ALIBABA CLOUD

Alibaba Cloud

PrivateLink

Quick Start

Document Version: 20220711

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.Use PrivateLink to share services between different VPCs that belong to the same Alibaba Cloud account

This topic describes how to use PrivateLink to allow a instance in a virtual private cloud (VPC) to provide services to another VPC that belongs to the same Alibaba Cloud account.

Context

VPCs are private networks that are isolated from each other. You can use PrivateLink to establish a secure and stable private connection between a VPC and an Alibaba Cloud service. This simplifies the network architecture and prevents security risks over the Internet.

To establish a PrivateLink connection, you must create an endpoint service and an endpoint.

- Endpoint services

  An endpoint service can be accessed by using an endpoint in another VPC over a PrivateLink connection. Endpoint services are created and managed by service providers.

- Endpoints

  An endpoint can be associated with an endpoint service to establish a PrivateLink connection that allows a VPC to access external services. Endpoints are created and managed by service consumers.

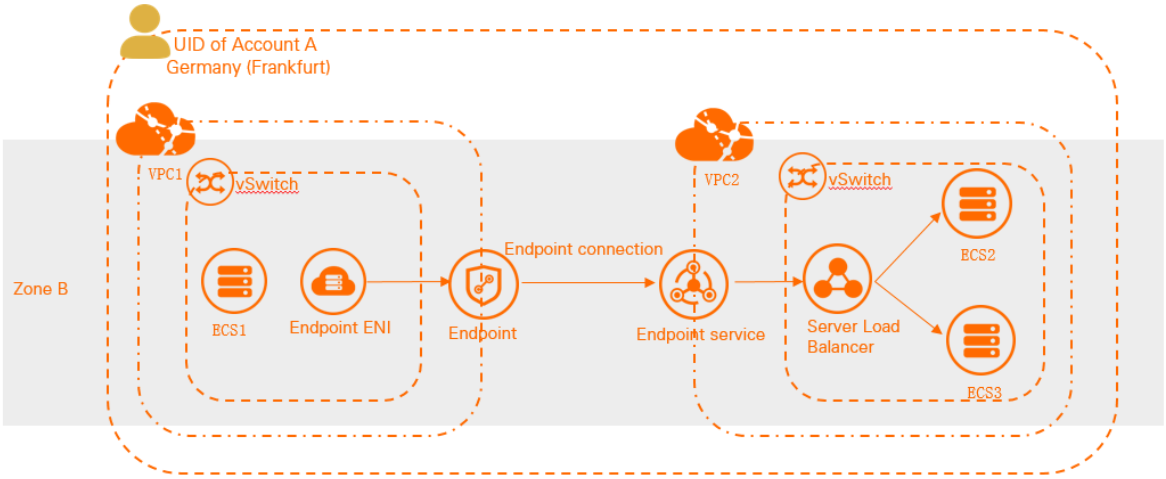
Entity	Description
Service provider	Create and manage endpoint services.
Service consumer	Create and manage endpoints.

Note

Scenarios

The following scenario is used as an example. A company created two VPCs named VPC1 and VPC2 in the Germany (Frankfurt) region with Account A, and deployed services on ECS2 and ECS3 in VPC2. Due to business development, resources in VPC1 require access to the services in VPC2 over a private network.

You can create a instance that supports PrivateLink in VPC2, add ECS2 and ECS3 as backend servers of the instance, create an endpoint service, and then specify the instance as a service resource. Then, you can create an endpoint in VPC1. After the endpoint is created and the connection between the endpoint and the endpoint service works as expected, ECS1 in VPC1 can access the services in VPC2.



The following table shows how CIDR blocks are specified for the VPCs in this example. Make sure that the CIDR blocks do not overlap.

Attribute	VPC1	VPC2
Region	Germany (Frankfurt)	Germany (Frankfurt)
CIDR block	• VPC CIDR block: 10.10.1.0/16 • vSwitch CIDR block: 10.0.0.0/24	• VPC CIDR block: 192.168.2.0/16 • vSwitch CIDR block: 192.168.24.0/24
vSwitch zone	Zone B	Zone B
ECS instance IP address	ECS1 IP address: 10.0.0.182	• ECS2 IP address: 192.168.20.200 • ECS2 IP address: 10.0.0.2

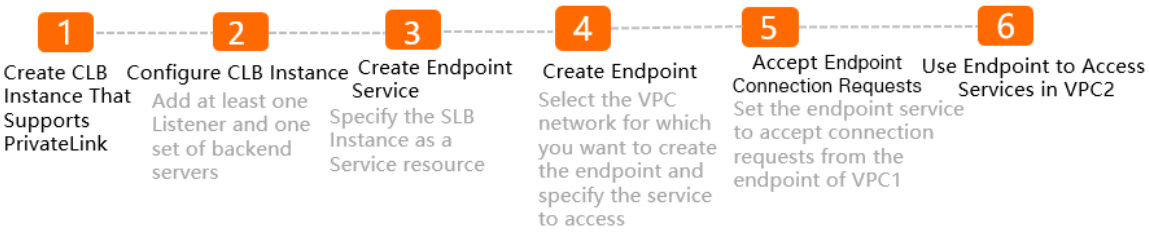
Limits

- The instance that serves as the service resource in VPC2 must be a pay-as-you-go internal-facing instance. Only pay-as-you-go internal-facing instances support PrivateLink.
- The endpoint in VPC1, the endpoint service in VPC2, and the instance that serves as the service resource must be deployed in the same zone of the same region.

Prerequisites

- VPC1 and VPC2 are created in the Germany (Frankfurt) region, and a vSwitch is created for each VPC. For more information, see Create a VPC and a vSwitch.
- ECS1 is created in VPC 1, ECS2 and ECS3 instances are created in VPC 2, and services are deployed on ECS2 and ECS3. For more information, see Create an instance by using the wizard.
- A security group is created in VPC1. For more information, see Create a security group.

Procedure



Step 1: Create an internal-facing CLB instance that supports PrivateLink

1.
2. On the **Instances** page, click **Create CLB**.
3. On the Server Load Balancer page, configure the instance based on the following information and click **Buy Now** to complete the payment.

Parameter	Description
Billing Method	Select a billing method for the CLB instance. In this example, **Pay-As-You-Go** is selected.
SLB region no	Select the region and zone where you want to create the instance. Make sure that the instance is deployed in the same region as the ECS instances that you want to add as backend servers. In this example, **Germany (Frankfurt)** and **Europe Central 1 Zone B** are selected.
Zone Type	Specify whether you want to deploy the CLB instance in one zone or across multiple zones. In this example, **Multi-zone** is selected.
Backup Zone	Select a secondary zone for the instance. Traffic is distributed to the secondary zone only when the primary zone is down. In this example, **Europe Central 1 Zone A** is selected.
Instance Name	Enter a name for the instance. The name must be 1 to 80 characters in length, and can contain letters, digits, hyphens (-), forward slashes (/), periods (.), and underscores (_).
Specification	Select a specification for the CLB instance. CLB instances of different specifications provide different features. In this example, **Small I (slb.s1.small)** is selected.
SLB instance	Specify whether the CLB instance is an Internet-facing or internal-facing instance. In this example, **Intranet** is selected.
Network Type	Select the network type of the instance. In this example, **VPC** is selected.
VPCId	VPC2 and a vSwitch in VPC 2 are selected.
IP Version	Select an IP version for the instance. In this example, **IPv4** is selected.

Parameter	Description
Feature	**Standard** is selected.
Flow out	**By Traffic** is selected.
Quantity	**1** is selected.
Resource Group	**Default Resource Group** is selected.

Step 2: Configure the CLB instance

After the instance is created, you must add at least one listener and one group of backend servers to the CLB instance. This way, traffic can be forwarded by the CLB instance.

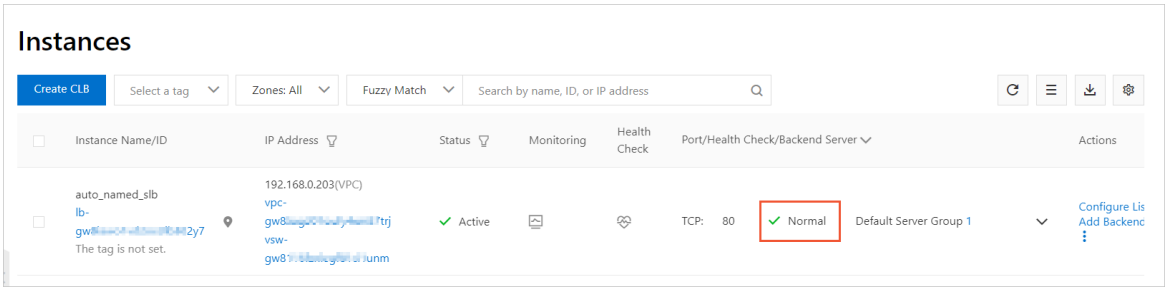
1. On the **Instances** page, find the instance that is created in Step 1 and click **Configure Listener** in the **Actions** column.
2. In the **Protocol and Listener** step, set the following parameters, use the default values for other parameters, and then click **Next**:
   - **Select Listener Protocol**: In this example, **TCP** is selected.
   - **Listening Port**: Specify the frontend port that is used to receive requests and distribute requests to backend servers.

     In this example, *80* is specified.
3. In the **Backend Servers** step, select **Default Server Group** and click **Add More** to add backend servers.
   i. In the **My Servers** panel, select ECS1 and ECS2 that you created, and click **Next**.
   ii. Specify weights for the servers and click **Add**.

   A backend server with a higher weight receives more requests. In this example, the default value 100 is used.
   iii. On the **Default Server Group** tab, specify a backend port and click **Next**. In this example, *80*, is specified.

   You can specify the same port for multiple backend servers of a instance.
4. In the **Health Check** step, configure health checks and click **Next**. In this example, the default values are used.
5. In the **Confirm** step, check the configurations and click **Submit**.
6. Click **OK** to go back to the **Instance** page.

   If the health check status of an ECS instance is **Normal**, the ECS instance is ready to process requests that are forwarded by .



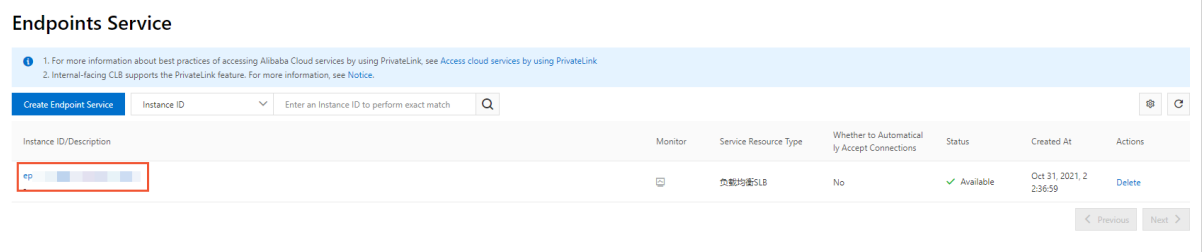
Step 3: Create an endpoint service

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where you want to create an endpoint service. In this example, **Germany (Frankfurt)** is selected.
3. On the **Endpoints Service** page, click **Create Endpoint Service**.
4. On the **Create Endpoint Service** page, set the following parameters and click **OK**.

Parameter	Description
Select Service Resource	Select a zone to distribute network traffic. Then, select the instance to be associated with the endpoint service. In this example, **Frankfurt Zone B** and the instance created in Step 1 that supports PrivateLink are selected.
Automatically Accept Endpoint Connections	Specify whether to automatically accept connection requests from endpoints. In this example, **No** is selected. ○ **Yes**: The endpoint service automatically accepts connection requests from endpoints. Then, the endpoint service can be accessed by using endpoints. ○ **No**: The endpoint connection of the endpoint service is in the **Disconnected** state. In this case, connection requests to the endpoint service must be manually accepted or denied by the service provider. ■ If the service provider accepts the connection request from an endpoint, the endpoint service can be accessed by using the endpoint. ■ If the service provider denies the connection request from an endpoint, the endpoint service cannot be accessed by using the endpoint.
Whether to Enable Zone Affinity	In this example, **Yes** is selected.
Description	Enter a description for the endpoint service. The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

After the endpoint service is created, the account ID of the service provider is automatically added to the whitelist.

You can view the ID and name of the endpoint service on the Endpoints Service page.



Step 4: Create an endpoint

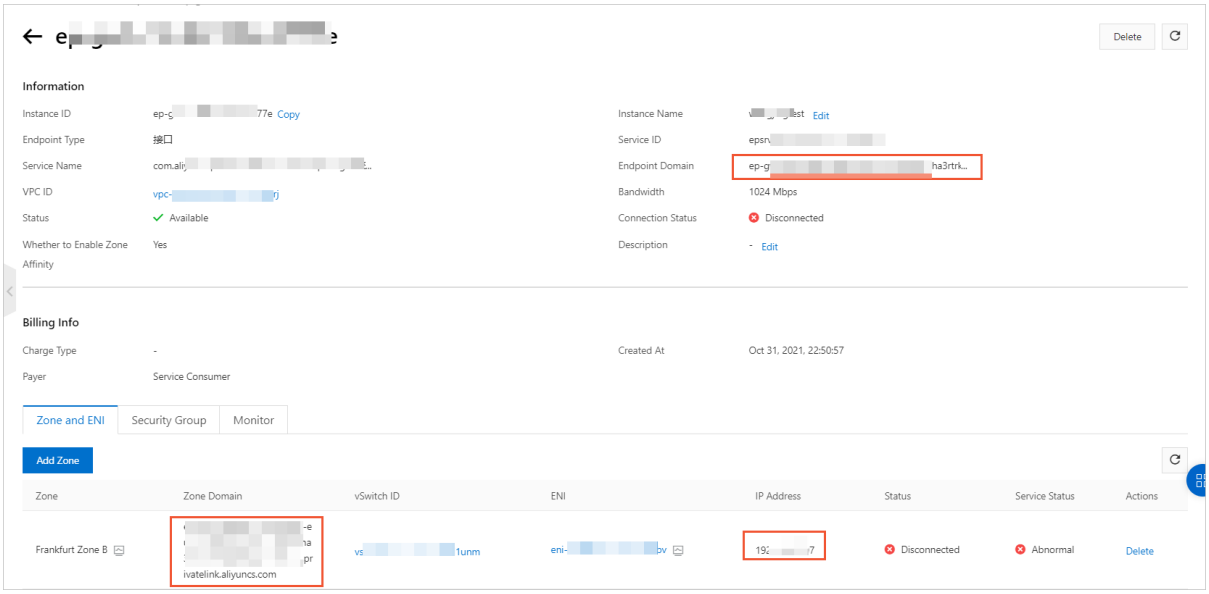
1. Log on to the Endpoint console.
2. In the top navigation bar, select the region where you want to create the endpoint. In this example, **Germany (Frankfurt)** is selected.
3. On the **Endpoints** page, click **Create Endpoint**.
4. On the **Create Endpoint** page, set the following parameters for the endpoint and click **OK**.

Parameter	Description
Endpoint Name	Enter a name for the endpoint. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter.
Endpoints Service	You can associate an endpoint with an endpoint service by using one of the following methods: ○ Click **Add by Service Name** and enter an endpoint service name. ○ Click **Select Service** and select the ID of the endpoint service. In this example, **Add by Service Name** is selected and the endpoint service created in Step 3 is selected.
VPC	Select the VPC where you want to create the endpoint. In this example, VPC1 is selected.
Security Groups	Select the security group to be associated with the endpoint elastic network interface (ENI). The security group is used to control data transfer from the VPC to the endpoint ENI. **Note** Make sure that the rules in the security group allow access to the endpoint ENI from clients.
Zone and vSwitch	Select the zone of the endpoint service and select a vSwitch in the zone. The system automatically creates an endpoint ENI in the vSwitch. In this example, **Frankfurt Zone B** is selected, and the vSwitch in VPC1 is selected.

Parameter	Description
Description	Enter a description for the endpoint. The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

After the endpoint is created, you can view the domain name or IP address that can be used to access the endpoint service. You can access the endpoint service by using one of the following methods:

- Use the domain name of the endpoint
- Use the IP address of the endpoint ENI
- Use the domain name of the zone



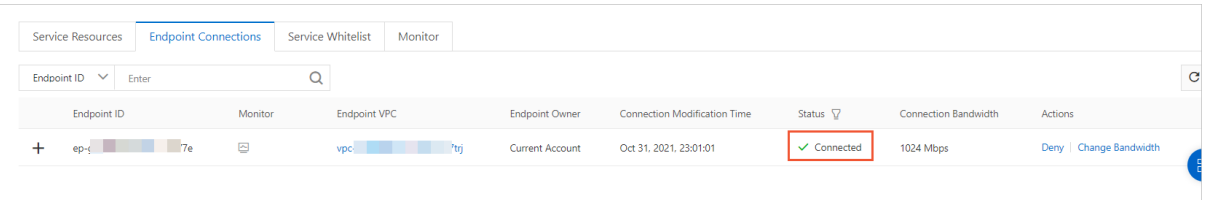
Step 5: Accept connection requests from endpoints

To establish an endpoint connection, an endpoint service must accept the connection request from an endpoint. In this example, resources in VPC1 can access the endpoint service in VPC2 by using the endpoint after the connection request is accepted.

> **Note** Skip this step if you set the Automatically Accept Endpoint Connections parameter to Yes in Step 3.

1. In the left-side navigation pane, click **Endpoints Service**.
2. In the top navigation bar, select the region where the endpoint service is deployed. In this example, **Germany (Frankfurt)** is selected.
3. On the **Endpoints Service** page, find the endpoint service that you created in Step 3, and then click its ID.
4. Click the **Endpoint Connections** tab, find the endpoint from which you want to accept the connection request, and then click **Allow** in the **Actions** column.
5. In the **Allow Connection** message, click **OK**.

After you accept the connection request, the connection status of the endpoint changes from **Disconnected** to **Connected**.



Step 6: Access services by using the endpoint

To test whether ECS1 in VPC1 can access the service deployed on ECS2 in VPC2 by using the endpoint, perform the following operations:

1. Open a browser on ECS1.
2. In the address bar of the browser, enter the domain name or IP address that can be used to access the endpoint service in VPC2, and check whether ECS1 can access the service that is deployed on ECS2.

   In this example, the domain name or IP address that is generated in Step 4 is entered.

   The test result shows that ECS1 in VPC1 can access the service deployed on ECS2 in VPC2.

2.Access services in a VPC that belongs to another account

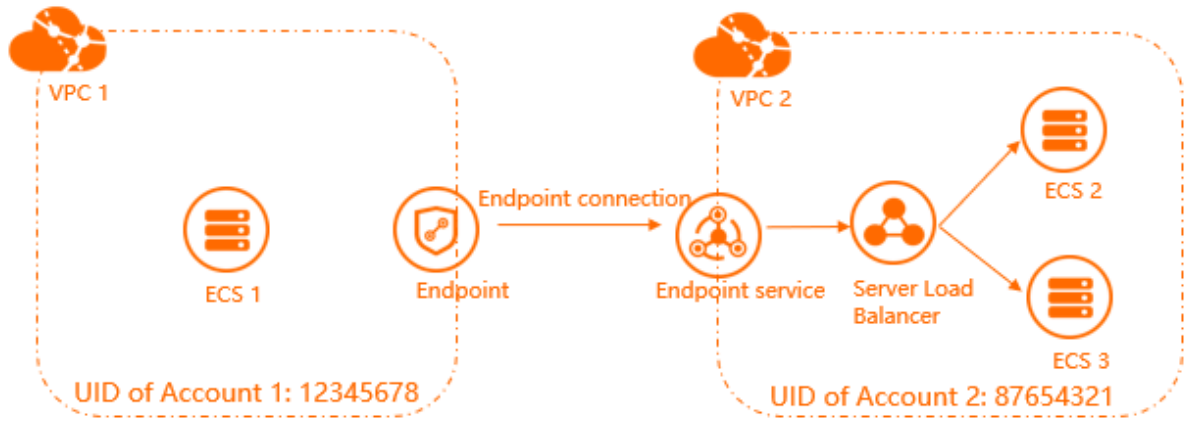
This topic describes how to use PrivateLink to enable a virtual private cloud (VPC) to access an internal-facing instance in a VPC that belongs to another Alibaba Cloud account.

Context

Scenario

The following scenario is used as an example. Two Alibaba Cloud accounts are created: Account A and Account B. VPC1 is created by using Account A and VPC2 is created by using Account B. Application services are deployed on Elastic Compute Service (ECS) instances in VPC2. The ECS instances in VPC2 are referred to as ECS2 and ECS3. Due to business growth, VPC1 needs to access services in VPC2 through a private connection to prevent security risks over the Internet.

In this scenario, you can perform the following operations: Create a CLB instance that supports PrivateLink in VPC2. Specify ECS2 and ECS3 as the backend servers of the CLB instance. Create an endpoint service in VPC2. Specify the CLB instance as the service resource of the endpoint service. Add the UID of Account A to the service whitelist of the endpoint service. Create an endpoint for VPC1. After the endpoint is created and connected to the endpoint service in VPC2, VPC1 can access the services in VPC2 if the status of the private connection is normal.



Limits

- The instance that serves as the service resource in VPC2 must be a pay-as-you-go internal-facing instance. Only pay-as-you-go internal-facing instances support PrivateLink.
- The endpoint in VPC1, the endpoint service in VPC2, and the instance that serves as the service resource must be deployed in the same zone of the same region.

Prerequisites

Before you start, make sure that the following requirements are met:

- Alibaba Cloud accounts are created. To create an Alibaba Cloud account, see create an Alibaba Cloud account.
- If this is your first time using PrivateLink, log on to the Activation page to activate PrivateLink.
- VPC1 and VPC2 are created in the Germany (Frankfurt) region, and a vSwitch is created for each VPC.

For more information, see Create a VPC and a vSwitch.

- ECS1 is created in VPC1. ECS2 and ECS3 are created in VPC2. Application services are deployed on ECS2 and ECS3. For more information, see Create an instance by using the wizard.
- A security group is created in VPC1. For more information, see Create a security group.

Procedure

Step 1: Create an internal-facing CLB instance that supports PrivateLink

To create an internal-facing CLB instance that supports PrivateLink, perform the following operations:

1. Log on to the CLB console with Account B.
2. On the **Instances** page, click **Create CLB**.
3.

Step 2: Configure the CLB instance

After the instance is created, you must add at least one listener and one group of backend servers to the CLB instance. This way, network traffic can be forwarded by the CLB instance.

1. On the **Instances** page, find the instance that is created in Step 1 and click **Configure Listener** in the **Actions** column.
2. On the **Protocol and Listener** wizard page, set the following parameters, use the default values for other parameters, and then click **Next**:
   - **Select Listener Protocol**: In this example, **TCP** is selected.
   - **Listening Port**: Specify the frontend port that is used to receive requests and distribute requests to backend servers.

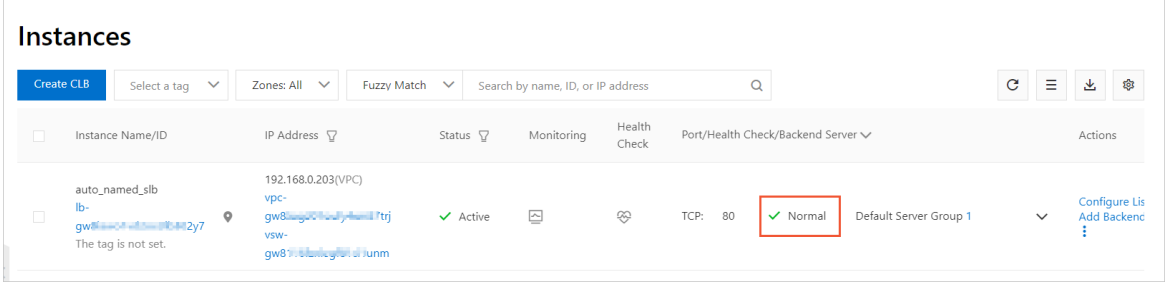
     In this example, *80* is specified.
3. On the **Backend Servers** wizard page, select **Default Server Group** and click **Add More** to add backend servers.
   i. In the **My Servers** panel, select ECS2 and ECS3 and click **Next**.
   ii. Set the weights of the backend servers and click **Add**.

   A backend server with a higher weight receives more requests. In this example, the default value 100 is used.
   iii. On the **Default Server Group** tab, specify a backend port and click **Next**. In this example, *80*, is specified.

   You can specify the same port for multiple backend servers of a instance.
4. On the **Health Check** wizard page, configure health checks and click **Next**. In this example, the default values are used.
5. On the **Confirm** wizard page, check the configurations and click **Submit**.

6. Click **OK** to go back to the **Instances** page.

   If the health status of an ECS instance is **Normal**, the ECS instance can process requests that are forwarded by .



Step 3: Create an endpoint service

After you create an endpoint service in a VPC, you can use an endpoint that is deployed in another VPC to access the endpoint service through PrivateLink connections.

1. Log on to the Endpoint Service console with Account B.
2.
3.
4. On the **Create Endpoint Service** page, set the following parameters and click **OK**.

Parameter	Description
Select Service Resource	Select a zone to distribute network traffic. Then, select the instance to be associated with the endpoint service. In this example, **Frankfurt Zone B** and the instance created in Step 1 that supports PrivateLink are selected.
Automatically Accept Endpoint Connections	Specify whether to automatically accept connection requests from endpoints. In this example, **No** is selected. ○ **Yes**: The endpoint service automatically accepts connection requests from endpoints. Then, the endpoint service can be accessed by using endpoints. ○ **No**: The endpoint connection of the endpoint service is in the **Disconnected** state. In this case, connection requests to the endpoint service must be manually accepted or denied by the service provider. ■ If the service provider accepts the connection request from an endpoint, the endpoint service can be accessed by using the endpoint. ■ If the service provider denies the connection request from an endpoint, the endpoint service cannot be accessed by using the endpoint.
Whether to Enable Zone Affinity	In this example, **Yes** is selected.

Parameter	Description
Description	Enter a description for the endpoint service. The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

After the endpoint service is created, you can view the ID and name of the endpoint service.

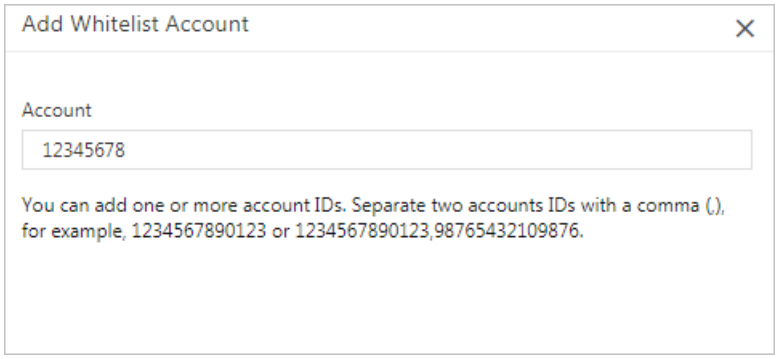
Step 4: Configure a whitelist for the endpoint service

You can configure a whitelist for an endpoint service. If the UID of your account is in the whitelist, you can use your account to create an endpoint and use the endpoint to connect to the endpoint service.

To add the UID of Account A to the whitelist of the endpoint service of Account B, perform the following operations:

1. Log on to the Endpoint Service console with Account B.
2. In the left-side navigation pane, click **Endpoints Service**.
3. On the **Endpoints Service** page, find the endpoint service that you created in Step 3, and then click its ID.
4. On the **Service Whitelist** tab, click **Add Whitelist Account**.
5. In the **Add Whitelist Account** dialog box, enter the account IDs that you want to add to the whitelist, and then click **OK**.

   In this example, the UID of Account A is entered.



Step 5: Create an endpoint

You can associate an endpoint with an endpoint service to establish a PrivateLink connection that allows a VPC to access external services.

1. Log on to the Endpoint Service console with Account A
2.
3.
4. On the **Create Endpoint** page, set the following parameters and click **OK**.

Parameter	Description

Parameter	Description
Endpoint Name	Enter a name for the endpoint. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter.
Endpoints Service	You can associate an endpoint with an endpoint service by using one of the following methods: ○ Click **Add by Service Name** and enter an endpoint service name. ○ Click **Select Service** and select the ID of the endpoint service. In this example, **Add by Service Name** is selected and the endpoint service created in Step 3 is selected.
VPC	Select the VPC where you want to create the endpoint. In this example, VPC1 is selected.
Security Groups	Select the security group to be associated with the endpoint elastic network interface (ENI). The security group is used to control data transfer from the VPC to the endpoint ENI. **Note** Make sure that the rules in the security group allow access to the endpoint ENI from clients.
Zone and vSwitch	Select the zone of the endpoint service and select a vSwitch in the zone. The system automatically creates an endpoint ENI in the vSwitch. In this example, **Frankfurt Zone B** is selected, and the vSwitch in VPC1 is selected.
Description	Enter a description for the endpoint. The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

Step 6: Accept connection requests from the endpoint

After you create an endpoint for VPC1, you must configure the endpoint service to allow connection requests from the endpoint. This way, VPC1 can use the endpoint to access the endpoint service in VPC2.

Note Skip this step if you set the Automatically Accept Endpoint Connections parameter to Yes in Step 3.

To allow the endpoint service of Account B to accept connection requests from the endpoint of Account A, perform the following operations:

1. Log on to the Endpoint Service console with Account B.
2. In the top navigation bar, select the region where the endpoint service is deployed. In this example,

Germany (Frankfurt) is selected.

3. On the **Endpoints Service** page, find the endpoint service that you created in Step 3 and click its ID.
4. Click the **Endpoint Connections** tab, find the endpoint created in Step 5 and click **Allow** in the **Actions** column.
5. In the **Allow Connection** message, click **OK**.

After you set the endpoint service to accept connection requests from the endpoint, the connection status of the endpoint changes from **Disconnected** to **Connected**.

Step 7: Use the endpoint to access services that are deployed in VPC2

To test whether ECS1 can access the services deployed on ECS2 by using the endpoint, perform the following operations:

1. Open a browser on ECS1.
2. In the address bar of the browser, enter the domain name or IP address that is used to access services on ECS2.

   In this example, the domain name or IP address that is generated in Step 5 is entered.

   The test result shows that ECS1 can access the services deployed on ECS2.

3.Specify an ALB instance as a service resource in PrivateLink

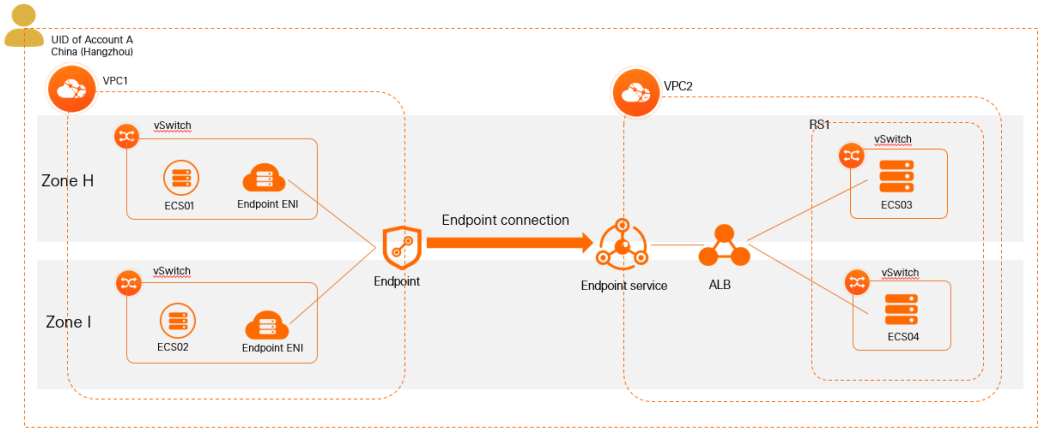
PrivateLink allows you to specify instances as the service resources of endpoint services. instances support cross-zone deployment. After you specify an instance as the service resource of an endpoint service, the instance can serve your workloads across multiple zones. You do not need to configure an instance for each zone.

Context

Alibaba Cloud provides two types of instances: and instances. is intended for Layer 7 load balancing, provides ultra-high processing capabilities, and supports content-based routing. You can specify an instance as the service resource in PrivateLink to meet your business requirements. For more information about the differences between and instances, see SLB Overview.

The following scenario is used as an example. You use an Alibaba Cloud account (Account A) to create two virtual private clouds (VPCs) in the China (Hangzhou) region. The VPCs are referred to as VPC1 and VPC2. In addition, you create two Elastic Compute Service (ECS) instances in each VPC. The ECS instances in VPC1 are referred to as ECS01 and ECS02. The ECS instances in VPC2 are referred to as ECS03 and ECS04. Different NGINX services are deployed on the ECS instances in VPC2. Due to business growth, the ECS instances in VPC1 need to access the ECS instances in VPC2.

In this scenario, you must create an instance that supports PrivateLink in VPC2. Make sure that the instance is deployed across Hangzhou Zone H and Hangzhou Zone I. Then, create a server group (RS1) for the ALB instance and add ECS03 and ECS04 to the server group. Create an endpoint service and specify the instance as a service resource of the endpoint service. Create an endpoint in VPC1 and connect the endpoint to the endpoint service. If the status of the connection is normal, the ECS instances in VPC1 can access the ECS instances in VPC2.



Limits

- When you create an instance that supports PrivateLink, make sure that the instance meets the following requirements: The **network type** is **internal-facing** and the **IP address type** is **static**.
- Make sure that the region and zones where you want to deploy the instance support PrivateLink. For more information about the regions and zones that support PrivateLink and the regions and zones that support instances, see Regions and zones that support PrivateLink and Regions and zones that support ALB instances.
- The endpoint and the endpoint service must be deployed in the same zone. In addition, the zone

must be one of the zones where the instance is deployed.

Prerequisites

- To specify an instance as a service resource in PrivateLink, your account must be included in the whitelist. You can or contact customer service to apply for the permissions.
- VPC1 and VPC2 are created in the China (Hangzhou) region. A vSwitch is created in each VPC. For more information, see Create a VPC and a vSwitch.
- ECS01 and ECS02 are created in VPC1. ECS01 is deployed in Zone H. ECS02 is deployed in Zone I. The ECS instances are used to send connection requests. ECS03 and ECS04 are created in VPC2. ECS03 is deployed in Zone H. ECS04 is deployed in Zone I. The ECS instances are used to process connection requests. Different NGINX services are deployed on ECS03 and ECS04. For more information about how to create ECS instances and deploy NGINX services, see Create an instance by using the wizard and Manually deploy an LNMP environment on an ECS instance that runs Alibaba Cloud Linux 2.
- A security group is created in VPC1. The following security rule is configured:
  - An inbound rule that allows Internet Control Message Protocol (ICMP) traffic to support operations such as pinging the ECS instance.
  - An inbound rule that allows traffic on SSH port 22 and Remote Desktop Protocol (RDP) port 3389 to access the ECS instance.
  - Port 80 is used for HTTP requests. Port 443 is used for HTTPS requests. You can enable these ports to allow VPC1 to access VPC2 by sending HTTP or HTTPS requests.

  For more information, see Create a security group.

The following table describes how networks are planned in this example. Your service will not be adversely affected if the CIDR blocks of your VPCs overlap with each other.

Item	VPC1	VPC2
Region	China (Hangzhou)	China (Hangzhou)
CIDR blocks	• VPC: 10.0.0.0/8 • vSwitch 1 CIDR block: 10.0.10.0/24 • vSwitch 2 CIDR block: 10.10.0.0/24	• VPC: 192.168.0.0/16 • vSwitch 1 CIDR block: 192.168.3.0/24 • vSwitch 2 CIDR block: 192.168.5.0/24
vSwitch zones	• vSwitch 1 in Zone H • vSwitch 2 in Zone I	• vSwitch 1 in Zone H • vSwitch 2 in Zone I
ECS instance IP addresses	• ECS01 in Zone H: 10.0.10.3 • ECS02 in Zone I: 10.0.0.27	• ECS03 in Zone H: 192.168.3.190 • ECS04 in Zone I: 192.168.5.20

Procedure

Step 1: Create an internal-facing ALB instance that supports PrivateLink

1.
2. On the **Instances** page, click **Create ALB**.
3. On the **ALB (Pay-As-You-Go) International Site** page, set the following parameters of the instance and click **Buy Now**.

Parameter	Description
Region	Select the region where you want to create the ALB instance. In this example, **China (Hangzhou)** is selected.
Network Type	Select a network type. In this scenario, only **Internal** is supported.
VPC	Select the VPC where you want to deploy the ALB instance. In this example, VPC2 is selected.
Zone	Select the zones where you want to deploy the ALB instance. You must select at least two zones. In this example, **Hangzhou Zone H**, a vSwitch in Hangzhou Zone H, **Hangzhou Zone I**, and a vSwitch in Hangzhou Zone I are selected.
IP Mode	Specify the type of IP address used by the ALB instance. In this example, **Static IP** is selected.
Edition	Select the edition of the ALB instance. In this example, **Basic** is selected.
Instance Name	Enter a name for the ALB instance.
Resource Group	Select the resource group to which the ALB instance belongs. In this example, **Default Resource Group** is selected.

Step 2: Create a server group

1.
2.
3. In the **Create Server Group** dialog box, set the following parameters and click **Create**.

Parameter	Description
Server Group Type	Select the type of server group that you want to create. In this example, **Instance** is selected.
Server Group Name	Enter a name for the server group. In this example, *RS1* is entered.
VPC	Select the VPC to which the backend servers belong. In this example, VPC2 is selected.
Backend Server Protocol	Select a backend protocol. In this example, **HTTP** is selected.

Parameter	Description
Scheduling Algorithm	Select a scheduling algorithm. In this example, **Weighted Round Robin** is selected.
Resource Group	Select the resource group to which the ALB instance belongs.
Session Persistence	Specify whether to enable session persistence. In this example, session persistence is disabled.
Configure Health Check	Specify whether to enable health checks. In this example, health checks are enabled.
Advanced Settings	After you enable health checks, you can click **Modify** next to **Advanced Settings** to configure the advanced settings. In this example, the default advanced settings are used.

4. After you create the server group, find RS1 on the Server Groups page and click its ID.
5. Click the **Backend Servers** tab and click **Add Backend Server**.
6. In the **Add Backend Server** panel, select ECS03 and ECS04 and click **Next**.
7. Set the ports and weights of ECS03 and ECS04. In this example, port *80* and the default weight 100 are set for the ECS instances. Then, click **OK**.

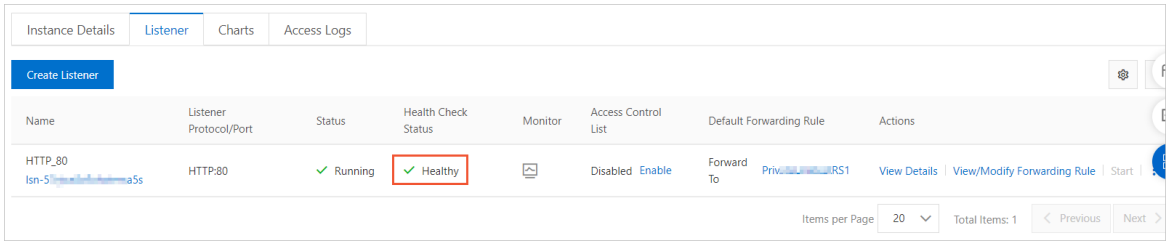
Step 3: Configure a listener

1.
2.
3. On the **Configure Listener** wizard page, set the following parameters and click **Next**.

Parameter	Description
Listener Protocol	Select a listening protocol. In this example, **HTTP** is selected.
Listener Port	Specify the listening port that is used to receive and process requests. In this example, *80* is entered.
Listener Name	Enter a name for the listener.
Advanced Settings	You can click **Modify** to modify the advanced settings. In this example, the default advanced settings are used.

4. On the **Select Server Group** wizard page, select RS1, which is created in Step 2. Then, click **Next**.
5. On the **Confirm** wizard page, confirm the configurations and click **Submit**.
6. In the **ALB Configuration Wizard** message, click **OK**. Then, return to the **Instances** page.

If the health check status of the listener is **Healthy**, it indicates that ECS03 and ECS04 can process requests forwarded by the instance.

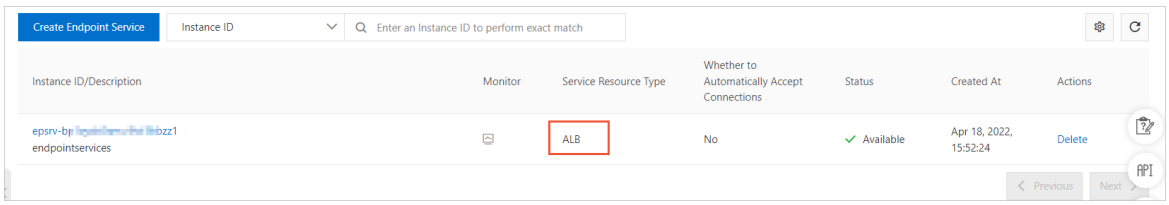


Step 4: Create an endpoint service

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where you want to create an endpoint service. In this example, **China (Hangzhou)** is selected.
3. On the **Endpoints Service** page, click **Create Endpoint Service**.
4. On the **Create Endpoint Service** page, set the following parameters and click **OK**.

Parameter	Description
Service Resource Type	Select the type of service resource to be added to the endpoint service. In this example, **ALB** is selected.
Select Service Resource	Select the zones where the service resource is deployed and then select the service resource. In this example, **Hangzhou Zone H** is selected. Then, click **+Add Resource from Another Zone** and select **Hangzhou Zone I**. For Hangzhou Zone H and Hangzhou Zone I, select the instance that is created in Step 1 as the service resource.
Automatically Accept Endpoint Connections	Specify whether to automatically accept connection requests from endpoints. In this example, **No** is selected.
Whether to Enable Zone Affinity	In this example, **No** is selected.
Description	Enter a description for the endpoint service.

After you create the endpoint service, you can view the endpoint service whose **Service Resource Type** is .



Step 5: Create an endpoint

1. Log on to the Endpoint console.

2. In the top navigation bar, select the region where you want to create the endpoint. In this example, **China (Hangzhou)** is selected.
3. On the **Endpoints** page, click **Create Endpoint**.
4. On the **Create Endpoint** page, set the following parameters of the endpoint and click **OK**.

Parameter	Description
Endpoint Name	Enter a name for the endpoint.
Endpoint Type	Select the type of endpoint that you want to create. In this example, **Interface Endpoint** is selected.
Endpoints Service	You can associate the endpoint with an endpoint service in one of the following ways: ○ Click **Add by Service Name** and enter the name of an endpoint service. ○ Click **Select Service** and select the ID of an endpoint service. In this example, **Select Service** is clicked, and the endpoint service that is created in Step 4 is selected.
VPC	Select the VPC to which the endpoint belongs. In this example, VPC1 is selected.
Security Groups	Select the security group to be associated with the endpoint elastic network interface (ENI). The security group can control network traffic from VPC1 to the endpoint. **Note** Make sure that the rules in the security group allow access to the endpoint ENI.
Zone and vSwitch	Select the zone of the endpoint service and select a vSwitch in the zone. The system automatically creates an endpoint ENI and attaches it to the vSwitch. In this example, **Hangzhou Zone H** is selected and a vSwitch in the zone is selected. Then, click **+Add vSwitch**, select **Hangzhou Zone I**, and then select a vSwitch in the zone.
Description	Enter a description for the endpoint.

After you create the endpoint, you can view the domain names and IP addresses of the zones.

Step 6: Accept connection requests

To establish an endpoint connection, the endpoint service must accept the connection requests from the associated endpoint. Then, VPC1 can use the endpoint to access the endpoint service.

Note Skip this step if you set the Automatically Accept Endpoint Connections parameter to Yes in Step 4.

1.
2. In the top navigation bar, select the region where the endpoint service is deployed. In this example,

China (Hangzhou) is selected.

3. On the **Endpoints Service** page, find the endpoint service created in Step 4 and click its ID.
4. On the details page of the endpoint service, click the **Endpoint Connections** tab, find the endpoint that you want to manage, and then click **Allow** in the **Actions** column.
5. In the **Allow Connection** dialog box, select the **Allow connections and automatically allocate service resources.** check box and click **OK**.

After the connection requests are accepted, the status of the endpoint connection changes from **Disconnected** to **Connected**. Then, the endpoint service can process requests from the endpoint. You can use the domain names and IP addresses of the zones in Step 5 to access the endpoint service.

Step 7: Test network connectivity

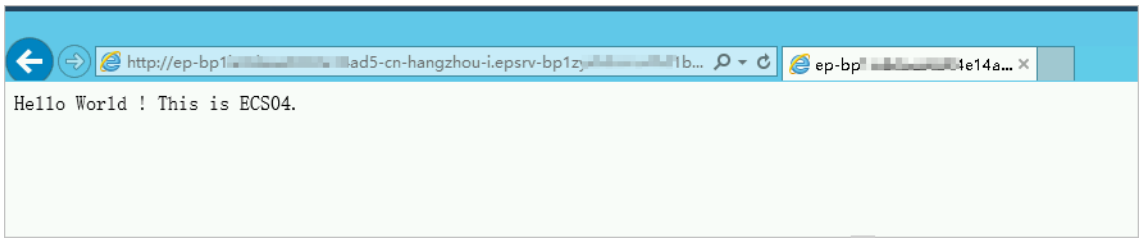
After you perform the preceding operations, VPC1 can access VPC2 through private connections. The following section shows how to test the network connectivity.

> **Note** In this example, the Windows Server 2012 operating system is installed on ECS01 and ECS02. The Alibaba Cloud Linux operating system is installed on ECS03 and ECS04. For more information about how to test the network connectivity of servers that run other operating systems, refer to the user guides of the operating systems.

- Check whether ECS01 in VPC1 can access services on ECS03 in VPC2.
  i. Log on to ECS01. For more information, see Connect to an ECS instance.
  ii. Open a browser on ECS01.
  iii. Enter the domain name or IP address of Zone H from Step 5 in the browser. In this example, the domain name of Zone H is entered. The following figure shows the test result.

  The test result shows that ECS01 can access the services deployed on ECS03.

- Check whether ECS02 in VPC1 can access the services on ECS04 in VPC2.
  i. Log on to ECS02.
  ii. Open a browser on ECS02.
  iii. Enter the domain name or IP address of Zone I from Step 5 in the browser. In this example, the domain name of Zone I is entered. The following figure shows the test result.



  The test result shows that ECS02 can access the services deployed on ECS04.

References

- CreateVpcEndpointService: creates an endpoint service.
- CreateVpcEndpoint: creates an endpoint.
- AttachResourceToVpcEndpointService: adds a service resource to an endpoint service.
- EnableVpcEndpointConnection: accepts connection requests from an endpoint.
- AttachSecurityGroupToVpcEndpoint: adds an endpoint to a security group.