stack.

4.1. Global internal domain names

4.1.1. Overview

All the operations of this feature require administrator privileges.

4.1.2. View an internal domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domains > Global Internal Domains**.
3. In the **Domain Name** search box, enter the domain name that you want to view.
4. Click **Search**.

   The search result is displayed.

4.1.3. Add a domain name

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Global Internal Domain Name**.
3. Click **Add Domain Name**.
4. In the dialog box that appears, enter **Global Internal Domain Name**.
5. Click **OK**.

4.1.4. Add a description for a domain name

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

Context

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Global Internal Domain Name**.
3. Find the domain name for which you want to add a description, click the icon in the Actions column, and then select **Description**.
4. In the dialog box that appears, enter a description.
5. Click **OK**.

4.1.5. Delete a domain name

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Global Internal Domain Name**.
3. Find the domain name that you want to delete, click the icon in the **Actions** column, and then select **Delete**.
4. In the message that appears, click **OK**.

4.1.6. Delete multiple domain names

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Global Internal Domain Name**.
3. Select one or more domain names that you want to delete and click **Delete** in the upper-right corner.
4. In the message that appears, click **OK**.

4.1.7. Configure DNS records

This topic describes how to configure DNS records in the Apsara Uni-manager Management Console.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Global Internal Domain Name**.

3. Find the domain name for which you want to configure DNS records, click the  icon in the Actions column, and then select **Configure DNS Records**.
4. On the **Configure DNS Records** page, click **Add DNS Record** in the upper-right corner.
5. Perform the following operations as needed:
   - Add a description for a DNS record

     Select the DNS record for which you want to add a description, click  in the Actions column, and then select **Description** from the shortcut menu. In the dialog box that appears, enter a description and click **OK**.
   - Delete a DNS record

     Select the DNS record that you want to delete, click  in the Actions column, and then select **Delete** from the shortcut menu. In the message that appears, click **OK**.
   - Modify a DNS record

     Select the DNS record that you want to modify, click  in the Actions column, and then select **Modify** from the shortcut menu. In the dialog box that appears, set the required parameters and click **OK**.
   - Delete DNS records in batches

     Select the DNS records that you want to delete and click **Delete** in the upper-right corner. In the message that appears, click **OK**.

4.1.8. View a resolution policy

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domains > Global Internal Domains**.
3. Find the target domain name, click the  icon in the Actions column, and then select **Configure DNS Records**.
4. On the page that appears, select the domain name for which you want to configure DNS records, and click **Weight** in the **Resolution Policy** column.
5. On the page that appears, view the details of **Resolution Policy**.

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 global forwarding domain names

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Forwarding Domain Names**.
3. In the **Domain Name** search box, enter the domain name that you want to query and click **Search**.

4.2.1.3. Add a domain name

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Forwarding Domain Names**.
3. Click **Add Domain Name**.
4. In the dialog box that appears, configure *Global Forwarding Domain*, *Forwarding Mode*, and *Forwarder IP Addresses*. Then, click **OK**.

4.2.1.4. Add a description for a domain name

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

Context

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Forwarding Domain Names**.

3. Select the domain name for which you want to add a description, click  in the Actions column, and then select **Description**.
4. In the dialog box that appears, enter a description and click **OK**.

4.2.1.5. Modify the forwarding configurations of a domain name

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Forwarding Domain Names**.
3. Find the domain name whose forwarding configurations you want to modify, click the  icon in the Actions column, and then select **Modify**.
4. In the dialog box that appears, change the value of *Forwarding Mode* or *Forwarder IP Addresses*, and click **OK**.

4.2.1.6. Delete a domain name

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Forwarding Domain Names**.
3. Find the domain name that you want to delete, click the  icon in the Actions column, and then select **Delete**.
4. Click **OK**.

4.2.1.7. Delete multiple domain names

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

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Domains > Forwarding Settings > Global Forwarding Domain Names**.

3. Select one or more domain names that you want to delete and click **Delete** in the upper-right corner.
4. In the message that appears, click **OK**.

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 administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Default Forwarding**.
3. Click the  icon in the Actions column and select **Enable**.
4. In the dialog box that appears, configure *Default Forwarding Mode* and *Forwarder IP Addresses*. Then, click **OK**.

   Make sure that Enable Default Forwarding is set to 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 administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Default Forwarding**.
3. Click the  icon in the Actions column and select **Modify**.
4. In the dialog box that appears, configure *Forwarding Mode* and *Forwarder IP Addresses*. Then, click **OK**.

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 administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Domain Names > Forwarding Settings > Global Default Forwarding**.

3. Click the  icon in the Actions column and select **Disable**.
4. In the message that appears, click **OK**.

4.3. Global recursive resolution

4.3.1. Enable global recursive resolution

Prerequisites

You have administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Internal Domains > Global Recursive Resolution**.
3. Click the  icon in the Actions column and select **Enable**.
4. In the dialog box that appears, click **OK**.

4.3.2. Disable global recursive resolution

Prerequisites

You have administrator permissions.

Procedure

1. Log on to the Apsara Stack DNS console.
2. Choose **Internal Domains > Global Recursive Resolution**.
3. Click the  icon in the Actions column and select **Disable**.
4. In the dialog box that appears, click **OK**.

5.PrivateZone (DNS Standard Edition only)

The PrivateZone feature allows you to create VPC-specific tenant domain names. You can bind the domain names to VPCs as required to achieve tenant isolation.

5.1. Tenant internal domain name

5.1.1. View a domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. In the **Domain Name** search box, enter the domain name that you want to view.
4. Click Search.

   The search result is displayed.

5.1.2. Add a domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Click **Add Domain Name**.
4. In the dialog box that appears, set *Tenant Internal Domain Name*.
5. Click **OK**.

5.1.3. Bind an organization to a VPC

Tenant domain names are isolated based on VPCs. To ensure that the DNS forwarding configurations take effect, you must bind the organization of domain names to a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name, click the  icon in the Actions column, and select **Associate VPCs**.
4. Select one or more VPCs from the list of VPCs to Select, click the right arrow to add them to the list of VPCs Selected, and then click **OK**.

5.1.4. Unbind a domain name from a VPC

This topic describes how to unbind a domain name from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name and click the number in the **VPCs Associated** column.
4. On the **VPCs Associated** page, find the target VPC, click the icon in the **Actions** column, and then select **Disassociate**.

   Make sure that the unbound VPC is no longer displayed on the VPCs Associated page.

5.1.5. Add a description for a domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select **Description**.
4. In the dialog box that appears, enter a description.
5. Click **OK**.

5.1.6. Delete a domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select **Delete**.
4. In the message that appears, click **OK**.

5.1.7. Delete multiple domain names

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal**

Domains.

3. Select one or more domain names that you want to delete and click **Delete** in the upper-right corner.
4. In the message that appears, click **OK**.

5.1.8. Configure DNS records

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name, click the  icon in the Actions column, and then select **Configure DNS Records**.
4. In the upper-right corner of the **Configure DNS Records** page, click **Add DNS Record**.
5. In the **Add DNS Record** dialog box, configure *Host*, *Type*, *TTL*, *Resolution Policy*, and *Record Set*. Then, click **OK**.

   The following tables describe the types of DNS records.

   - A record

Resolution policy	Formatting rule
None	You can enter up to 100 unique IPv4 addresses, each in a separate row. Make sure that the IPv4 addresses are valid. Example: ■ 192.168.1.1 ■ 192.168.1.2 ■ 192.168.1.3
Weight	You can enter up to 100 unique IPv4 addresses, each in a separate row. Format: ■ [IPv4 address] [Weight] (The IPv4 address and weight are separated with a space.) ■ Make sure that the IPv4 addresses are valid. ■ The weight value is an integer ranging from 0 to 999. A larger value indicates a greater weight. Example: ■ 192.168.1.1 20 ■ 192.168.1.1 30 ■ 192.168.1.1 50

   - AAAA record

Resolution policy	Formatting rule
None	You can enter up to 100 unique IPv6 addresses, each in a separate row. Make sure that the IPv6 addresses are valid. Example: ■ 2400:3200::6666 ■ 2400:3200::6688 ■ 2400:3200::8888
Weight	You can enter up to 100 unique IPv6 addresses, each in a separate row. Format: ■ [IPv6 address] [Weight] (The IPv6 address and weight are separated with a space.) ■ Make sure that the IPv6 addresses are valid. ■ The weight value is an integer ranging from 0 to 999. A larger value indicates a greater weight. Example: ■ 2400:3200::6666 20 ■ 2400:3200::6688 20 ■ 2400:3200::8888 60

- CNAME record

Resolution policy	Formatting rule
None	You can enter only one domain name. The domain name must be a fully qualified domain name (FQDN) that ends with a dot (.). It must be 1 to 255 characters in length. Example: www.example.com.
Weight	You can enter up to 100 unique domain names, each in a separate row. Format: ■ [Domain name] [Weight] (The domain name and weight are separated with a space.) ■ The domain name must be an FQDN that ends with a period (.). It must be 1 to 255 characters in length. ■ The weight value is an integer ranging from 0 to 999. A larger value indicates a greater weight. Example: ■ www1.example.com. 20 ■ www2.example.com. 20 ■ www3.example.com. 60

- MX record

Resolution policy	Formatting rule
None	You can enter 100 unique email server hostnames, each in a separate row. Format: ■ [Priority] [Email server hostname] (The priority and hostname are separated with a space.) ■ The priority value is 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 (.). It must be 1 to 255 characters in length. Example: ■ 10 mailserver1.example.com. ■ 20 mailserver2.example.com.

- TXT record

Resolution policy	Formatting rule
None	You can enter up to 100 unique character strings, each in a separate row. A string must be 1 to 255 characters in length. No row can be left blank. Example: "v=spf1 ip4:192.168.0.1/16 ip6:2001::1/96 ~all"

- PTR record

Resolution policy	Formatting rule
None	You can enter up to 100 unique domain names, each in a separate row. The DNS server address must be an FQDN that ends with a period (.). It must be 1 to 255 characters in length. Example: ■ www1.example.com. ■ www2.example.com. ■ www3.example.com.

- SRV record

Resolution policy	Formatting rule

Resolution policy	Formatting rule
None	You can enter up to 100 unique application server hostnames, each in a separate row. Format: ■ [Priority] [Weight] [Port number] [Application server hostname] (Every two items are separated with a space.) ■ The priority value is an integer ranging from 0 to 999. A smaller value indicates a higher priority. ■ The weight value is an integer ranging from 0 to 999. A larger value indicates a greater weight. ■ The port number is an integer ranging from 0 to 65535. It indicates the TCP or UDP port used for network communications. ■ The application server hostname must be an FQDN that ends with a period (.). It must be 1 to 255 characters in length. Example: ■ 1 10 8080 www1.example.com. ■ 2 20 8081 www2.example.com.

- NAPTR record

Resolution policy	Formatting rule

Resolution policy	Formatting rule
None	You can enter up to 100 unique NAPTR record values, each in a separate row. Format: ■ [Serial number] [Priority] [Flag] [Service information] [Regular expression] [Substitute domain name] (Every two items are separated with a space.) ■ The serial number is an integer ranging from 0 to 999. A smaller value indicates a higher priority. ■ The priority value is 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 blank or be a character from A to Z, a to z, or 0 to 9. It is not case-sensitive and must be enclosed in double quotation marks (""). ■ The service information can be left blank or be a string of 1 to 32 characters. It must start with a letter and be enclosed in double quotation marks (""). ■ The regular expression can be left blank 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 (.). It must be 1 to 255 characters in length. Example: ■ 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

Resolution policy	Formatting rule
None	You can enter up to 100 unique CAA records, each in a separate row. Format: ■ [Certificate authority flag] [Certificate property tag] [Authorization information] (Every two items are separated with a space.) ■ The certification authority flag is 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 (""). Example: ■ 0 issue "caa.example.com" ■ 0 issuewild ";" ■ 0 iodef "mailto:example@example.com"

- NS record

Resolution policy	Formatting rule
None	You can enter up to 100 unique DNS server addresses, each in a separate row. The DNS server address must be an FQDN that ends with a period (.). It must be 1 to 255 characters in length. Wildcard domain names are not allowed. Example: ■ ns1.example.com. ■ ns2.example.com.

6. After you add DNS records, perform the following operations as required:
   - Add a description for a DNS record.

     Find the target DNS record, click the icon in the Actions column, and then select **Description**. In the dialog box that appears, enter a description and click **OK**.
   - Delete a DNS record.

     Find the target DNS record, click the icon in the Actions column, and then select **Delete**. In the message that appears, click **OK**.
   - Modify a DNS record.

     Find the target DNS record, click the icon in the Actions column, and then select **Modify**. In the dialog box that appears, modify the required parameters and click **OK**.
   - Delete multiple DNS records.

     Select the DNS records that you want to modify and click **Delete** in the upper-right corner. In the message that appears, click **OK**.

5.1.9. View a resolution policy

This topic describes how to view the details of a resolution policy.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Internal Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select Configure DNS Records.
4. View the resolution policy in the DNS Records list.

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. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. In the **Domain Name** search box, enter the domain name that you want to view.
4. Click **Search**.

   The search result is displayed.

5.2.1.2. Add a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Click **Add Domain Name**.
4. In the dialog box that appears, configure parameters such as *Domain Name*, *Forwarding Mode*, and *Forwarder IP Addresses*.

Parameter	Description
Domain Name	The domain name, which must meet the following formatting rules: ○ The domain name must be 1 to 255 characters in length. This includes the period (.) at the end of the domain name. ○ The domain name can contain multiple domain name segments that are separated with periods (.). A domain name segment must be 1 to 63 characters in length. It cannot contain consecutive periods (.) or be left blank. ○ The domain name can only contain letters (a to z, A to Z), digits (0 to 9), hyphens (-), and underscores (_). ○ The domain name must start with a letter, digit, or underscore (_) and end with a letter, digit, or period (.). ○ The domain name is not case-sensitive. The system saves the domain name in lowercase letters. ○ The period (.) at the end of the domain name is optional. The system adds a period (.) to the end of the domain name.

Parameter	Description
Forwarding Mode	For both domain name-based forwarding and default forwarding, the following two forwarding modes are supported: ○ Forward All Requests without Recursion: forwards DNS requests to the target DNS server. If the target DNS server cannot resolve the domain names, a message is returned to the DNS client indicating that the query failed. ○ Forward All Requests with Recursion: A specified DNS server is preferentially used to resolve domain names. If the specified DNS server cannot resolve the domain names, the local DNS is used instead. If you enter internal IP addresses in the Forwarder IP Addresses 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.
Forwarder IP Addresses	A list of destination IP addresses. **Note** Multiple IP addresses are separated with semicolons (;).

5. Click **OK**.

5.2.1.3. Bind an organization to a VPC

Tenant domain names are isolated based on VPCs. You must bind the organization of domain names to a VPC before the DNS forwarding configurations can take effect.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Find the target domain name, click the  icon in the Actions column, and then select **Associate VPCs**.
4. Select one or more VPCs from the list of VPCs to Select, click the right arrow to add them to the list of VPCs Selected, and then click **OK**.

5.2.1.4. Unbind a domain name from a VPC

This topic describes how to unbind a domain name from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Find the target domain name and click the number in the **VPCs Associated** column.

4. On the VPCs Associated page, find the target VPC, click the icon in the Actions column, and then select **Disassociate**.

   Make sure that the unbound VPC is no longer displayed on the VPCs Associated page.

5.2.1.5. Modify the forwarding configurations of a domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select **Modify**.
4. In the dialog box that appears, change the value of **Forwarding Mode** or **Forwarder IP Addresses**.
5. Click **OK**.

5.2.1.6. Add a description for a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select **Description**.
4. In the dialog box that appears, enter a description.
5. Click **OK**.

5.2.1.7. Delete a tenant forwarding domain name

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Find the target domain name, click the icon in the Actions column, and then select **Delete**.
4. In the message that appears, click **OK**.

5.2.1.8. Delete multiple tenant forwarding domain names

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Forwarding Domains**.
3. Select one or more domain names that you want to delete and click **Delete** in the upper-right corner.
4. In the message that appears, click **OK**.

5.2.2. Tenant default forwarding configurations

5.2.2.1. View default forwarding configurations

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.

5.2.2.2. Add a default forwarding configuration

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Click **Add Settings**.
4. In the dialog box that appears, configure parameters such as *Forwarding Mode* and *Forwarder IP Addresses*.

Parameter	Description

Parameter	Description
Forwarding Mode	For both domain name-based forwarding and default forwarding, the following two forwarding modes are available: ○ Forward All Requests without Recursion: Only a specified DNS server is used to resolve domain names. If the specified DNS server cannot resolve the domain names, a message is returned to the DNS client to indicate that the query failed. ○ Forward All Requests with Recursion: A specified DNS server is preferentially used to resolve domain names. If the specified DNS server cannot resolve the domain names, a local DNS server is used instead. If you enter internal IP addresses in the Forwarder IP Addresses 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.
Forwarder IP Addresses	A list of destination IP addresses. **Note** Multiple IP addresses are separated with semicolons (;).

5. Click **OK**.

5.2.2.3. Bind an organization to a VPC

Tenant domain names are isolated based on VPCs. You must bind the organization of domain names to a VPC before the DNS forwarding configurations can take effect.

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Find the target organization, click the  icon in the Actions column, and then select **Associate VPCs**.
4. Select one or more VPCs from the list of VPCs to Select, click the right arrow to add them to the list of VPCs Selected, and then click **OK**.

5.2.2.4. Unbind a domain name from a VPC

This topic describes how to unbind a domain name from a VPC.

Procedure

1. Log on to the Apsara Stack DNS console.

2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Find the target domain name and click the number in the **VPCs Associated** column.
4. On the VPCs Associated page, find the target VPC, click the icon in the Actions column, and then select **Disassociate**.

   Make sure that the unbound VPC is no longer displayed on the VPCs Associated page.

5.2.2.5. Modify a default forwarding configuration

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Find the target organization, click the icon in the Actions column, and then select **Modify**.
4. In the dialog box that appears, change the value of **Forwarding Mode** or **Forwarder IP Addresses**.
5. Click **OK**.

5.2.2.6. Add a default forwarding configuration

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Find the target organization, click the icon in the Actions column, and then select **Description**.
4. In the dialog box that appears, enter **Description**.
5. Click **OK**.

5.2.2.7. Delete a default forwarding configuration

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Find the target organization, click the  icon in the Actions column, and then select **Delete**.
4. In the dialog box that appears, click **OK**.

5.2.2.8. Delete multiple default forwarding configurations

Prerequisites

You have the permissions of a system administrator or level-1 organization administrator.

Procedure

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Forwarding Configurations > Tenant Forwarding Settings > Tenant Default Forwarding**.
3. Select one or more domain names that you want to delete and click **Delete** in the upper-right corner.
4. In the message that appears, click **OK**.

6.Internal Global Traffic Manager (internal GTM Standard Edition only)

Internal Global Traffic Manager (GTM) supports multi-cloud disaster recovery for domain names of customers. This feature manages traffic loads between multiple Apsara Stack networks.

6.1. Scheduling instance management

6.1.1. 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.

6.1.1.1. Create a scheduling instance

After you create a scheduling instance, you can associate the scheduling instance with a scheduling domain and address pool.

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Instances** > Scheduling Instance.

2. Click **Create Scheduling Instance** in the upper-right corner of the instance list.

3. In the dialog box that appears, configure Scheduling Instance Name, CNAME Access Domain Name, and Global TTL. Then, click **OK**.

6.1.1.2. Modify a scheduling instance

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Instances** > Scheduling Instance.

2. Find the instance that you want to modify and click **Modify** in the Actions column.

3. Modify the parameter settings as prompted and click **OK**.

6.1.1.3. Configure a scheduling instance

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

1. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the **Scheduling Instances** tab of the page that appears, click the **Scheduling Instances** tab.
2. Find the scheduling instance whose access policies you want to view and click **Configure** in the **Actions** column.
3. On the Access Policy Configuration page, view information about all the access policies of the scheduling instance. The information includes **Access Policy Name**, **DNS Request Source**, **Address Type**, **Effective Address Pool**, and **Last Modified At**.

4. Click the closing angle bracket (>) next to an access policy to view the details, including information about the **primary and secondary address pools**.
5. View the setting of **Address Pool Switchover Policy**. The default value is **Automatic**. You can change the value to **Manual**.If Address Pool Switchover Policy is set to Automatic, the system automatically selects an available address pool. If Address Pool Switchover Policy is set 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 Min. Number of Available Addresses that you specified when you configure the access policy. If the number of normal addresses in the address pool is less than the value of Min. Number of Available Addresses, 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	-	Primary address pool (including the normal addresses that are intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently returned are deleted, or their weight values are set to 0.)
Available	Unavailable	-	Primary address pool (including the normal addresses that are intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently returned are deleted, or their weight values are set to 0.)
Unavailable	Available	-	Secondary address pool (including the normal addresses that are intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently 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 intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently 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 intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently 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 intelligently returned and the addresses that are always online. Abnormal addresses that are intelligently 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 normal addresses that are intelligently returned and all addresses that are always online (with the health status ignored). The abnormal addresses that are intelligently 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.

6.1.1.3.1. Create an access policy for a scheduling instance

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

1. Log on to the Apsara Stack DNS console. In the left-side navigation pane, click Internal Global Traffic Manager. On the Scheduling Instances tab of the Global Traffic Management on the Internal Network page, find the scheduling instance for which you want to create an access policy and click Configure in the Actions column. On the page that appears, click **Create Access Policy**.
2. In the Create Access Policy dialog box, specify **Access Policy Name**, select items in the **DNS Request Source** section, and then configure parameters in the **Primary/Secondary Address**

Pool Configuration section. In the DNS Request Source section, if you select Global default, you cannot select other items. The parameters on the Primary Address Pool tab must be configured, and the parameters on the Secondary Address Pool tab can be left empty.

3. In the **Primary/Secondary Address Pool Configuration** section, you can set **Address Type** to IPv4, IPv6, or Domain Name to select different types of address pools. You can also set **Min. Number of Available Addresses**. 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 Min. Number of Available Addresses must be an integer ranging from 1 to 100.
4. Click **OK**.

The following table describes the limits on address type conflicts between 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 type conflicts between the primary address pools and those between 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 type and the other is of the IPv6 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 type and the other is of the IPv6 type.

6.1.1.3.2. Modify the access policy of a scheduling instance

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 complies with 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 Configuration page, find the access policy that you want to modify and click **Modify** in the Actions column.
2. In the Modify Access Policy dialog box, modify **Access Policy Name**, select items in the **DNS Request Source** section, and then configure parameters in the **Primary/Secondary Address**

Pool Configuration section. In the DNS Request Source section, if you select Global default, you cannot select other items. The parameters on the Primary Address Pool tab must be configured, and the parameters on the Secondary Address Pool tab can be left empty.

3. In the Primary/Secondary Address Pool Configuration section, you can set **Address Type** to IPv4, IPv6, or Domain Name to select address pools of different types. You can also set Min. Number of Available Addresses. 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 this parameter must be an integer ranging from 1 to 100.
4. Click **OK**.

6.1.1.3.3. Delete the access policy of a scheduling instance

1. On the Access Policy Configuration page, find the target access policy and click Delete in the Actions column.

2. In the dialog box that appears, click OK after you verify that the displayed information is correct.

6.1.1.4. Delete a scheduling instance

1. Log on to the Apsara Stack DNS console and choose Recursion Configurations > Scheduling Instances > Scheduling Instance.

2. Find the target instance and click Delete in the Actions column.

3. In the dialog box that appears, click OK.

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

6.1.2. Address Pool

The Address Pool tab allows you to manage address pools. You can associate address pools with scheduling instances. The 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 polling or weight.

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the **Scheduling Instance** tab of the Global Traffic Management on the Internal Network page, click the **Address Pool** tab.
3. Find the address pool whose information you want to view and click the closing angle bracket (>) next to the name of the address pool to view its detailed information. The information includes Address Pool ID, Address Pool Name, Address Type, Load Balancing Policy (Among Addresses), Created At, Last Modified At, Health Check, and Health Check Status.

6.1.2.1. Create an address pool

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

1. Log on to the Apsara Stack DNS console.

2. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the Scheduling Instance tab of the Global Traffic Management on the Internal Network page, click the Address Pool tab.
3. On the Address Pool tab, click **Create Address Pool**.
4. In the Create Address Pool dialog box, specify **Address Pool Name**, **Address Type**, and **Load Balancing Policy (Among Addresses)**, and add addresses one by one in the **Address List** section. You can also click **Batch Add** to add multiple addresses at a time. After you enter the required information, click **OK**.

Parameter	Description
Address Pool Name	The name can contain a maximum of 20 characters.
Address Type	You can select IPv4, IPv6, or Domain Name from the drop-down list of this parameter. This configuration cannot be changed.
Load Balancing Policy (Among Addresses)	You can select Polling or Weight from the drop-down list of this parameter. This configuration cannot be changed.
Mode	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 Offline: 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.

6.1.2.2. Modify the configurations of an address pool

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

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the **Scheduling Instance** tab of the Global Traffic Management on the Internal Network page, click the **Address Pool** tab.
3. Find the address pool that you want to modify and click **Modify** in the Actions column.
4. In the Modify Address Pool dialog box, you can change only **Address Pool Name** and the addresses in **Address (One in Each Row)**.
5. Click **OK**.

6.1.2.3. Delete an address pool

1. Log on to the Apsara Stack DNS console and choose Recursion Configurations > Scheduling Instances > Address Pool.
2. Find the target address pool and click Delete in the Actions column.
3. In the dialog box that appears, click OK after you verify that the displayed information is correct.

6.1.2.4. Enable health check

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

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the **Scheduling Instance** tab of the Global Traffic Management on the Internal Network page, click the **Address Pool** tab.
3. Find the address pool for which you want to configure a health check, and click **Health Check** in the Actions column.
4. In the Health Check dialog box, turn on or turn off **Health Check Switch**, specify the parameters in the **Protocol Settings**, **Health Check Settings**, and **Node Settings** sections, and then click **OK**.

Section	Parameter	Description	Protocol
Protocol Settings	Port	The port number that is used for health checks on the destination address. The value must be an integer in the range of 1 to 65535. This parameter cannot be empty.	HTTP/HTTPS/TCP/UDP
	Path	The HTTP or HTTPS path that is used for health checks on the destination address. This path is used to check whether the HTTP or HTTPS service of the destination address 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 name. The path can be empty. The default value is /. The path name can contain a maximum of 255 characters.	HTTP/HTTPS
	Host Configuration	The host configuration that is used for health checks. If you do not specify this parameter, the primary domain name is used.	HTTP/HTTPS

Section	Parameter	Description	Protocol
	Returned Error Code Greater Than or Equal to	The minimum value of the HTTP status code when the health check result is abnormal. The HTTP status code returned must be greater than or equal to the value of this parameter.	HTTP/HTTPS
	ICMP Packages Sent	The number of ICMP packets sent each time an Internet Control Message Protocol (ICMP) health check is performed.	ICMP
	Packet Loss Rate	The threshold of the packet loss rate. The threshold is used to determine whether the result of an ICMP health check is abnormal.	ICMP
Health Check Settings	Check interval	The time interval at which health checks are performed on the destination address.	
	Timeout Duration	The timeout duration for which the system waits after an exception occurs during a health check.	
	Failure Threshold	The minimum number of consecutive health check failures when the status of the destination address is abnormal during a health check.	
Node Settings	Selected node	The nodes that initiate health checks on the destination address.	

6.1.3. Scheduling Domain

The Scheduling Domain tab allows you to add, delete, and query scheduling domains.

You can log on to the Apsara Stack DNS console and choose Internal Global Traffic Manager > Scheduling Instances > Scheduling Domain to go to the scheduling domain list.

6.1.3.1. Create a scheduling domain

1. Log on to the Apsara Stack DNS console and choose Recursion Configurations > Scheduling Instances > Scheduling Domain. Then, click Create Scheduling Domain in the upper-right corner of the scheduling domain list.

2. In the dialog box that appears, enter the custom domain name and click OK.

6.1.3.2. Add a description for a scheduling domain

1. In the left-side navigation pane, choose Internal Global Traffic Manager > Scheduling Instances > Scheduling Domain.

2. Find the scheduling domain for which you want to add a description and click Edit in the Actions column.

3. In the dialog box that appears, add a description in the Edit field and click OK.

6.1.3.3. Delete a scheduling domain

1. In the left-side navigation pane, choose Internal Global Traffic Manager > Scheduling Instances > Scheduling Domain.

2. Find the scheduling domain that you want to delete and click Delete in the Actions column.

3. In the message that appears, click OK after you verify that the displayed information is correct.

6.1.4. View alert logs

> **Note**
>
> By default, the system saves alert logs of the last 90 days.

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, click **Internal Global Traffic Manager**. On the **Scheduling Instance** tab of the Global Traffic Management on the Internal Network page, click the **Alert Logs** tab.
3. In the alert log list, view address pool information, such as the status of the address pool, health check results of addresses, and switchover between primary and secondary address pools. You can query alert logs of address pools by time or behavior, or by using a keyword.

6.2. Scheduling line management

6.2.1. IP Address Line Configuration

The IP Address Line Configuration tab allows you to define lines based on IP addresses. The lines are used to group request sources to achieve intelligent load balancing.

6.2.1.1. Add a line

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Line Management** > IP Address Line Configuration.

2. Click **Add Line** in the upper-right corner of the line list.

3. In the dialog box that appears, configure the parameters as prompted and click **OK**.

6.2.1.2. Sort lines

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Line Management** > IP Address Line Configuration.

2. Find the line whose sequence you want to change and click **Sort** in the Actions column.
3. Specify Sort Behavior as prompted and click **OK**.

6.2.1.3. Modify the configurations of a line

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Line Management** > IP Address Line Configuration.
2. Find the line whose configurations you want to modify and click **Modify** in the Actions column.
3. Modify the configurations as prompted and click **OK**.

6.2.1.4. Delete a line

1. In the left-side navigation pane, choose **Internal Global Traffic Manager** > **Scheduling Line Management** > **IP Address Line Configuration**.
2. Find the line that you want to delete and click **Delete** in the Actions column.
3. In the message that appears, click **OK**.

6.3. Data synchronization management

Data synchronization management is used to synchronize Global Traffic Manager (GTM) data between clouds.

6.3.1. Synchronization cluster management

Synchronization clusters involve two operations: **Set Emergency Group** and **Merge GTM Control Domain**.

You can perform the following operations to go to the synchronization cluster management page:

1. Log on to the Apsara Stack DNS console.
2. In the left-side navigation pane, choose **Internal Global Traffic Manager**.
3. On the page that appears, click the **Data Synchronization** tab.

Set Emergency Group

You can select some service instances to form a cluster to provide services.

- Enable the emergency group feature: If the synchronization cluster is abnormal, click **Set Emergency Group**. In the Set Emergency Group dialog box, turn on Emergency Group Switch, select available service instances to form an emergency group, and then click **OK**.
- Disable the emergency group feature: If the synchronization cluster is restored to normal, click **Set Emergency Group**. In the Set Emergency Group dialog box, turn off the Emergency Group Switch and click **OK**.

Merge GTM Control Domain

In multi-cloud scenarios, you can click **Merge GTM Control Domain** and enter the IP address of the leader service instance of the merged Global Traffic Manager (GTM) control domain to form a large synchronization cluster.

View the status of the synchronization cluster

You can view the status of the synchronization cluster on the Synchronization Cluster Management tab.

View the service instances in the synchronization cluster

You can view the following information of the service instances in the current synchronization cluster:

Instance IP Address, Instance Role, Status, Latest Synchronization Log ID, IP Address, and Instance Description.

You can also perform the following operations to switch the role of a service instance in the synchronization cluster from follower to leader:

1. Find the service instance with the follower role and click **Switch Primary** in the Actions column.
2. In the message that appears, click **OK**.