Virtual Private Cloud

Product Documentation

Contents

Virtual Private Cloud 7
- Product Introduction 7
  - VPC Overview 7
  - Strengths 10
  - Use Cases 11
  - Basic Concepts 15
    - IP Addresses 15
    - Region and Availability Zone 18
  - Quota Limitation 19
- Quick Start 21
  - Quickly Building an IPv4 VPC 21
  - Quickly Building an IPv6 VPC 25
- Operation Guide 33
  - Network Planning 33
  - Virtual Private Cloud and Subnet 38
    - Restrictions 38
    - Managing Virtual Private Cloud 39
    - Editing IPv4 CIDR 43
    - Editing IPv6 CIDR 45
    - Managing Subnets 47
    - Enabling or Disabling Multicast 52
  - Route Tables 54
    - Overview 54
    - Restrictions 56
    - Managing Route Tables 57
  - IP and Network Interface 60
    - Elastic Public IP (EIP) 60
    - Managing ENI 61
    - HAVIP 62
      - Overview 62
      - Restrictions 66
      - Creating a High Availability Virtual IP 67
      - Binding or Unbinding EIP 71
      - Querying Highly Available Virtual IP 73
      - Releasing Highly Available Virtual IP 74
  - VPC Connection 75
    - Overview 75
    - Connecting to the Public Network 78
    - Connecting to Other VPCs 81
    - Connecting to Local Data Centers 82
    - VPC Terminal Nodes 83
      - Overview 83
      - Directions 85
      - Endpoint Service 86
      - Endpoint 92
  - Security Management 96
    - Security Groups 96
      - Overview of Security Groups 96
      - Creating Security Group 98
      - Adding Security Group Rule 101
      - Restrictions 104
      - Managing Security Group 105
        - Viewing Security Group 105
        - Remove from Security Group 106
        - Clone Security Group 107
        - Delete Security Group 108
        - Associated Instances 109
      - Managing Security Group Rule 111
        - View Security Group Rules 111
        - Modify Security Group Rule 112
        - Delete Security Group Rule 113
        - Import security group rules 114
        - Export Security Group Rule 115
      - Security Group Use Cases 116
      - Common Server Ports 121
    - Network ACL 123
      - Rule Overview 123
      - Restrictions 127
      - Managing Network ACL 128
    - Parameter Template 132
      - Restrictions 132
      - Managing Parameter Templates 134
    - Cloud Access Management 140
      - CAM Overview 140
      - Authorizable Resource Type 142
      - VPC CAM Policy Examples 145
      - Resource-level Permissions Supported by VPC API Operations 149
  - Network Probing 164
- Best Practice 168
  - Configure the cloud server as a public gateway 168
  - Adjust the Priority of NAT Gateway and EIP 175
  - Building High Availability Primary/Secondary Cluster with HAVIP+Keepalived 176
  - Building High Availability DB with HAVIP+Windows Server Failover Cluster 184
  - Cross-account VPC service sharing via Private Link 185
  - Multicast Communication Scenarios for Dedicated Tunnels 190
- FAQs 195
  - General 195
    - IP range and IP related 195
    - Product Quotas Related 197

- Connection Categories ... 198
  - Connecting to the Public Network ... 198
- Safety Categories ... 200
  - VPC Security Related ... 200
  - Port and security group related ... 201
- API Documentation ... 204
- Virtual Private Cloud (VPC)(vpc) ... 204
  - version(2017-03-12) ... 204
    - API overview ... 204
    - CallingMethod ... 216
      - signaturev1 ... 216
      - signaturev3 ... 224
      - request ... 233
      - result ... 234
      - PublicParameter ... 237
    - CCN APIs ... 239
      - AcceptAttachCcnInstances ... 239
      - AttachCcnInstances ... 241
      - DescribeCcnAttachedInstances ... 243
      - DescribeCcnRegionBandwidthLimits ... 244
      - DescribeCcnRoutes ... 246
      - DetachCcnInstances ... 248
      - RejectAttachCcnInstances ... 250
      - SetCcnRegionBandwidthLimits ... 252
    - Direct Connect Gateway APIs ... 253
      - CreateDirectConnectGateway ... 253
      - CreateLocalDestinationIpPortTranslationNatRule ... 254
      - CreateLocalIpTranslationAclRule ... 256
      - CreateLocalIpTranslationNatRule ... 258
      - CreateLocalSourceIpPortTranslationAclRule ... 260
      - CreateLocalSourceIpPortTranslationNatRule ... 262
      - DeleteDirectConnectGateway ... 264
      - DeleteLocalDestinationIpPortTranslationNatRule ... 266
      - DeleteLocalIpTranslationAclRule ... 268
      - DeleteLocalIpTranslationNatRule ... 271
      - DeleteLocalSourceIpPortTranslationAclRule ... 273
      - DeleteLocalSourceIpPortTranslationNatRule ... 275
      - DescribeDirectConnectGateways ... 277
      - DescribeLocalDestinationIpPortTranslationNatRules ... 279
      - DescribeLocalIpTranslationAclRules ... 281
      - DescribeLocalIpTranslationNatRules ... 283
      - DescribeLocalSourceIpPortTranslationAclRules ... 285
      - DescribeLocalSourceIpPortTranslationNatRules ... 287
      - DescribePeerIpTranslationNatRules ... 289
      - ModifyDirectConnectGatewayAttribute ... 291
      - ModifyLocalDestinationIpPortTranslationNatRule ... 292
      - ModifyLocalIpTranslationAclRule ... 295
      - ModifyLocalIpTranslationNatRule ... 297
      - ModifyLocalSourceIpPortTranslationAclRule ... 300
      - ModifyLocalSourceIpPortTranslationNatRule ... 302
      - ModifyPeerIpTranslationNatRule ... 304
    - ENI APIs ... 307
      - AssignIpv6Addresses ... 307
      - AssignPrivateIpAddresses ... 308
      - AssociateNetworkInterfaceSecurityGroups ... 309
      - AttachNetworkInterface ... 310
      - CreateAndAttachNetworkInterface ... 312
      - CreateNetworkInterface ... 313
      - DeleteNetworkInterface ... 314
      - DescribeNetworkInterfaceLimit ... 316
      - DescribeNetworkInterfaces ... 318
      - DescribeNetworkInterfacesEx ... 319
      - DetachNetworkInterface ... 321
      - DisassociateNetworkInterfaceSecurityGroups ... 323
      - MigrateNetworkInterface ... 324
      - MigratePrivateIpAddress ... 326
      - ModifyIpv6AddressesAttribute ... 328
      - ModifyNetworkInterfaceAttribute ... 330
      - ModifyPrivateIpAddressesAttribute ... 331
      - UnassignIpv6Addresses ... 333
      - UnassignPrivateIpAddresses ... 335
    - Elastic IP APIs ... 337
      - AllocateAddresses ... 337
      - AssociateAddress ... 338
      - DescribeAddressQuota ... 339
      - DescribeAddresses ... 341
      - DescribeNetworkInterfaceExtendIps ... 342
      - DescribeTaskResult ... 344
      - DisassociateAddress ... 346
      - ModifyAddressAttribute ... 348
      - ModifyAddressesBandwidth ... 350
      - ModifyNetworkInterfaceExtendIp ... 352
      - ReleaseAddresses ... 354
      - TransformAddress ... 356
    - Elastic IPv6 APIs ... 357
      - AllocateIp6AddressesBandwidth ... 357
      - DescribeIp6Addresses ... 358
      - ModifyIp6AddressesBandwidth ... 359
      - ReleaseIp6AddressesBandwidth ... 360
    - Gateway Traffic Monitoring APIs ... 361
      - DescribeGatewayFlowQos ... 361

- DisableGatewayFlowMonitor ... 363
- EnableGatewayFlowMonitor ... 365
- ModifyGatewayFlowQos ... 367
- High Availability Virtual IP APIs ... 369
  - CreateHaVip ... 369
  - DeleteHaVip ... 370
  - DescribeHaVips ... 372
  - HaVipAssociateAddressIp ... 374
  - HaVipDisassociateAddressIp ... 376
  - ModifyHaVipAttribute ... 377
- IPv6 Translation Service APIs ... 379
  - AddIp6Rules ... 379
  - CreateIp6Translators ... 381
  - DeleteIp6Translators ... 383
  - DescribeIp6TranslatorQuota ... 385
  - DescribeIp6Translators ... 386
  - ModifyIp6Rule ... 387
  - ModifyIp6Translator ... 389
  - RemoveIp6Rules ... 391
- NAT Gateway APIs ... 392
  - AssociateNatGatewayAddress ... 392
  - CreateNatGateway ... 393
  - CreateNatGatewayDestinationIpPortTranslationNatRule ... 395
  - CreateNatGatewaySourceIpTranslationNatRule ... 396
  - DeleteNatGateway ... 398
  - DeleteNatGatewayDestinationIpPortTranslationNatRule ... 400
  - DeleteNatGatewaySourceIpTranslationNatRule ... 401
  - DescribeNatGatewayDestinationIpPortTranslationNatRules ... 403
  - DescribeNatGatewaySourceIpTranslationNatRules ... 405
  - DescribeNatGateways ... 407
  - DisassociateNatGatewayAddress ... 409
  - ModifyNatGatewayAddressStatus ... 411
  - ModifyNatGatewayAttribute ... 413
  - ModifyNatGatewayDestinationIpPortTranslationNatRule ... 414
  - ModifyNatGatewaySourceIpTranslationNatRule ... 415
  - ResetNatGatewayConnection ... 417
- Network ACL APIs ... 418
  - AssociateNetworkAclSubnets ... 418
  - CreateNetworkAcl ... 420
  - DeleteNetworkAcl ... 422
  - DescribeNetworkAcls ... 424
  - DisassociateNetworkAclSubnets ... 425
  - ModifyNetworkAclAttribute ... 427
  - ModifyNetworkAclEntries ... 429
- Network Parameter Template APIs ... 431
  - CreateAddressTemplate ... 431
  - CreateAddressTemplateGroup ... 432
  - CreateServiceTemplate ... 434
  - CreateServiceTemplateGroup ... 435
  - DeleteAddressTemplate ... 437
  - DeleteAddressTemplateGroup ... 439
  - DeleteServiceTemplate ... 441
  - DeleteServiceTemplateGroup ... 443
  - DescribeAddressTemplateGroups ... 445
  - DescribeAddressTemplates ... 447
  - DescribeServiceTemplateGroups ... 449
  - DescribeServiceTemplates ... 451
  - DescribeTemplateLimits ... 453
  - ModifyAddressTemplateAttribute ... 455
  - ModifyAddressTemplateGroupAttribute ... 457
  - ModifyServiceTemplateAttribute ... 459
  - ModifyServiceTemplateGroupAttribute ... 460
- Network Probe APIs ... 462
  - CheckNetDetectState ... 462
  - CreateNetDetect ... 463
  - DeleteNetDetect ... 465
  - DescribeNetDetectStates ... 467
  - DescribeNetDetects ... 469
  - ModifyNetDetect ... 471
- Other APIs ... 473
  - CreateVpcEndPoint ... 473
  - DescribeGatewayFlowMonitorDetail ... 476
- Peering Connection APIs ... 477
  - AcceptVpcPeeringConnection ... 477
  - AcceptVpcPeeringConnectionEx ... 479
  - CreateVpcPeeringConnection ... 481
  - CreateVpcPeeringConnectionEx ... 483
  - DeleteVpcPeeringConnection ... 485
  - DeleteVpcPeeringConnectionEx ... 487
  - EnableVpcPeeringConnection ... 489
  - EnableVpcPeeringConnectionEx ... 491
  - ModifyVpcPeeringConnection ... 493
  - ModifyVpcPeeringConnectionEx ... 495
  - RejectVpcPeeringConnection ... 497
  - RejectVpcPeeringConnectionEx ... 499
- Private Link APIs ... 501
  - CreateVpcEndPointService ... 501
  - CreateVpcEndPointServiceWhiteList ... 503
  - DeleteVpcEndPoint ... 505
  - DeleteVpcEndPointService ... 507
  - DeleteVpcEndPointServiceWhiteList ... 509

- DescribeVpcEndPoint ... 511
- DescribeVpcEndPointService ... 513
- DescribeVpcEndPointServiceWhiteList ... 515
- DisassociateVpcEndPointSecurityGroups ... 517
- EnableVpcEndPointConnect ... 519
- EnableVpcEndPointConnection ... 521
- ModifyVpcEndPointAttribute ... 523
- ModifyVpcEndPointServiceAttribute ... 525
- ModifyVpcEndPointServiceWhiteList ... 527

• Routing Table APIs ... 529
- CreateIpv6Routes ... 529
- CreateRouteTable ... 531
- CreateRoutes ... 532
- DeleteIpv6Routes ... 534
- DeleteRouteTable ... 536
- DeleteRoutes ... 538
- DescribeRouteConflicts ... 540
- DescribeRouteTables ... 542
- DisableRoutes ... 544
- EnableRoutes ... 546
- ModifyIpv6Routes ... 548
- ModifyRouteTableAttribute ... 550
- ReplaceRouteTableAssociation ... 552
- ReplaceRoutes ... 553
- ResetRoutes ... 555

• Security Group APIs ... 557
- CreateDefaultSecurityGroup ... 557
- CreateSecurityGroup ... 559
- CreateSecurityGroupPolicies ... 561
- CreateSecurityGroupWithPolicies ... 563
- DeleteSecurityGroup ... 565
- DeleteSecurityGroupPolicies ... 566
- DescribeDBInstancesWithSecurityGroup ... 567
- DescribeSecurityGroupAssociationStatistics ... 569
- DescribeSecurityGroupLimits ... 570
- DescribeSecurityGroupPolicies ... 572
- DescribeSecurityGroupReferences ... 574
- DescribeSecurityGroups ... 576
- ModifySecurityGroupAttribute ... 577
- ModifySecurityGroupPolicies ... 578
- ReplaceSecurityGroupPolicy ... 579

• Subnet APIs ... 580
- AssignIpv6SubnetCidrBlock ... 580
- CheckDefaultSubnet ... 582
- CheckIpInSubnet ... 583
- CreateSubnet ... 585
- CreateSubnets ... 587
- DeleteSubnet ... 588
- DescribeSubnets ... 589
- ModifySubnetAttribute ... 591
- UnassignIpv6SubnetCidrBlock ... 593

• VPC APIs ... 595
- AssignIpv6CidrBlock ... 595
- AttachClassicLinkVpc ... 597
- CheckAssistantCidr ... 599
- CreateAssistantCidr ... 601
- CreateDefaultVpc ... 603
- CreateLocalGateway ... 605
- CreateVpc ... 607
- DeleteAssistantCidr ... 609
- DeleteLocalGateway ... 611
- DeleteVpc ... 613
- DescribeAccountAttributes ... 614
- DescribeAssistantCidr ... 616
- DescribeClassicLinkInstances ... 618
- DescribeIpv6Section ... 620
- DescribeIpv6Vpc ... 622
- DescribeLocalGateway ... 624
- DescribeNmsCidrs ... 625
- DescribeUsedIpAddress ... 627
- DescribeVpcInstances ... 628
- DescribeVpcIpv6Addresses ... 630
- DescribeVpcLimits ... 632
- DescribeVpcPrivateIpAddresses ... 634
- DescribeVpcs ... 636
- DetachClassicLinkVpc ... 638
- ModifyAssistantCidr ... 639
- ModifyLocalGateway ... 641
- ModifyVpcAttribute ... 643
- ResetHaVip ... 644
- UnassignIpv6CidrBlock ... 646

• VPN Gateway APIs ... 648
- CreateCustomerGateway ... 648
- CreateGatewayVpnSSLClient ... 649
- CreateVpnConnection ... 651
- CreateVpnGateway ... 652
- CreateVpnGatewaySSLServer ... 653
- DeleteCustomerGateway ... 654
- DeleteVpnConnection ... 655
- DeleteVpnGateway ... 657
- DeleteVpnGatewaySSLClient ... 659

- DeleteVpnGatewaySSLServer 661
- DescribeCustomerGatewayVendors 663
- DescribeCustomerGateways 665
- DescribeVpcResourceDashboard 666
- DescribeVpnConnections 668
- DescribeVpnGatewayCcnRoutes 669
- DescribeVpnGatewaySSLClients 671
- DescribeVpnGatewaySSLServers 674
- DescribeVpnGateways 677
- DisableVpnGatewaySSLClientCert 678
- DownloadCustomerGatewayConfiguration 680
- DownloadVpnGatewaySSLClientCert 681
- EnableVpnGatewaySSLClientCert 683
- InquiryPriceCreateVpnGateway 685
- InquiryPriceResetVpnGatewayInternetMaxBandwidth 686
- ModifyCustomerGatewayAttribute 687
- ModifyVpnConnectionAttribute 688
- ModifyVpnGatewayAttribute 689
- ModifyVpnGatewayCcnRoutes 690
- ModifyVpnGatewaySSLClient 692
- ResetVpnConnection 694
- ResetVpnGatewayInternetMaxBandwidth 696

- Data structure 697
- ErrorCode 725

Product Introduction
VPC Overview

VPC is a logically isolated network space you can custom on the cloud. Similar to the traditional network running in your data center, services hosted within a VPC include CVMs, CLB, cloud databases, and more.

This document introduces the core components of a VPC, various connection methods, and security aspects of a VPC.

Core Components

A VPC has three core components: VPC IP range, subnet, and route table.

VPC IP Range

When you create a VPC, you need to use CIDR (Classless Inter-Domain Routing) to designate the IP address group for the VPC.

VPC supports IPv4 CIDR blocks in any of the following private IP ranges:

- 10.0.0.0-10.255.255.255 (The mask range must be between 16 and 28.)
- 172.16.0.0-172.31.255.255 (The mask range must be between 16 and 28.)
- 192.168.0.0-192.168.255.255 (The mask range must be between 16 and 28.)
- Non-standard IPv4 private IP ranges (The mask range must be between 16 and 28.)

> Note:
>
> From 2020-09-16, VPC started supporting non-standard IPv4 private IP ranges (which are not covered by the three major private IP ranges defined in RFC 1918). If needed, please submit a ticket to apply.

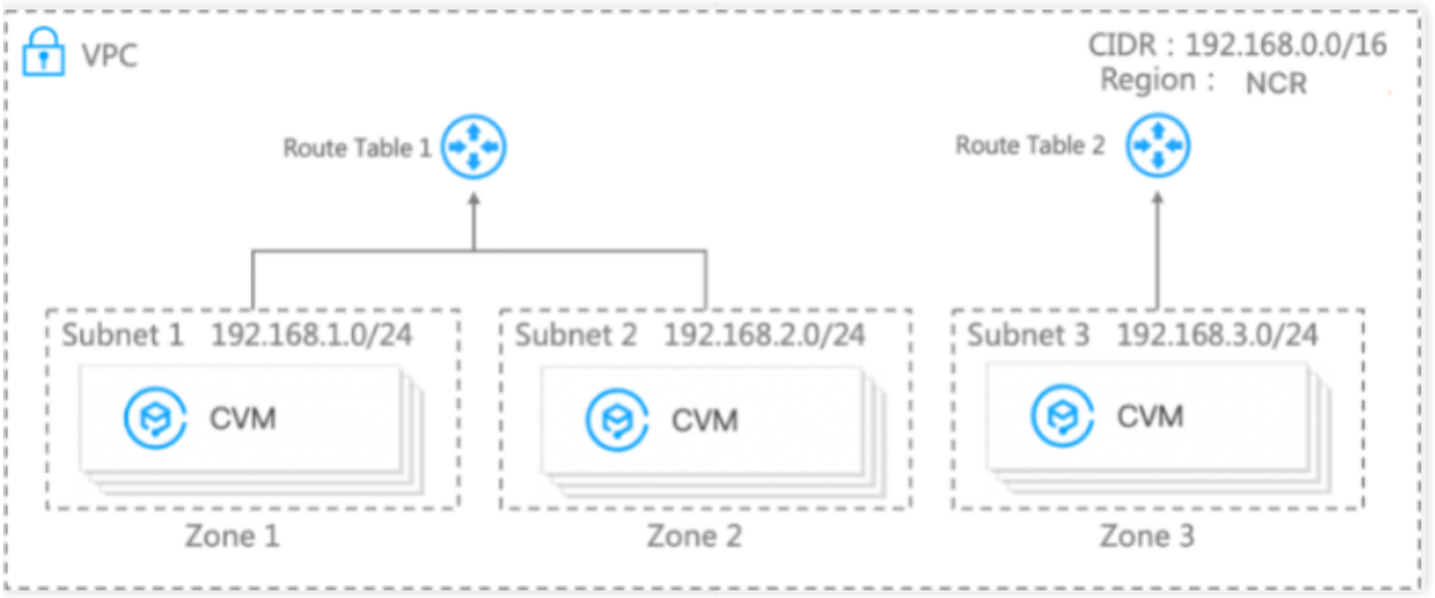
Subnet

A VPC consists of at least one subnet, and the CIDR of the subnet must be within the CIDR of the VPC.

A subnet is a network used to manage the network plane of elastic CVM and can provide services such as IP address management and DNS. All cloud resources in the VPC such as Cloud Virtual Machine (CVM), Cloud Database (CDB), etc. must be deployed in the subnet.

A VPC has region attributes (e.g., NCR), while a subnet has availability zone attributes (e.g., Availability Zone 1). Subnets within a VPC can belong to different availability zones within the same region. Resources within subnets of the same VPC can communicate with each other over a private network regardless of whether they are in the same availability zone or not.

Elastic CVMs in different VPCs can communicate by creating a peering connection.



Route Tables

A route table consists of multiple routing policies that control the outbound traffic direction of subnets in the VPC. Each subnet can only be associated with one route table, while each route table can be associated with multiple subnets. You can create multiple route tables for subnets with different traffic routes.

A route table controls traffic routes by using routing policies. A routing policy consists of the destination, next hop type, and next hop:

- Destination: Specifies the destination IP range to which you want to forward the traffic. It should be an IP range. If you want to enter a single IP address, set the mask to 32 (for example, 172.16.1.1/32). The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.
- Next hop type: Indicates the egress of data packets for the VPC. The next hop type of VPC supports NAT Gateway, Peering Connection, VPN Gateway, Direct Connect Gateway, CVM, and others.
- Next hop: Specifies the next hop instance (identified by the next hop ID) to which the traffic is forwarded, such as a NAT gateway in the VPC.

VPC Connection

The cloud platform offers a wide range of VPC connection solutions to meet different scenario needs:

- CVM and CloudDB instances in a VPC can connect to the public network via an EIP or NAT gateway.
- Through peering connections, different VPCs can communicate with each other.
- Through VPN connections, Direct Connect, VPCs, and local data centers can be interconnected.

- Through private links, VPCs are provided the ability to access other VPCs across accounts via the private network.

VPC Security

VPCs are logically isolated network spaces on the cloud, and different VPCs are isolated from each other, ensuring the security of your business:

- Security Group: A security group is a stateful virtual firewall for filtering packets. As an important means of network security isolation, it can be used to control the outbound and inbound traffic for instances.
- Network ACL: A network ACL is a stateless virtual firewall for filtering packets at the subnet level. It can be used to control the inbound and outbound data streams for subnets at the protocol and port granularities.
- Cloud Access Management (CAM): CAM provides secure management of access rights to all resources under a cloud account. Through CAM, you can manage the access rights to VPCs, for example, by controlling user access to VPCs through identity management and policy management.

Strengths

Custom network

The VPC offers you powerful network management capabilities. You can customize the IP range, divide subnets on demand just like in a traditional network, and customize the deployment of your cloud-based business through the flexible configuration of the route table and route rules.

VPC also offers a visual network topology to help you better plan your network.

Scalability

Using VPCs, you can flexibly deploy according to business needs by creating different subnets within one or multiple VPCs to deploy different parts of the business. You can also expand the network architecture as needed by connecting VPCs with your local data center and other VPCs.

Rich Access

VPC provides different access modes to meet the needs for cloud communications:

- Accessing the Internet: You can interact with the Internet using normal public IP, EIP, NAT gateway, CLB, etc.
- Accessing other VPCs: You can use peering connections to enable inter-VPC communication; cross-VPC unilateral service access is achieved through a private link.
- Accessing the local data center: You can use VPN connections and DC access to access your local data center.

Security and Reliability

VPC utilizes tunnel technology to build virtual networks on top of physical ones, using the GRE protocol to ensure complete isolation between VPCs, offering users independent, isolated, and secure cloud networks. For CVMs within the VPC, we also provide different levels of network access control, such as security groups and Network ACLs.

Simple and easy to use

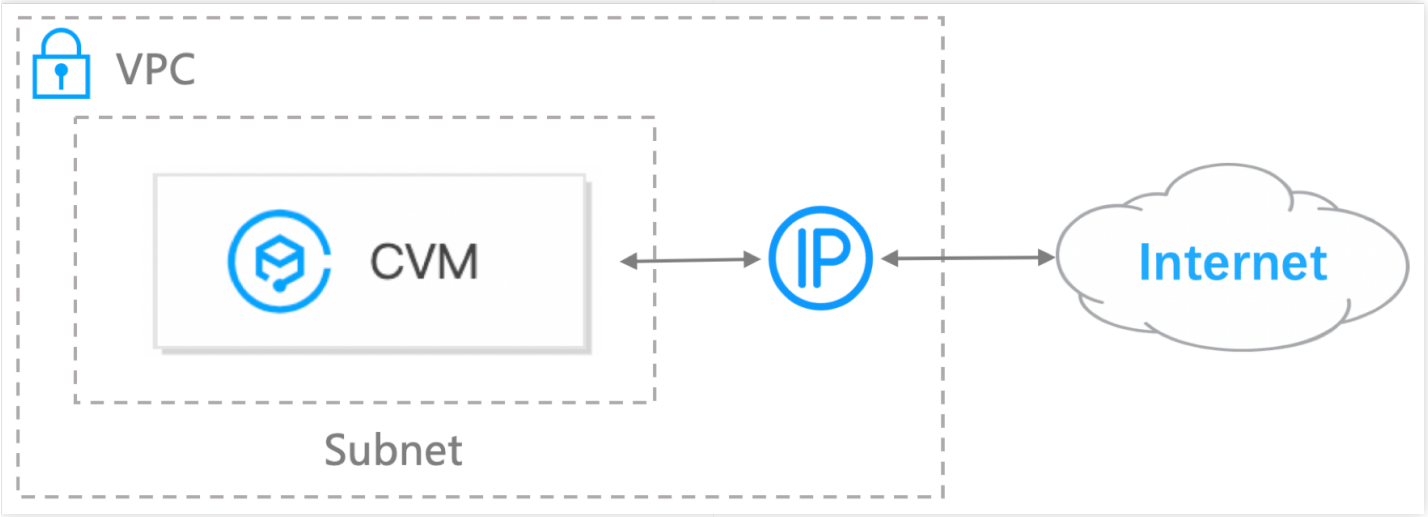
You can quickly create and manage VPC through methods such as the console and API. The productized network functions and rich troubleshooting features can significantly reduce your operation and maintenance costs.

Use Cases

Accessing Public Network

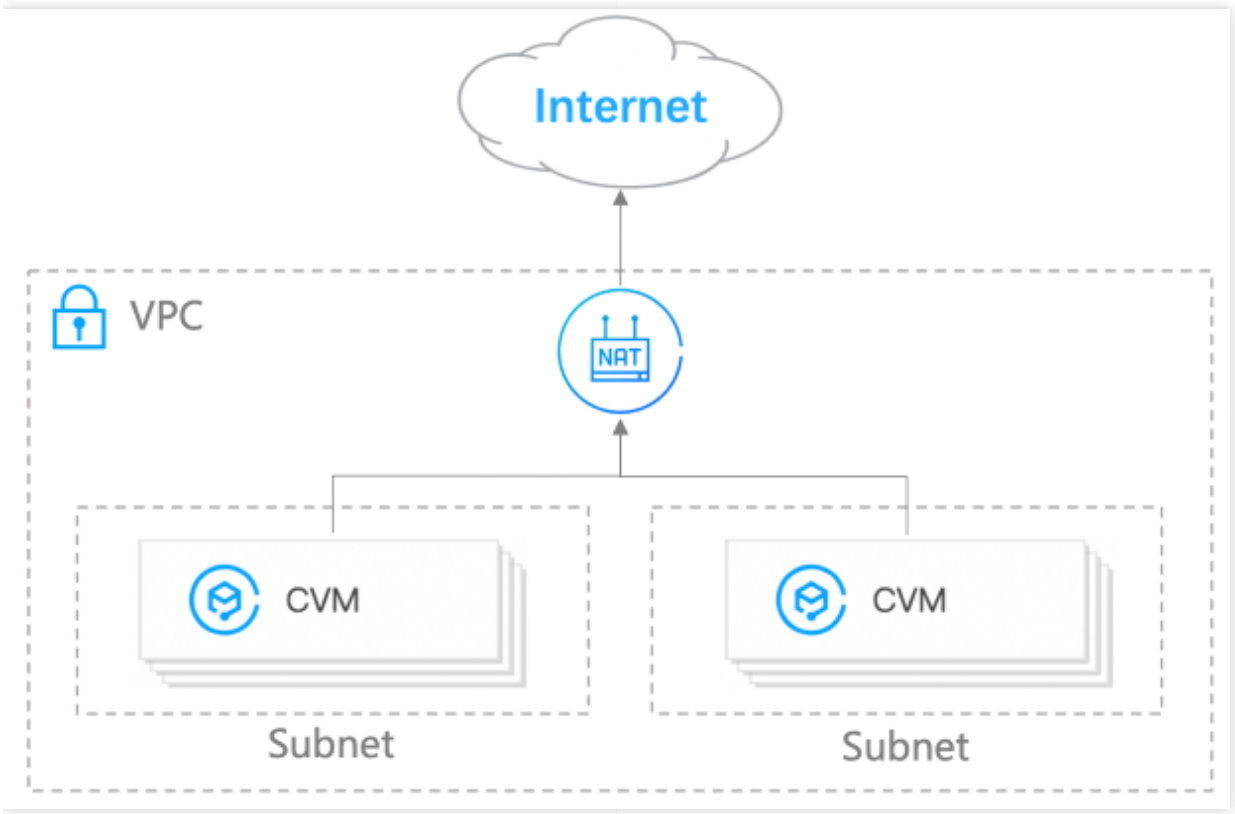
Single CVM Accessing the Public Network

When your business volume is small, and you only have a single CVM, you can apply for a public network IP and bind it to the CVM to enable the feature of accessing the public network.



Multiple CVMs Securely Accessing the Public Network

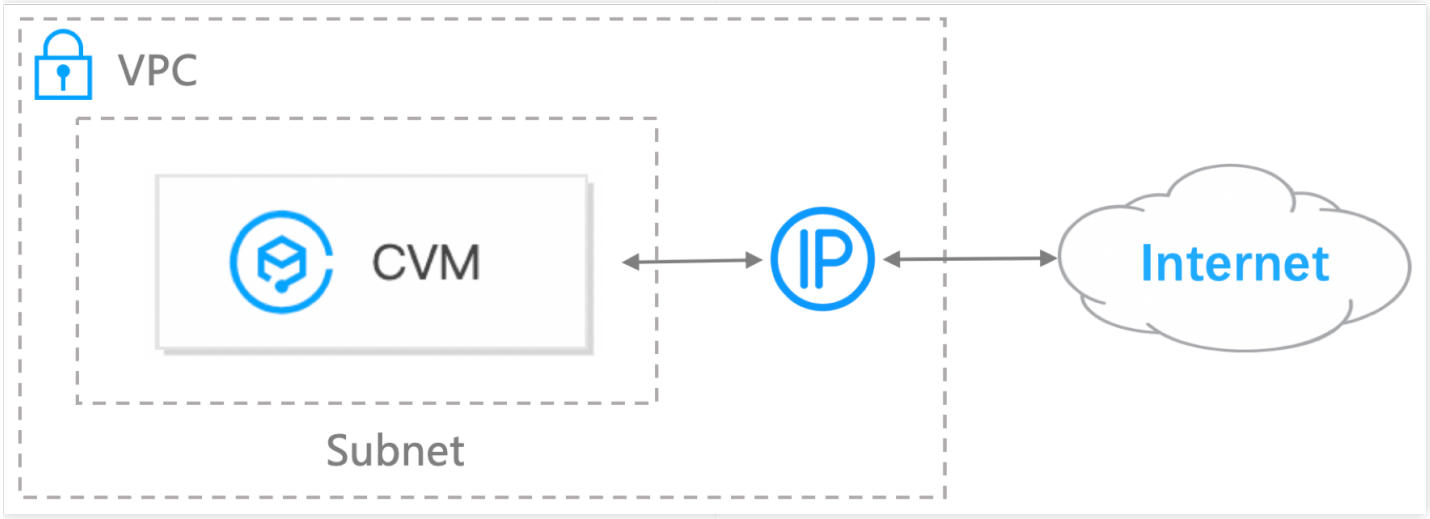
When you have multiple CVMs that need simultaneous access to the public network and don't want to expose the private IP addresses of the CVMs, you can use a NAT gateway. NAT gateway has SNAT function, which allows multiple CVMs to access the public network through the public network IP address of the NAT gateway. When DNAT is not configured, external users are unable to directly access the NAT gateway, ensuring security. When there are multiple public network IPs on a NAT gateway, the NAT gateway automatically performs CLB.



Providing Services to the Public Network

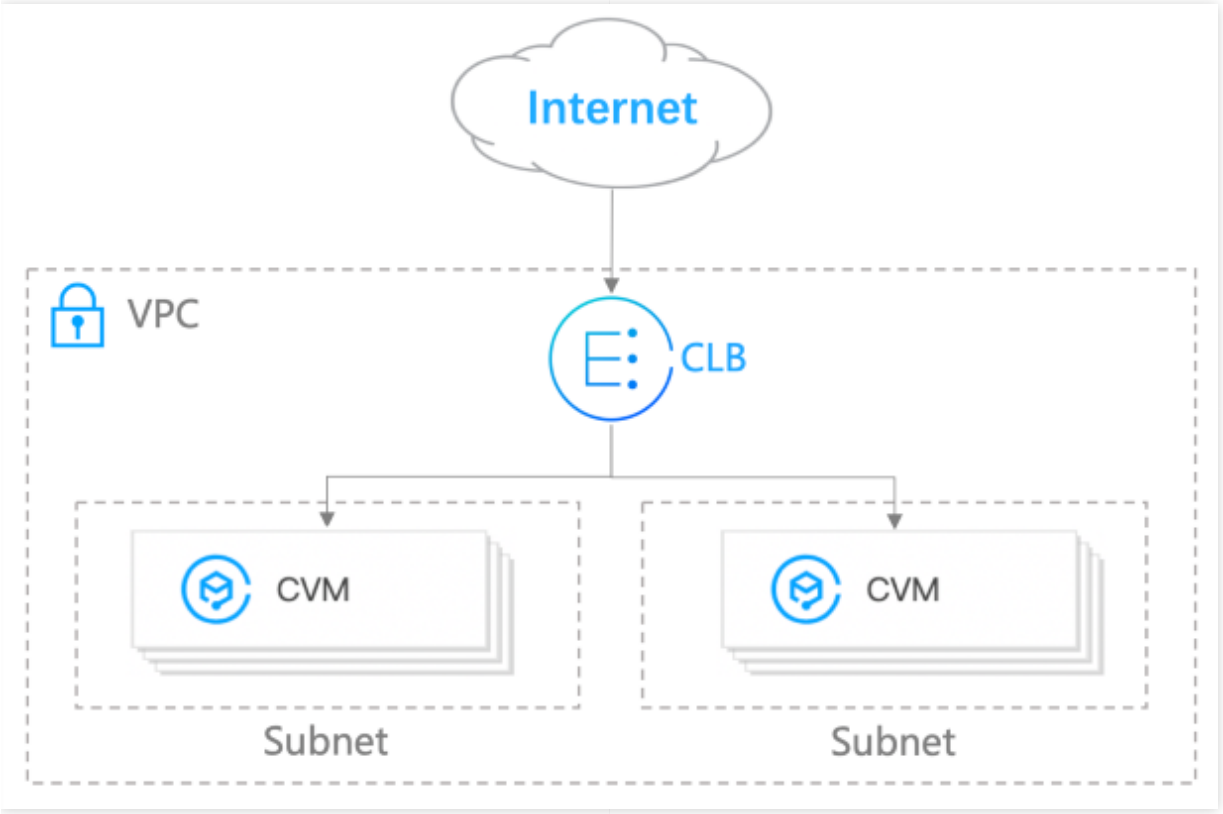
Single CVM Providing Services

You can host services such as websites on CVMs in the VPC and use a public network IP to provide services externally.



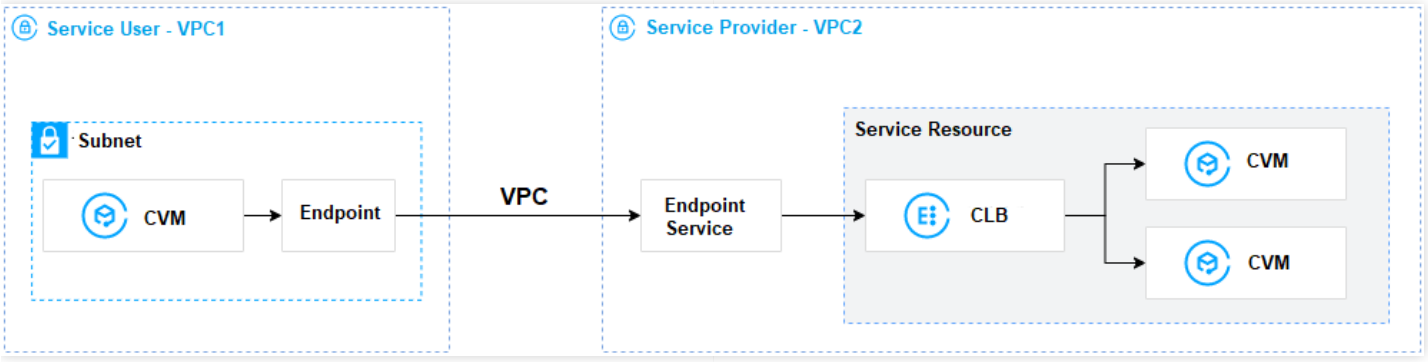
Multiple CVMs CLB

When you have many servers to deploy complex businesses and face high public network traffic, using CLB is advisable. CLB can automatically allocate application traffic among multiple CVM instances in the cloud, allowing you to achieve a higher level of application fault tolerance.



Cross-VPC Service Sharing

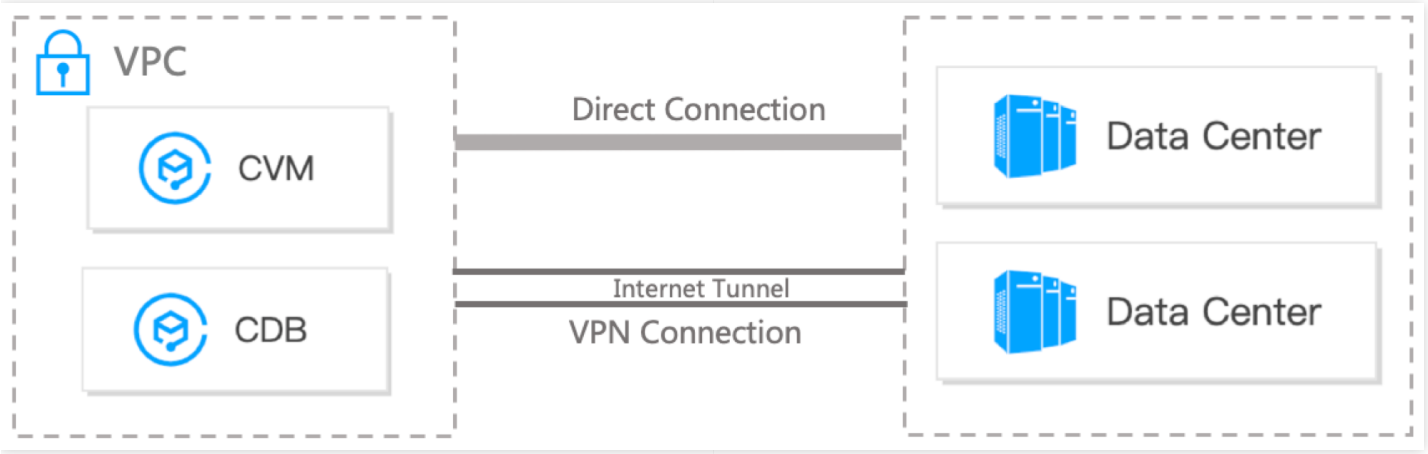
When you need to share application services deployed in a VPC with other VPCs in different accounts, you can use Private Link to achieve unidirectional cross-VPC access for intranet services. Compared to public network services, this can save public network bandwidth, offer higher security, and greatly simplify the network architecture.



Deploy Hybrid Cloud

Connecting to Local Data Centers

VPC offers various methods, such as dedicated access and VPN connections, which can link your local data center with cloud-based VPC, easily constructing a hybrid cloud architecture. Using a local data center can ensure the security of your core data. You can also scale the number of cloud resources (such as CVM and CDB) based on the volume of business, thereby reducing IT Ops costs.



Basic Concepts
IP Addresses

IP addresses are divided into two categories: IPv4 and IPv6. IPv4 is widely used, but the network address resources are limited. IPv6 can solve the problem of limited network address resources well.

IPv4 Address

The cloud platform has two types of IPv4 addresses: private network IPv4 address and public network IPv4 address. If you do not take the initiative to unbind or replace, neither the private network IPv4 nor the public network IPv4 change.

Private Network IPv4 Address

The private network IPv4 address is the implementation form of the cloud platform's IPv4 private network services and cannot be accessed through the IPv4 Internet. Once each CVM instance is created, it is assigned a private network IPv4 address, which can be automatically allocated by the system. In the VPC environment, the private network IPv4 address can also be customized by users.

Attribute

- IPv4 private network services have user attributes and different users are isolated from each other; that is, by default, they cannot access another user's cloud service via the IPv4 private network.
- IPv4 private network services have regional attributes, and different regions are isolated from each other. That is, by default, cloud services and VPCs in different regions under the same account cannot be accessed through the IPv4 private network.

Applicable Scenario

The private network IPv4 address is applicable to the following scenarios:

- IPv4 private network access between CLB and CVM instances in the same VPC.
- IPv4 private network access between CVM instances in the same VPC.
- IPv4 private network access between CVM instances and other cloud services (such as TDB) in the same VPC.

Related Operations

- To obtain the private network IPv4 address of the instance and set DNS, see Obtaining the Private Network IP Address and Setting DNS.
- To modify the private network IPv4 address of a CVM instance in VPC, see Modifying Private Network

IP Address.

Public Network IPv4 Address

Public network IPv4 addresses are divided into two categories: normal public IP and EIP, both of which can provide CVM with the ability to access or be accessed by IPv4 public networks.

Main Differences

The main differences between normal public IP and EIP are as follows:

Comparison Items	Normal Public IP	EIP
Use Scenario	If you want the system to automatically assign a public network IP address when you create a CVM, and after the CVM is released, the normal public IP is released together without retaining the public network IP address, you can select a normal public IP.	If you want to use a public network IP address for a long time and bind it to the designated CVM based on business needs. You can select an EIP, which can be bound and unbound repeatedly. After the CVM is released, EIP still exists.
Ability to access/be accessed by the public network	As public IP addresses, they have the same ability to access and be accessed by the public network.	As public IP addresses, they have the same ability to access and be accessed by the public network.
How to Obtain	It is only allocated when the CVM is purchased. If it is not allocated when purchased, it cannot be obtained.	- Apply for EIP at the console. - Convert normal public IP to EIP.
Features	Consistent with the CVM lifecycle, after the CVM is released, the normal public IP is also released.	- Independently enjoyed IP resources can be bound and unbound with CVMs, NAT gateways, etc., at any time. - It can be released when no longer needed.
Quota	There is no fixed quota for the number of IPs, which is consistent with the quota for the available CVM.	Each account can apply for 20 IP addresses in each region.
Quota	For the quota of normal public IP (including normal public IP and EIP) bound to each CVM, see Limitations on Binding CVM.	For the quota of normal public IP (including normal public IP and EIP) bound to each CVM, see Limitations on Binding CVM.
Operation - Convert IP	It can be converted. For details, see Converting Normal Public IP to EIP. After a normal public IP is converted to	EIP cannot be converted into normal public IP.

Comparison Items	Normal Public IP	EIP
	an EIP, only the IP attributes change, and the IP address remains unchanged.	
Operation - Release IP	If you no longer need a normal public IP, you can select More > IP/Network Interface > Refund Public Network IP to refund in the operation column of the.	It can be released on the EIP console. For details, see Releasing EIP.

IPv6 Address

The IPv6 address of the cloud platform can be used as both an private network IPv6 address and a public network IPv6 address. By default, it is an private network IPv6 address. When the public network capability needs to be enabled, this address can be changed into a public network IPv6 address. If you do not take the initiative to release or reallocate, this IPv6 address does not
change.

Private Network IPv6 Address

The private network IPv6 address is the implementation form of the cloud platform's IPv6 private network service and cannot be accessed through the IPv6 Internet. When you create a CVM instance, you can choose to allocate an IPv6 address free of charge, which will be automatically allocated by the system or obtained after creation. In VPC environments, private network IPv6 addresses can also be customized by users.

Attribute

- IPv6 private network services have user attributes and different users are isolated from each other; that is, by default, they cannot access another user's cloud service via the IPv6 private network.
- IPv6 private network services have region attributes and different regions are isolated from each other; that is, by default, cloud services and VPCs in different regions under the same account cannot be accessed through the IPv6 private network.

Applicable Scenario

The private network IPv6 address is applicable to IPv6 private network access between CVM instances under the same VPC.

Public Network IPv6 Address

After the IPv6 address is opened to the public network, it has the ability to access the IPv6 public network and be accessed by the IPv6 public network as a public network IPv6 address.

Region and Availability Zone

Region

Introduction

Region refers to the geographical area of a physical data center. Different regions of the cloud platform are completely isolated to ensure maximum stability and fault tolerance between different regions. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the following table or query the region list through the API to see the complete region list.

Availability Zone

Introduction

Availability Zone refers to a physical data center of the cloud platform where the power and network are independent in the same region. The goal is to ensure that failures within the availability zones are isolated from each other (except for major disasters or power failures) preventing fault propagation and ensuring that users' businesses continue to provide online services. By launching instances in independent availability zones, users can protect applications from the impact of single-location failures.
You can query the availability zone list through the API to view the complete availability zone list.

Quota Limitation

Virtual Private Cloud and Subnet

Resources	Limitation (Unit: count)
Number of VPCs per account in each region	5
Number of subnets in each VPC	10
Number of secondary CIDRs in each VPC	5
Default HAVIP quota per VPC	10. Max. 50.

Route Table

Resources	Limitation (Unit: count)
Number of route tables in each VPC	10
Number of route tables associated with each subnet	1
Number of routing policies per route table	50

Security Group

Description	Limitation
Number of Security Groups	50/region
Number of Security Group Rules	100/inbound, 100/ outbound
Number of Cloud Virtual Machine instances associated with a single security group	100
Number of security groups a Cloud Virtual Machine can be associated with	5
Number of rule entries for each security group that references the security group IDs	10 entries

Network ACL

Resources	Limitation

Resources	Limitation
Number of Network ACLs per VPC	50
Number of Rules per Network ACL	Inbound: 20 Outbound: 20
Number of Network ACLs Associated with Each Subnet	1

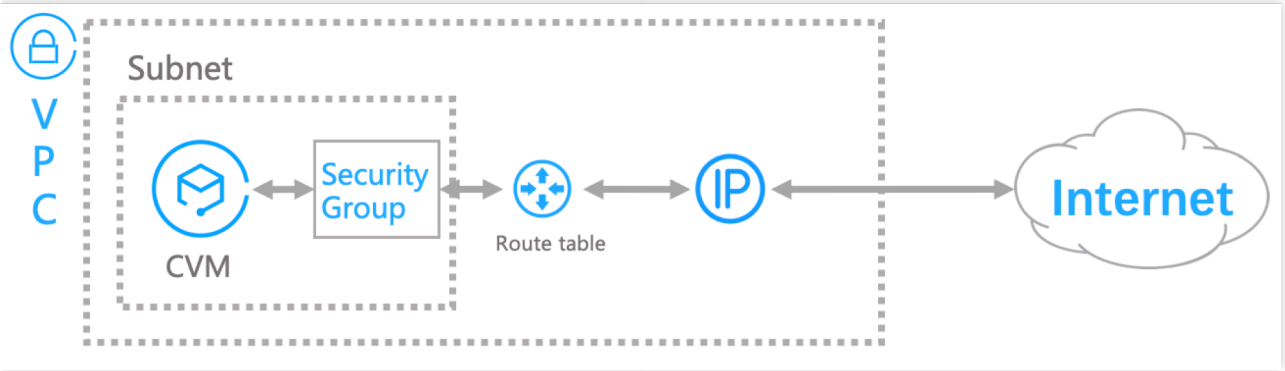
Parameter Template

Instance	Limitation (Unit: count)
IP Address Objects (ipm)	Maximum 1,000 per tenant
IP Address Group Objects (ipmg)	Maximum 1,000 per tenant
Protocol Port Objects (ppm)	Maximum 1,000 per tenant
Protocol Port Group Objects (ppmg)	Maximum 1,000 per tenant
IP Address Members in An IP Address Object (ipm)	Maximum 20 per tenant
IP Address Object Members (ipm) in An IP Address Group Object (ipmg)	Maximum 20 per tenant
Protocol Port Members Within A Protocol Port Group Object (ppm)	Maximum 20 per tenant
Protocol Port Object Members (ppm) in A Protocol Port Group Object (ppmg)	Maximum 20 per tenant
The Number of IP Address Group Objects (ipmg) that Can Reference the Same IP Address Objects (ipms)	Maximum 50 per tenant
The Number of Protocol Port Group Objects (ppmg) that Can Reference the Same Protocol Port Object (ppm)	Maximum 50 per tenant

Quick Start
Quickly Building an IPv4 VPC

Overview

This document, using the example of deploying a CVM capable of connecting to the Internet, guides you through rapidly establishing an IPv4 VPC. Detailed directions are introduced as follows: From creating VPCs and subnets, to creating CVMs and allocating public IP addresses, and finally controlling inbound and outbound traffic to CVMs via security groups.

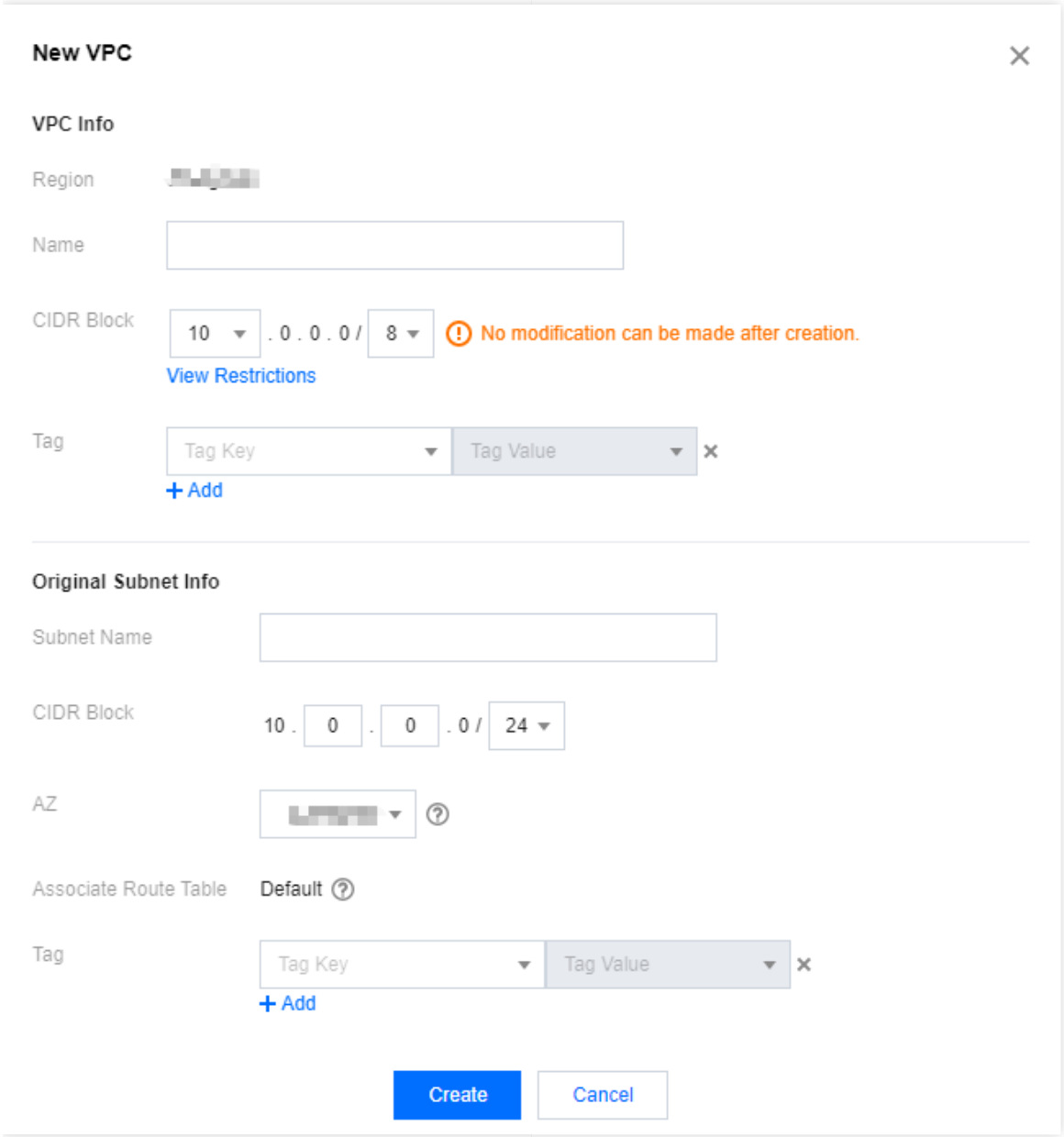


Directions

Step 1: Create PVCs and Subnets

1. Log in to the Virtual Private Cloud console.
2. At the top, choose the region to which the VPC belongs, and click Create.
3. In the pop-up dialog box New VPC, fill in the VPC information and initial subnet information, and click Create.

> Note:
>
> Once the CIDRs (that is, IP ranges) of the VPC and subnets are created, they cannot be modified. Plan the network in advance.



- The VPC Information
  - Name: VPC name.
  - IPv4 CIDR:
    - You can select any one of the standard IP ranges 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 and 192.168.0.0-192.168.255.255 as the VPC IP range. The IP mask range should be between 16 and 28, such as 10.0.0.0/16.
    - The non-standard IPv4 private address ranges can also be selected (the mask range should be between 16 and 28).

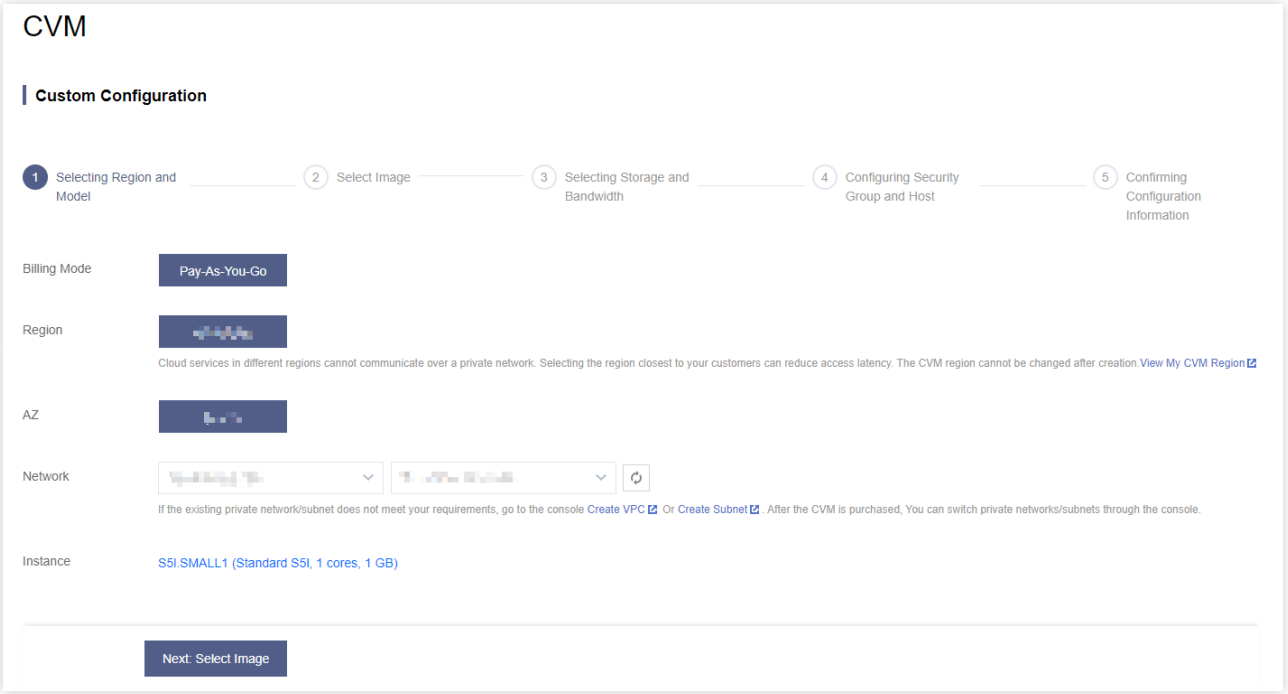
> Note:
>
> Since September 16, 2020, VPCs have started to support non-standard IPv4 private address ranges (non-standard IPv4 private address ranges refer to those that are not defined within the three major private address ranges specified in RFC 1918). If you need to use them, you may submit a ticket for application.

- Initial Subnet Information
  - IPv4 CIDR:
    - You can choose a VPC IP range that is within the range of the VPC IP range or the same as the VPC IP range. For example, if the VPC IP range is 10.0.0.0/16, you can select the range between 10.0.0.0/16-10.0.255.255/28 as the subnet IP range.
    - If the VPC to which the subnet belongs needs to communicate with other VPCs or IDCs, ensure that the subnet's IP range does not overlap with the peer's IP range. Otherwise, private network interconnection is impossible.
- Availability Zone: Select an availability zone of the subnet. The same VPC can have subnets of different availability zones. By default, subnets of different availability zones under the same VPC are private network interconnected.

Step 2: Purchase CVMs

1. Log in to the Cloud Virtual Machine Console.
2. At the top left of the list page, click Create to enter the CVM purchase page.
3. On the custom configuration page, configure CVM instances according to actual needs and interface prompts. The example is as follows:

   i. On the Select Region and Instance page, choose the VPC and subnet you have created, choose the instance model, and click Next: Select Image.



   ii. In the Select Image interface, choose the image version. In this example, CentOS 7.4 64-bit is chosen. You can also choose other models according to your actual needs. After completion, click Next: Select Storage and Bandwidth.

   iii. On the 3. Select Storage and Bandwidth page, set the system disk type and public network IP address. In this example, choose not to allocate temporarily. Click Next: Configure Security Groups and Host.

> Note:
>
> If you choose to allocate now, the system will automatically allocate a public network IP address to your CVM. If you choose not to allocate a public network IP address temporarily, you need to apply for and bind an EIP in the CVM console so that the CVM can access the public network.

iv. On the 4. Configure Security Groups and Hosts page, in this example, choose Create Security Group, set log-in method and password, and click Next: Confirm Configuration Information.

v. Confirm the information on the 5. Confirm Configuration Information page, and click Activate to complete the purchase of CVM instances.

Step 3: Apply for EIP and Bind to CVM

Apply for an EIP (IP resources which can be independently purchased and held), and bind the EIP to the CVM instance to realize public network access.

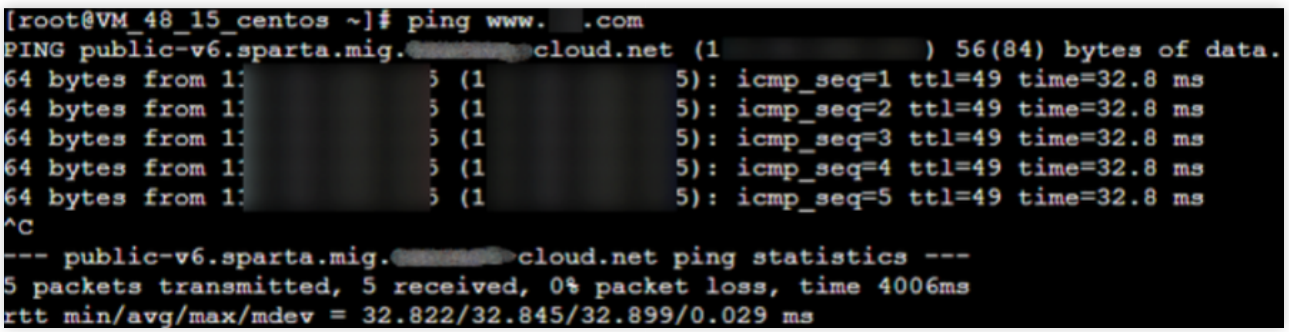
1. Log in to the EIP console.
2. On the EIP management page, choose the region where the created CVM is located and click Apply.
3. In the pop-up Apply for EIP window, configure relevant parameters, and then click OK to complete the application of EIP.
4. On the EIP management page, find the applied EIP and click More > Bind.
5. In the pop-up Bind Resources window, choose CVM Instance as the binding resource type. Then choose the created CVM and click OK.

Step 4: Test the Connectivity of Public Network

Complete the following operations to test the public network connectivity of CVM instances.

> Note:
>
> Before testing, make sure that the security group has allowed access to the corresponding IP/port. For example, allow ICMP protocol and public network Ping server. You can confirm it by View Security Group Rules.

1. Log in to the CVM instance with the EIP bound.
2. Run ping other public network addresses , such as ping www.google.com to test the connectivity of the public network.

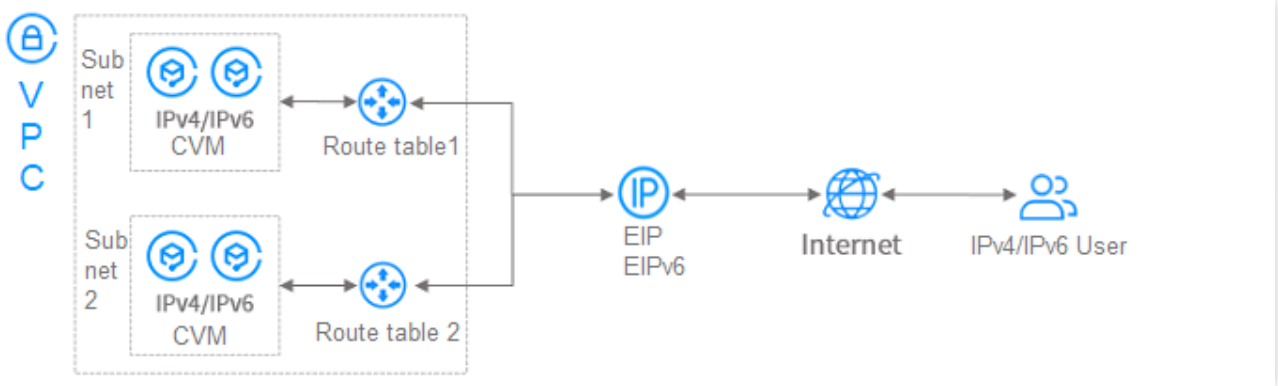


Quickly Building an IPv6 VPC

Overview

This tutorial will help you build a Virtual Private Cloud (VPC) with an IPv6 CIDR. IPv6 for the Cloud Virtual Machines (CVMs) or Elastic Network Interfaces (ENIs) in the VPC is enabled so that VPC and public network communications via IPv6 are implemented.

1. CVMs are IPv6-enabled to communicate with other CVMs in the VPC through the IPv6 private network.
2. CVMs are IPv6-enabled to communicate bidirectionally with IPv6 users on the Internet.



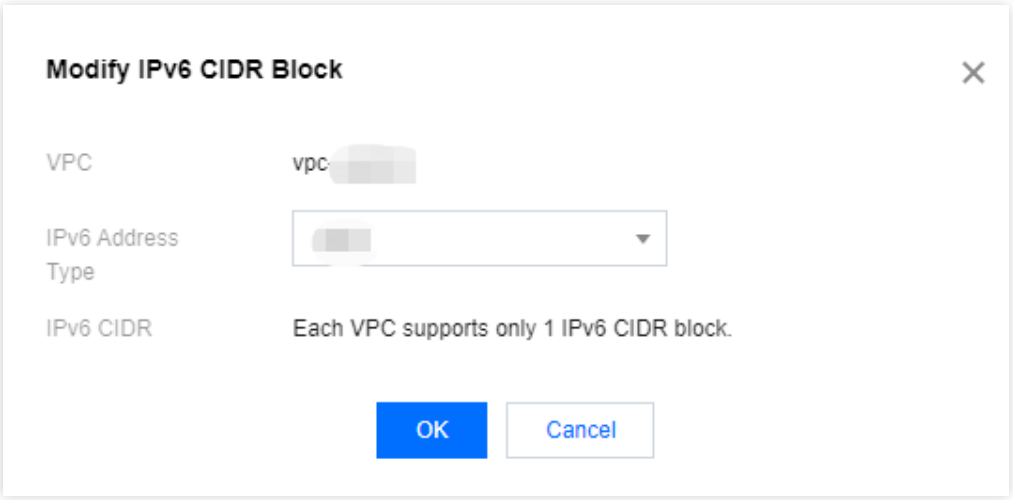
Instructions

1. The IPv6 address is a GUA address. Each VPC is allocated with one /56 IPv6 CIDR. Each subnet is allocated with one /64 IPv6 CIDR. Each ENI is allocated with one IPv6 address.
2. Both the primary network interface and the secondary network interface support applying for IPv6 addresses. For more information about the relationship between CVM and ENI, see Elastic Network Interface product documentation.

Directions

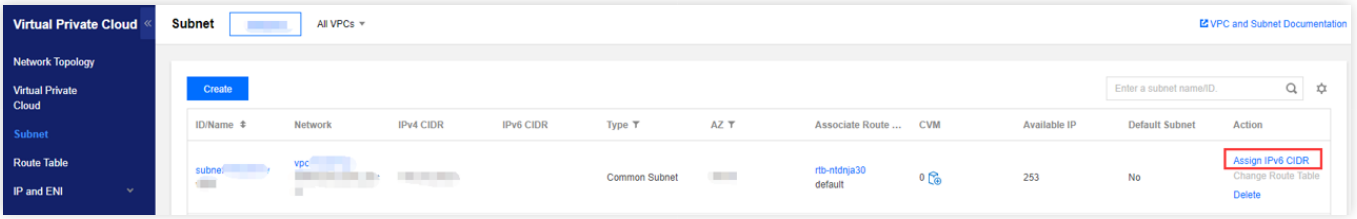
Step 1: Allocate IPv6 CIDR to VPC

1. Log in to the Virtual Private Cloud console.
2. In the left sidebar, choose VPC. Under the operation column of the row corresponding to the VPC where you want to enable IPv6, click Edit IPv6 CIDR.
3. In the pop-up dialog box Modify IPv6 CIDR Block, choose IPv6 address type and click OK to complete obtaining the VPC IPv6 CIDR. Currently, one VPC only supports one IPv6 CIDR.



Step 2: Allocate IPv6 CIDR to Subnet

1. Log in to the Virtual Private Cloud console.
2. In the left sidebar, choose Subnet. Under the operation column of the row corresponding to the subnet where you want to enable IPv6, click Assign Ipv6 CIDR.
3. Click OK to confirm the operation. The system will allocate a /64 IPv6 CIDR from the VPC's /56 IPv6 CIDR, and you can see the IPv6 address segment in the list.



Step 3: Purchase a CVM and allocate an IPv6 address to its ENI

1. Log in to the Cloud Virtual Machine Console.

2. At the top left of the list page, click Create to enter the CVM purchase page.

3. On the custom configuration page, configure CVM instances according to actual needs and interface prompts. Choose not to allocate IPv6 addresses temporarily.

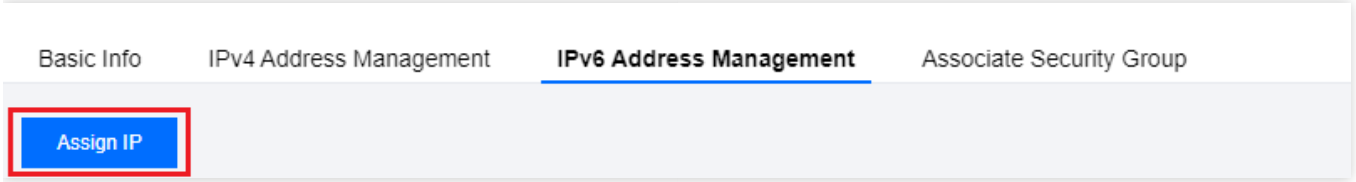
   > Note:
   >
   > If the CVM is not allocated with an IPv6 address when you purchase it, under the operation column of the row corresponding to the CVM instance, you can choose EIP > Manage IPv6 Addresses to allocate an IPv6 address to the primary NIC.

4. After purchasing the CVM, log in to the VPC console.

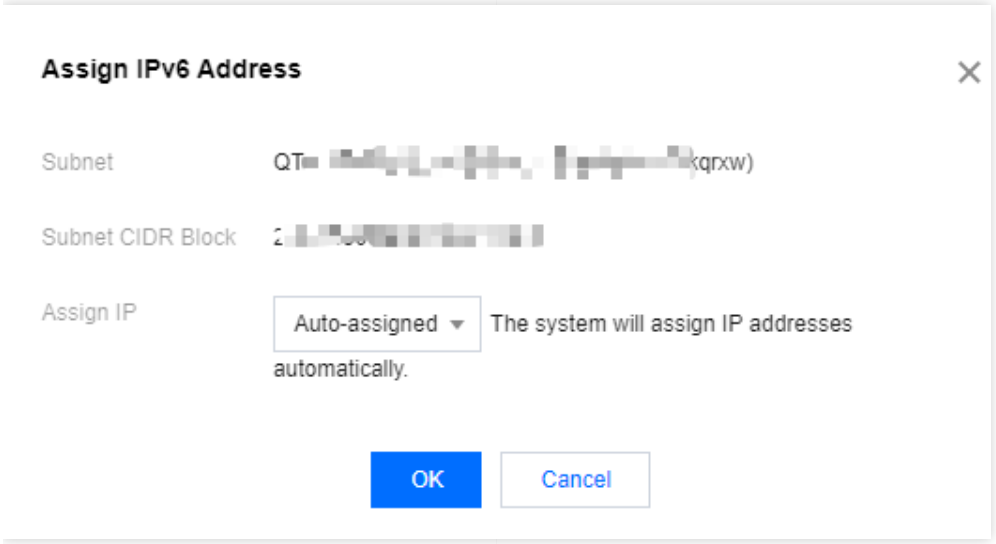
5. In the left sidebar, choose IP and NIC > ENI. Click Create to create an ENI under the subnet in Step 2, and bind it to the purchased CVM.

6. Click the ID of this ENI to go to the details page. Choose the IPv6 Address Management tab and click Allocate IP.

> Note:
>
> The standard quote of an ENI is one IPv6 address. If you need more IPv6 addresses, please contact the cloud platform administrator to modify the quota for you. A maximum of 10 IPv6 addresses can be allocated to one ENI.



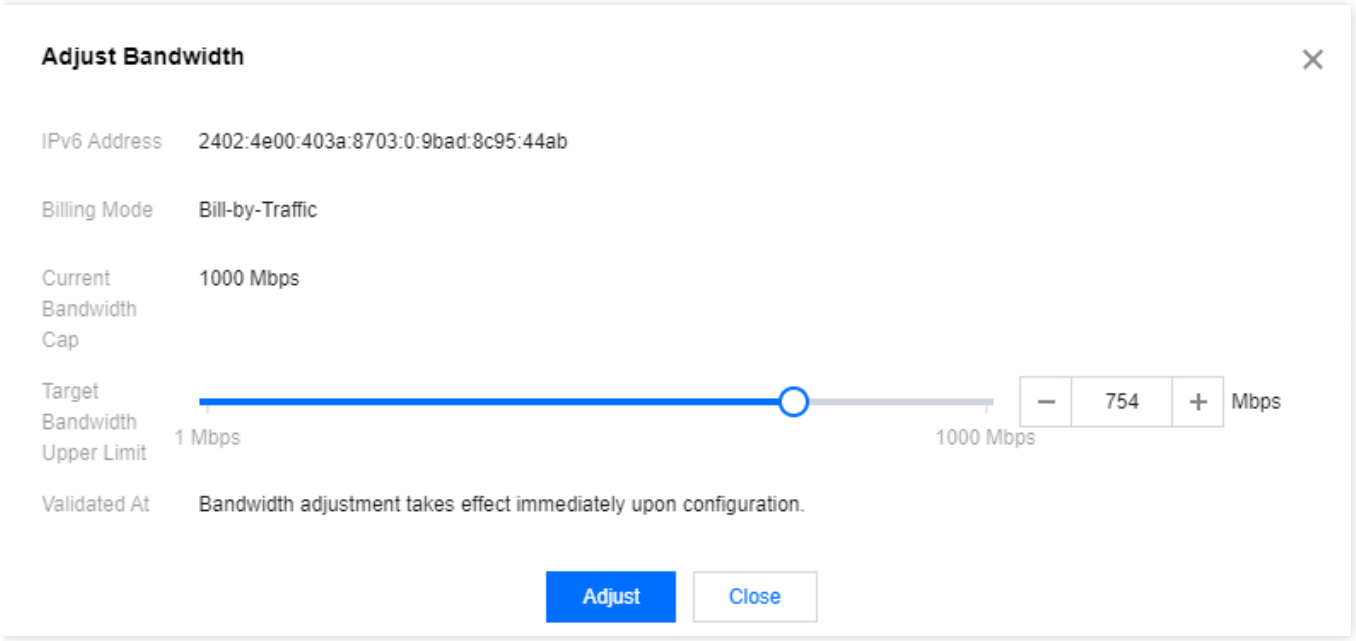
7. In the pop-up dialog box Allocate IPv6 Address, allocate an IPv6 address to the NIC by automatically allocating or manually filling in. Click OK. The system will allocate an IPv6 address for the ENI, as shown below.



Step 4: Enable Public Network for the ENI's IPv6

1. Log in to the Virtual Private Cloud console.
2. In the left sidebar, choose IP and NIC > EIPv6.
3. Click Adjust Bandwidth under the operation column to set the public network bandwidth and click Adjust.

> Note:
>
> If the bandwidth is not set to 0, the public network will be enabled. If it is set to 0, the public network will be disabled.

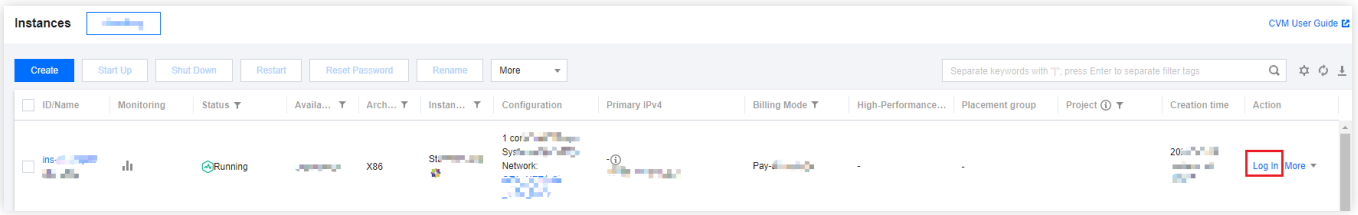


Step 5: Log In to the CVM and Enable IPv6

CVMs have different operation methods to enable IPv6. This step illustrates the process using the example of newly purchased CentOS 7.5 and CentOS 7.6.

Enabling IPv6 for newly purchased CentOS7.5/CentOS7.6

1. Go to the CVM console and log in to the instance.



2. Execute the following command to open the ifcfg-eth0 file in the folder /etc/sysconfig/network-scripts/ .

   vim /etc/sysconfig/network-scripts/ifcfg-eth0

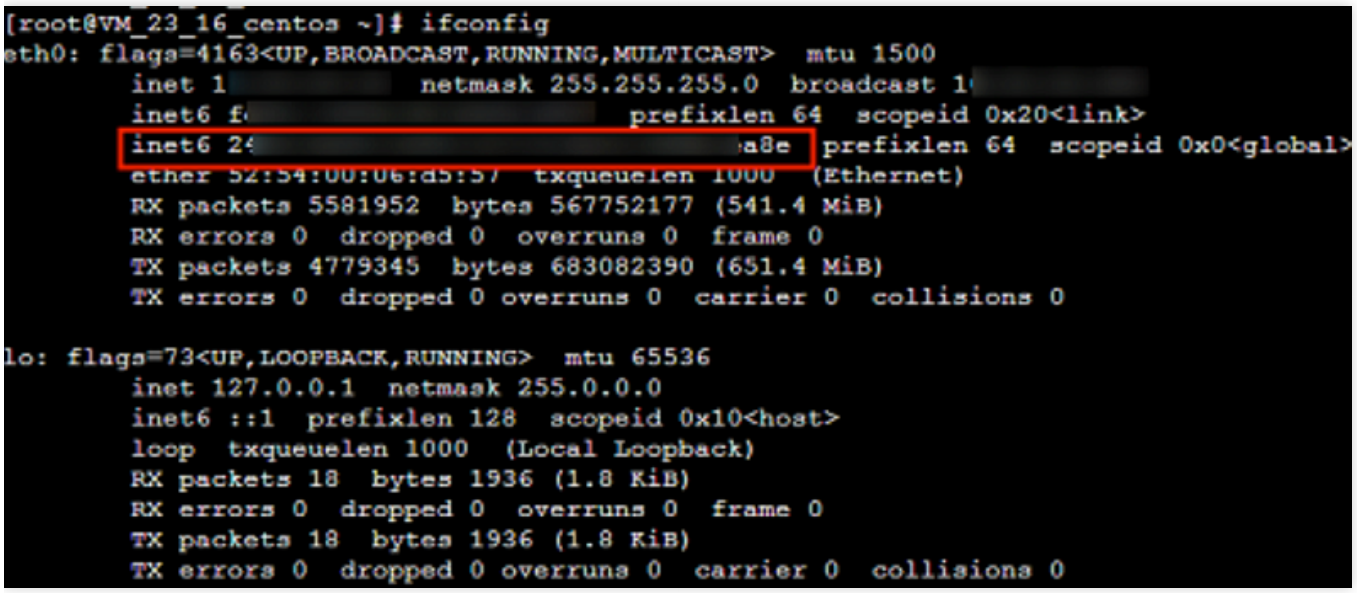
3. Press i to switch to edit mode and add the following content.

   DHCPV6C=yes

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
HWADDR=52:54:00:06:d5:57
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
DHCPV6C=yes
~
```

4. Press Esc and enter :wq to save the file and return.
5. Execute the following commands in sequence to check whether an IPv6 address has been obtained.

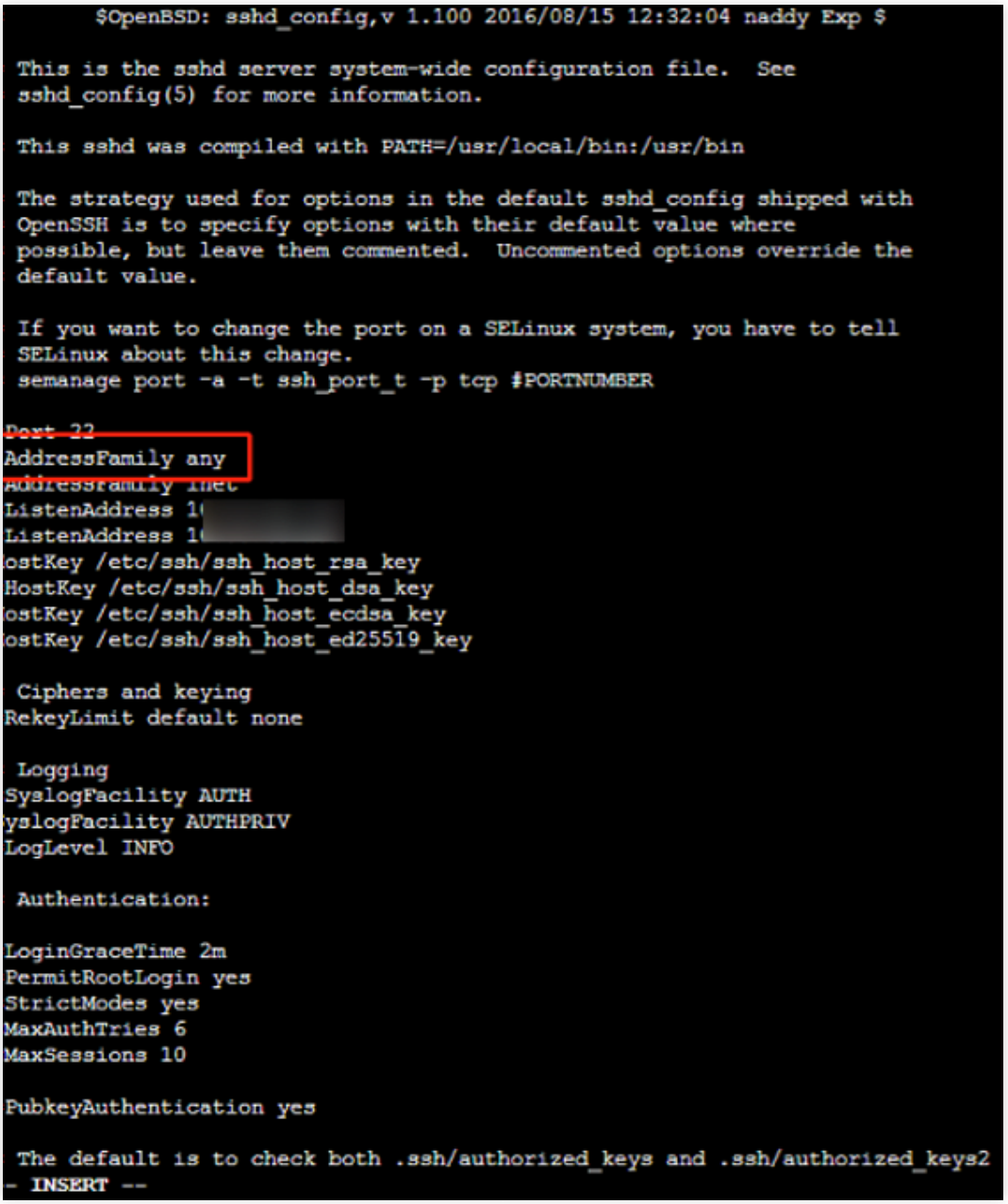
   dhclient -6
   ifconfig



6. Execute the following command to open sshd_config file in the folder /etc/ssh/ .

   vim /etc/ssh/sshd_config

7. Press i to switch to edit mode and delete AddressFamily any comment (delete the preceding #), and enable IPv6 listening for applications such as ssh.



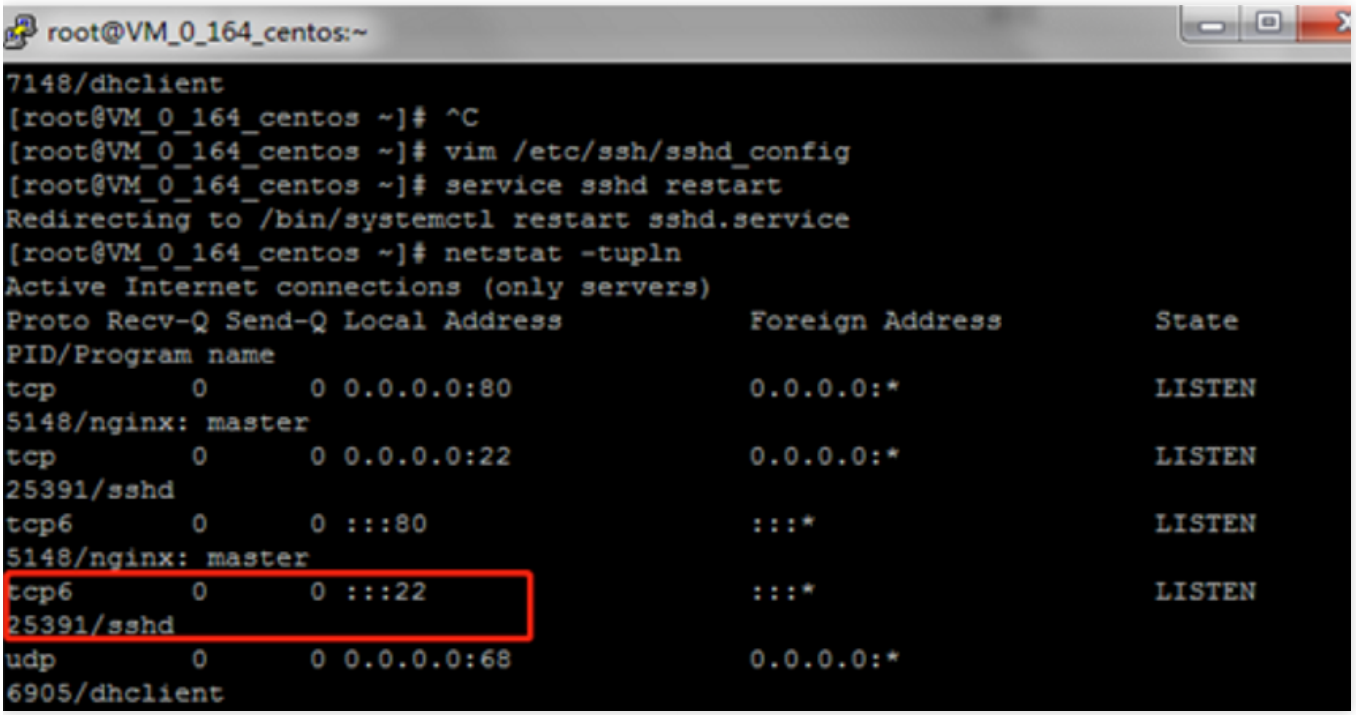
8. Press "Esc", enter ":wq", to save the file and exit.

9. Run the following command to restart the SSH process.

    service sshd restart

10. Run the following command to check if SSH is now listening on IPv6.

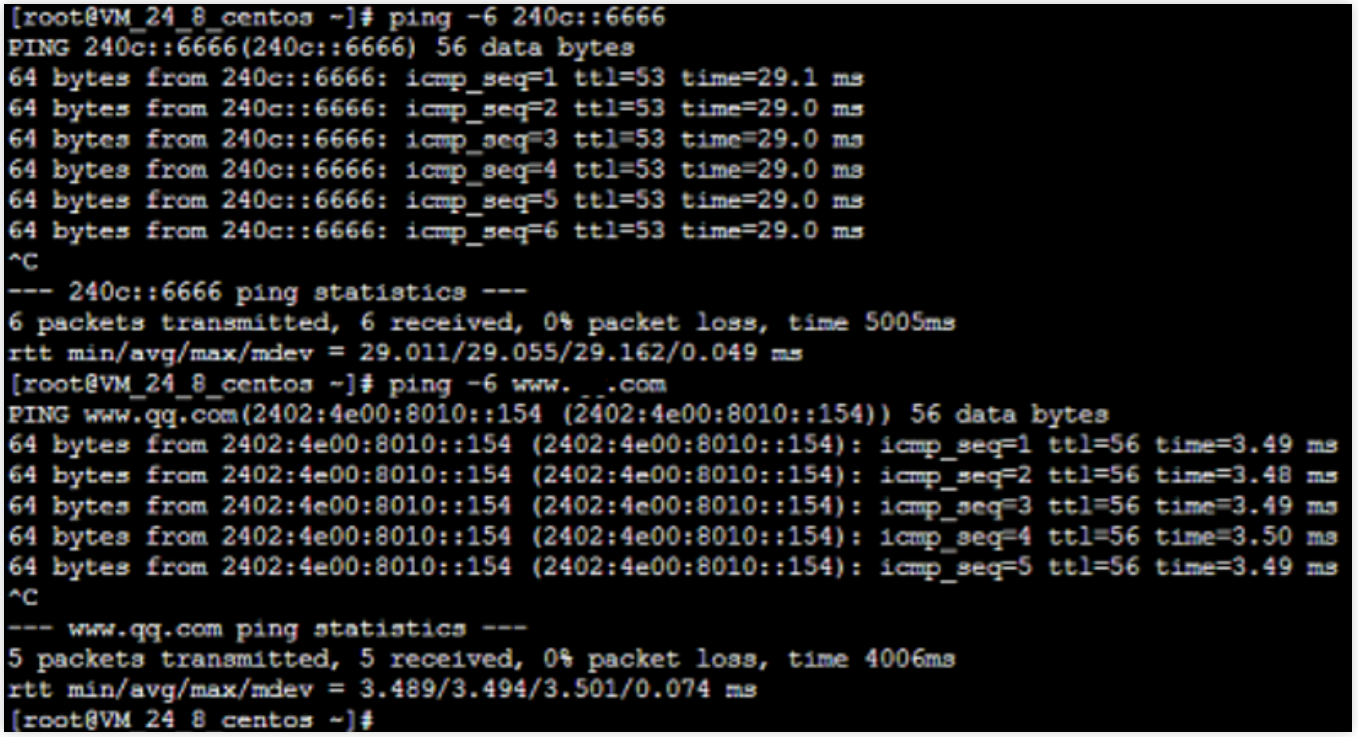
netstat -tupln



Step 6: Test IPv6 Connectivity

Connectivity of IPv6 can be tested via operations such as ping and ssh.

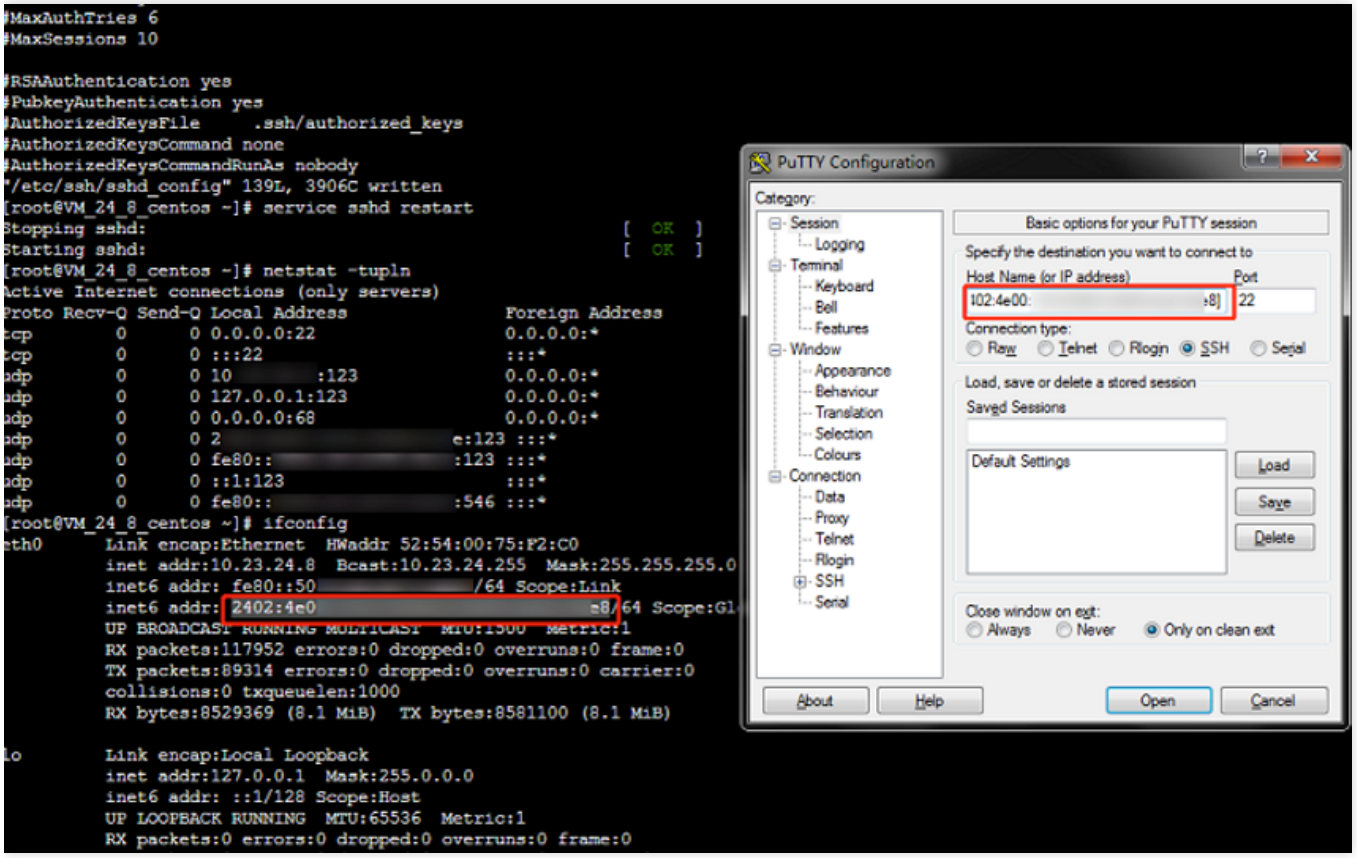
1. From the CVM ping6 240c::6666 or ping6 www.google.com , as shown in the following figure.



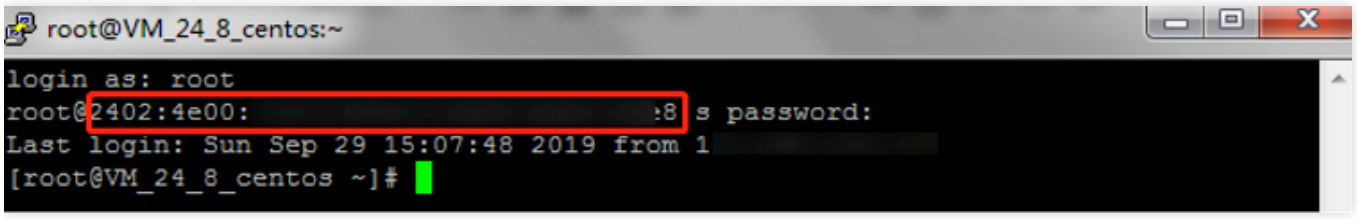
2. From the public network IPv6 address ssh CVM, and the specific steps are as follows:

Run the following command to view the IPv6 address, and use PuTTY or Xshell and other software to test whether you can use ssh to log in to the CVM through the IPv6 address.

ifconfig



The successful result is shown in the figure below.



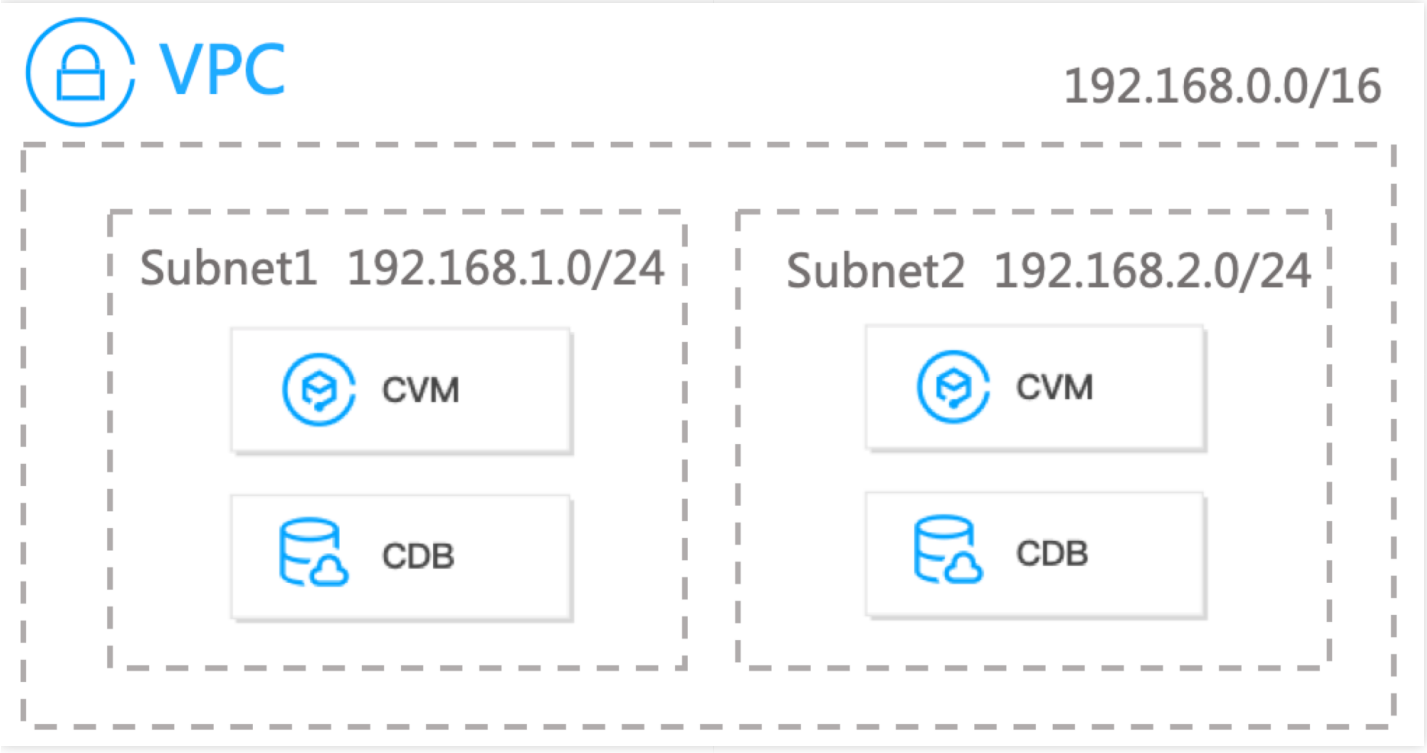
Operation Guide
Network Planning

Before using VPC, you need to plan the number of VPCs and their IP ranges according to your business needs, avoiding issues caused by temporary scale-out.
During planning, you need to take the region, VPCs, the number of subnets, IP ranges, and route tables into account.

Plan VPC

Plan one VPC

If your operations are small and all deployed in the same region, while there is no need for network isolation, it is recommended to plan one VPC.
You can create multiple subnets and route tables in one VPC for fine-grained management of traffic.

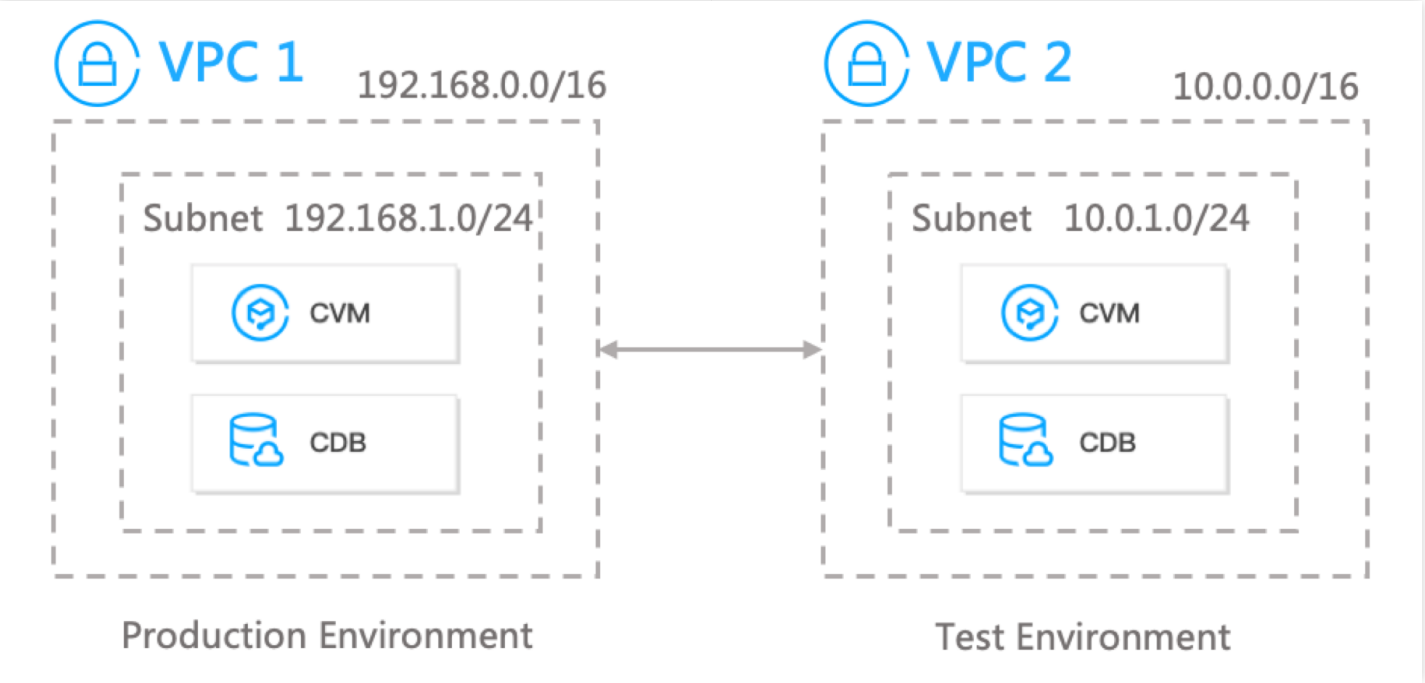


Plan multiple VPCs

It is recommended to plan multiple VPCs in the following scenarios:

- Multiple services must be isolated from each other
  Because private network interconnection is enabled by default in the same VPC, you need to plan

multiple VPCs when different services in the same region need to be isolated.



Plan Subnet

Converge CloudEach VPC supports creating up to 10 subnets, with each subnet representing a block of IP addresses within the VPC. The subnet's IP range must be within or identical with the VPC's IP range.
The following points should be kept in mind when planning a subnet:

- Subnet Size and IP Capacity
  When creating a subnet, make sure that the IP capacity of the IP range meets the demands. However, the subnet should not be too large in case no new subnets can be created during subsequent service expansion.
- Subnet's IP Range
  If the VPC to which the subnet belongs needs to communicate with other VPCs or IDCs, ensure that the subnet's IP range does not overlap with the peer's IP range. Otherwise, private network interconnection is impossible.
- Service Needs
  Within the same VPC, subnets can be divided according to business modules. For example, Web layer, logic layer and data layer are deployed in different subnets, and network ACL can be used for inter-subnet access control.

Plan IP Range

Converge CloudVPC CIDR supports any of the following private IP ranges:

- 10.0.0.0-10.255.255.255 (The mask range must be between 16 and 28.)
- 172.16.0.0-172.31.255.255 (The mask range must be between 16 and 28.)
- 192.168.0.0-192.168.255.255 (The mask range must be between 16 and 28.)
- Non-standard IPv4 private IP ranges (The mask range must be between 16 and 28.)

> Note:
>
> Since September 16, 2020, VPCs began to support non-standard IPv4 private IP ranges (non-standard IPv4 private IP ranges are the three major private IP ranges not defined in RFC 1918). To use them, please
>
> Submit a Ticket
>
> Application.

IP Range Description

About VPC Interconnection

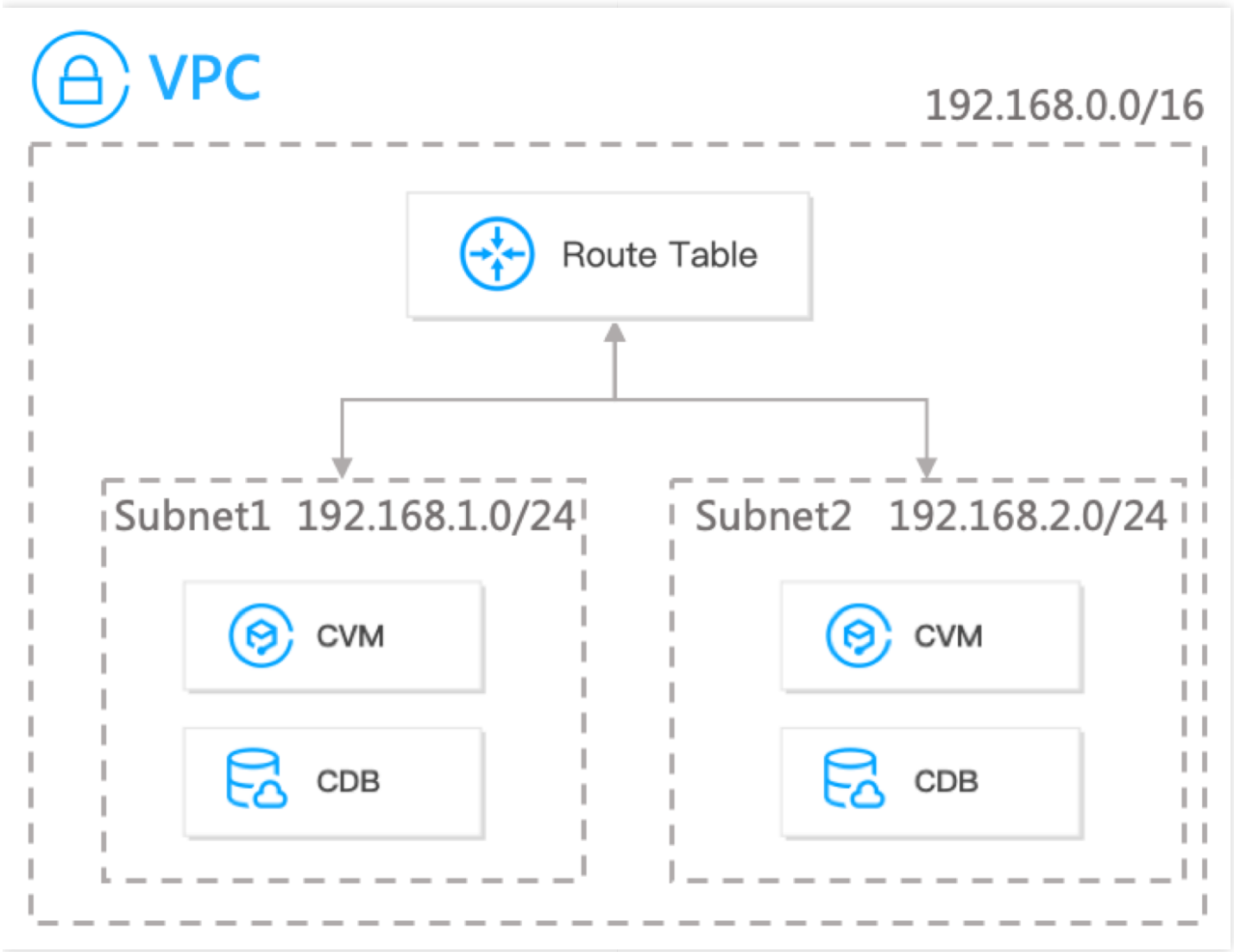
- If you need to establish multiple VPCs, and there is a communication demand between the VPCs or between the VPC and the IDC, please avoid overlap of multiple VPC IP ranges and do not use peering connection.
- If the subnet IP ranges have overlapped, you can re-create your VPCs and purchase CVMs.

Plan Route Table

A route table is used to control the traffic direction within a subnet, and each subnet can only be bound to one route table. VPCs support default route tables and custom route tables.

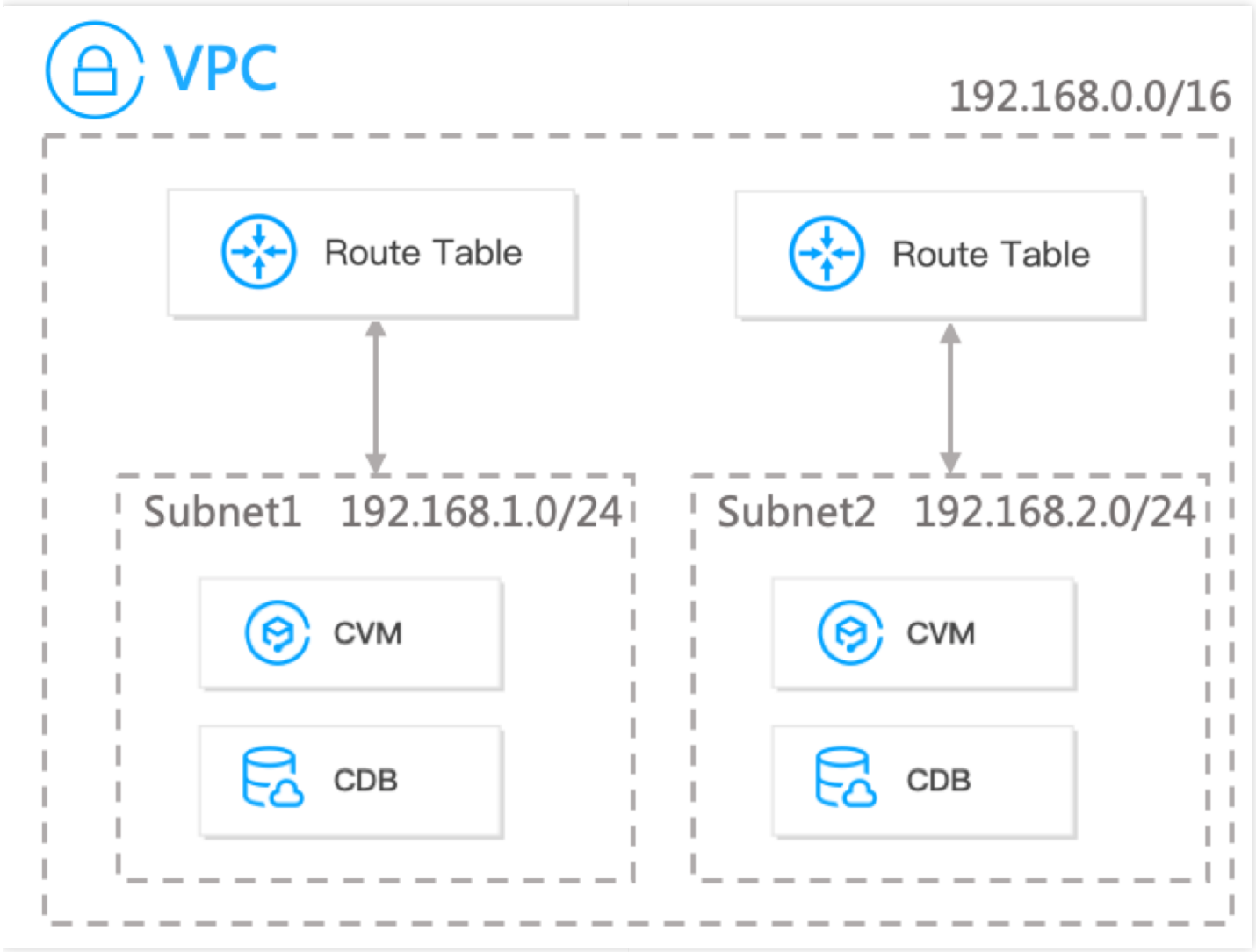
Plan one Route Table

If the traffic direction requirements of different subnets in your VPCs are identical or similar, it is recommended to plan one route table. You can create different routing policies to control the traffic direction.



Plan multiple Route Tables

If the traffic direction requirements of different subnets in your VPCs are quite different, it is recommended to plan multiple route tables. Subnets with different requirements are each bound with corresponding routing tables. Traffic flow is controlled through routing policies.


VPC
192.168.0.0/16
Route Table
Route Table
Subnet1 192.168.1.0/24
CVM
CDB
Subnet2 192.168.2.0/24
CVM
CDB

Virtual Private Cloud and Subnet Restrictions

Usage Limitations

- The IP ranges of a VPC and subnet cannot be modified after creation.
- The cloud platform reserves the first two IP addresses and the last IP address of each subnet for IP networking. For example, if the subnet CIDR is 172.16.0.0/24 , the IP addresses reserved by the cloud platform are: 172.16.0.0 , 172.16.0.1 and 172.16.0.255 .
- When CVMs are added to a VPC, the system will randomly assign a private network IP address to this instance in the specified subnet by default, and users can reassign the private network IP address of each CVM after the creation of CVMs.

Quota Limitation

Resources	Limitation (units)
Number of VPCs per account in each region	5
Number of subnets in each VPC	10
Number of secondary CIDRs in each VPC	5

Managing Virtual Private Cloud

Virtual Private Cloud (VPC) is fundamental for using cloud services. For example, when purchasing instances like CVM, you need to select the VPC to which the corresponding instance belongs. This document describes the lifecycle of VPC usage.

Background

1. Create VPC: Before creating a VPC, you need to conduct network planning. The CIDRs of a VPC and subnet cannot be changed after creation.
2. View VPC: You can view the basic information and the resources contained within a VPC.
3. Delete VPC: When a VPC is deleted, its associated subnets and route tables will also be deleted.

Create VPC

A VPC contains at least one subnet, and only in the subnet can cloud service resources be added.

1. Log in to the Virtual Private Cloud console.

2. Select Virtual Private Cloud in the left navigation bar.

3. On the Virtual Private Cloud page, select the region to which the VPC belongs and click Create.

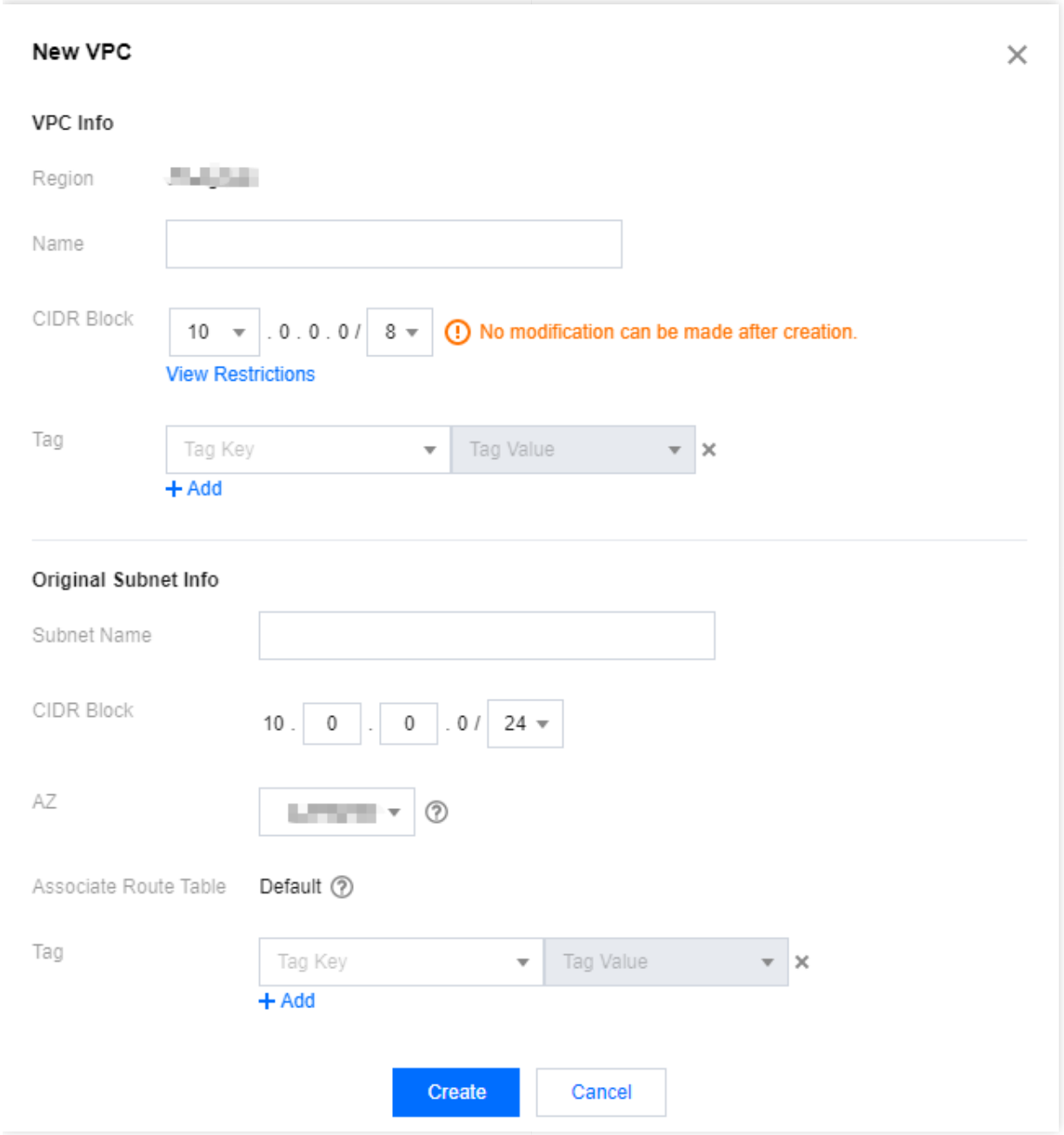
4. In the pop-up New VPC dialog box, fill in the VPC information and initial subnet information.

   > Note:
   >
   > VPCs and subnet CIDRs cannot be modified after creation.

   - VPC CIDR supports using any of the following IP ranges. If there is a need for private network communication between different VPCs, make sure that the CIDR configurations of the VPCs at both ends do not overlap:
     - 10.0.0.0 - 10.255.255.255 (The mask range must be between 16 and 28.)
     - 172.16.0.0 - 172.31.255.255 (the mask range must be between 16 and 28)
     - 192.168.0.0 - 192.168.255.255 (the mask range must be between 16 and 28)
     - If there is a request to use another CIDR, contact the platform administrator to complete the deployment of custom CIDRs in the backend.
   - Tag: You can add tags as needed, which helps you to manage your resources and can be adjusted on demand.
   - The CIDR of the subnet must be within or the same as that of the VPC.

For example, if the IP range of a VPC is 192.168.0.0/16 , then the IP range of the subnet within that VPC can be 192.168.0.0/16 , 192.168.0.0/17 , and so on.

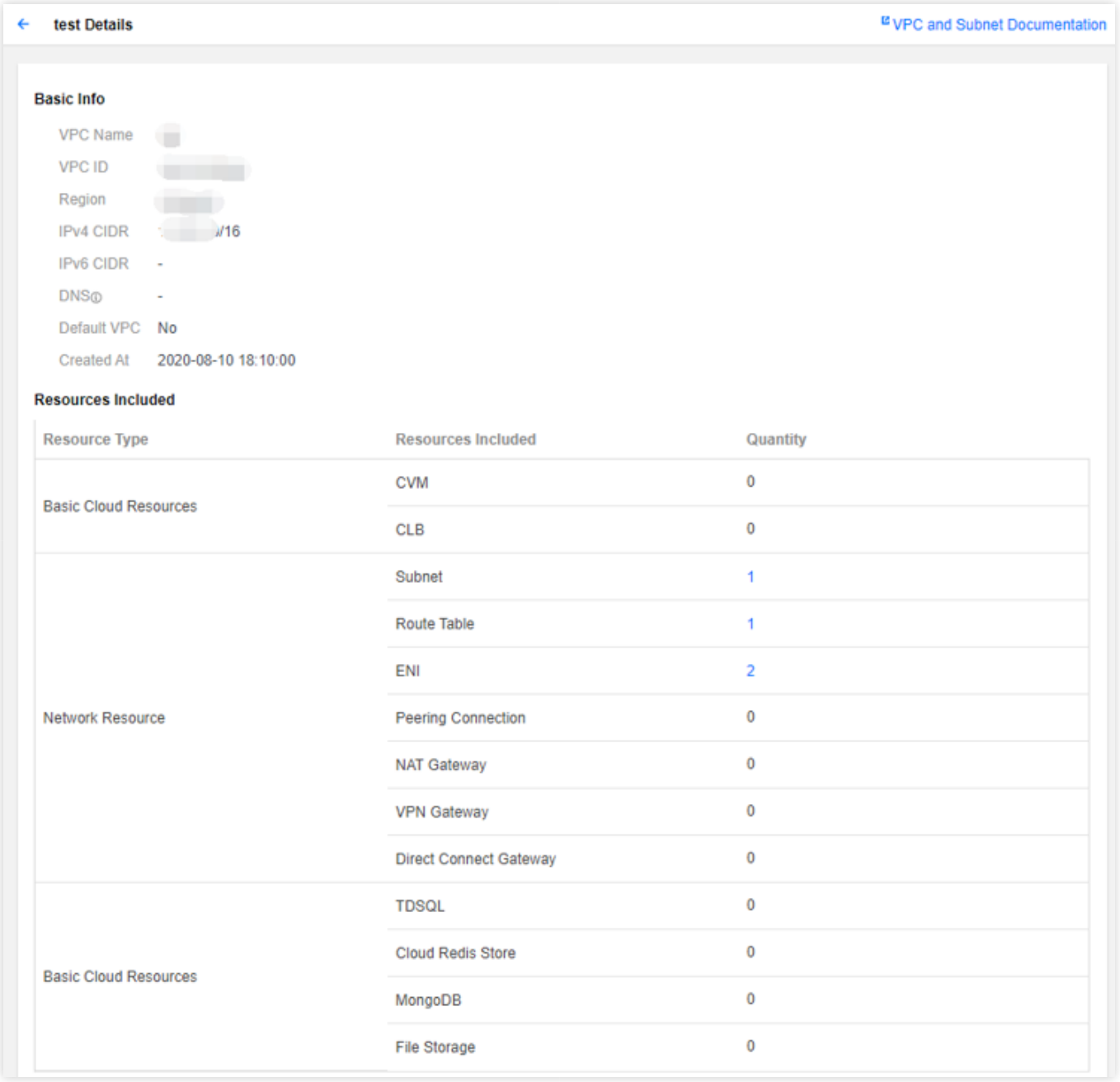
- Within the same VPC, it is possible to have subnets located in different availability zones. By default, private network interconnection is available for subnets in different availability zones within the same VPC. The same VPC can have subnets of different availability zones. By default, subnets of different availability zones under the same VPC are private network interconnected.
- Associated route table: A subnet must be associated with a route table for traffic forwarding control. The initial subnet is associated with a default route table, which is delivered by the system by default and indicates private network interconnection within the VPC.



5. After the parameters are set, click Create to complete the creation of the VPC, and the successfully created VPC is displayed in the list.

View VPC

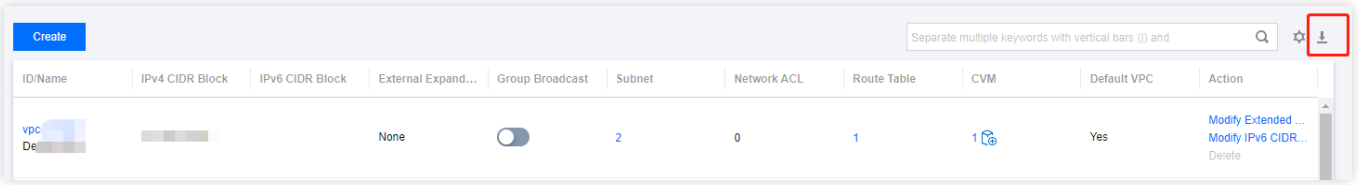
1. Log in to the Virtual Private Cloud console.
2. Select Virtual Private Cloud in the left navigation bar.
3. In the VPC list, click the VPC ID you want to view.
   The details page shows the basic information of and the cloud resources contained in a VPC, such as Cloud Virtual Machine and Cloud Load Balancer. Click the resource number to enter the corresponding resource management interface.



Export VPC List

VPC supports the list export feature.

1. Log in to the Virtual Private Cloud console.
2. Select Virtual Private Cloud in the left navigation bar.
3. Click the export icon at the top right of the interface to download the VPC list in .csv format to your local device.



Delete VPC

> Note:
>
> Prerequisites for VPC deletion: The IP addresses of the VPC to be deleted are not in use, and there are no cloud resources (such as CVM, cloud databases (CDB) and gateways) in the VPC.

1. Log in to the Virtual Private Cloud console.
2. Select Virtual Private Cloud in the left navigation bar.
3. In the VPC list, click Delete in the Action column to the right of the VPC to be deleted, and confirm the operation.

Editing IPv4 CIDR

VPC supports adding one primary CIDR, and the primary CIDR cannot be changed after creation. When the primary CIDR cannot meet the business assignment, you can create secondary CIDR to expand the IP range. A VPC can support adding multiple secondary CIDRs.
Subnets support allocating IP ranges from either the primary or secondary CIDR. Regardless of whether a subnet belongs to the primary or secondary CIDR, different subnets within the same VPC are by default interconnected.

Usage Limitations

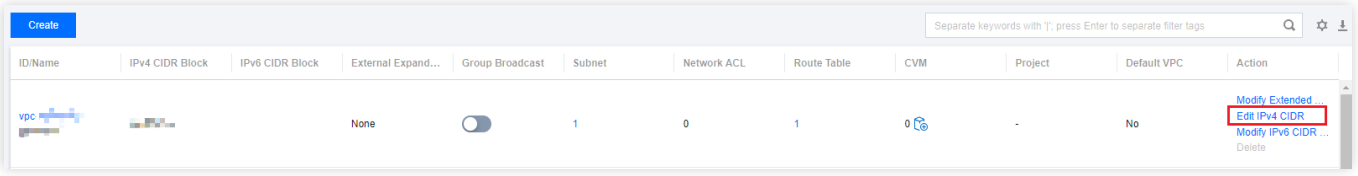
- Peering connection does not support the transmission of secondary CIDRs.
- The VPN gateway and standard direct connect gateway support the transmission of secondary CIDRs, but the direct connect gateway has the following restrictions:
  - The standard direct connect gateway supports the transmission of 10 secondary CIDRs.
  - The NAT-type direct connect gateway does not support the transmission of secondary CIDRs.

Create Secondary CIDR

1. Log in to the Virtual Private Cloud console.

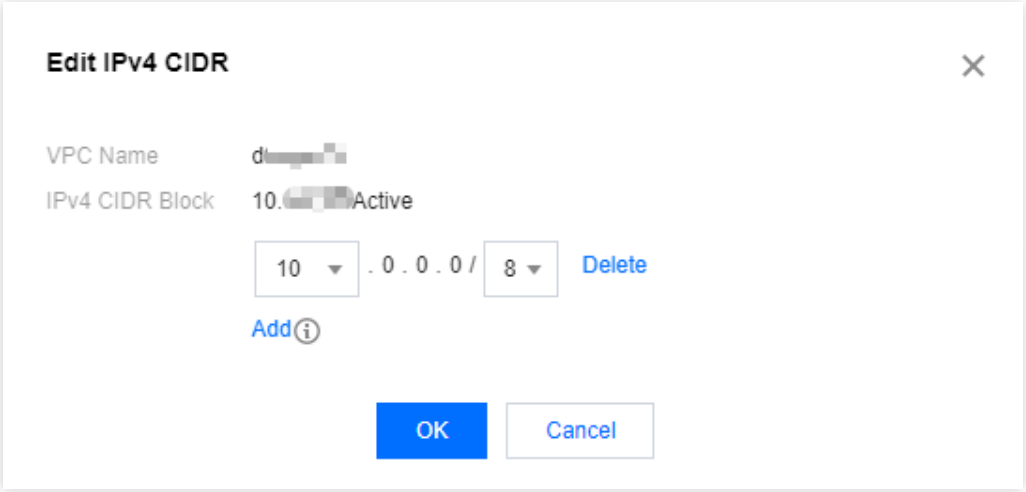
2. Select Virtual Private Cloud in the left navigation bar.

3. In the VPC list, click Edit IPv4 CIDR in the Action column to the right of the target VPC.



4. In the pop-up Edit dialog box, click Add and edit the secondary CIDR.

> Note:
>
> i. A maximum of 5 secondary CIDRs can be added.
> ii. Secondary CIDRs can overlap with the destination IP ranges of custom routing, but this needs to be done with caution because the routes of secondary CIDRs are Local routes, and Local routes have a higher priority than custom subnet routes.



5. Click OK to complete the creation of secondary CIDRs.

Delete secondary CIDR

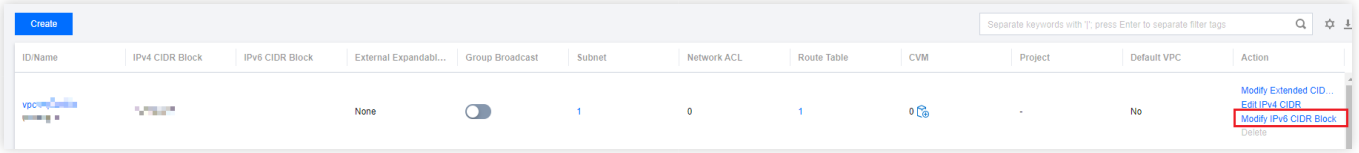
1. Log in to the Virtual Private Cloud console.
2. In the VPC list, click Edit IPv4 CIDR in the Action column to the right of the VPC of the secondary CIDR to be deleted.
3. In the pop-up edit dialog box, click Delete after the secondary CIDR.
4. Click OK to complete the deletion.

Editing IPv6 CIDR

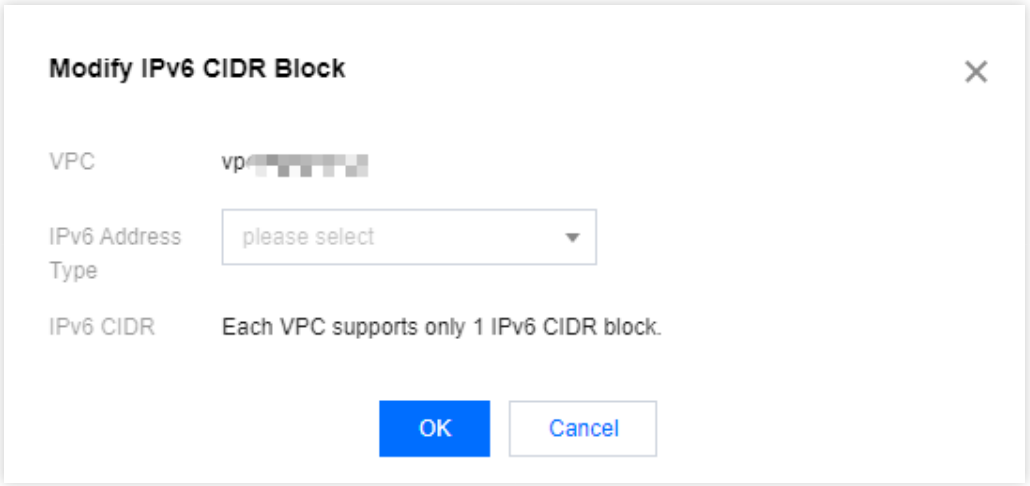
VPC supports IPv6 feature. When there are IPv6 service needs, you need to assign an IPv6 CIDR IP range to your VPC first, and then cloud resources in the VPC can be assigned IPv6 addresses within the VPC's IPv6 CIDR, enabling IPv6 communication for your services. This section describes how to assign IPv6 CIDR to the VPC through the console.

Assign IPv6 CIDR

1. Log in to the Virtual Private Cloud console.
2. Select Virtual Private Cloud in the left navigation bar.
3. In the VPC list, click Edit IPv6 CIDR in the Action column to the right side of the target VPC.



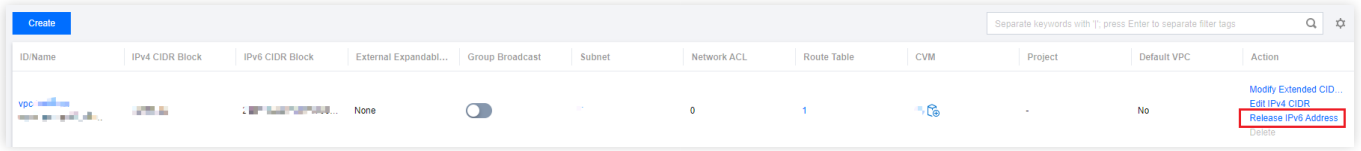
4. Select the IPv6 address type in the pop-up Edit dialog box. The system will assign an IPv6 CIDR of /56 to this VPC.



5. Click OK to complete the IPv6 CIDR assignment.

Release IPv6 CIDR

1. Log in to the Virtual Private Cloud console.
2. Select Virtual Private Cloud in the left navigation bar.
3. In the VPC list, click Release IPv6 Address in the Action column to the right side of the target VPC to release this IPv6 address range.


Create
Separate keywords with '|'; press Enter to separate filter tags
ID/Name
IPv4 CIDR Block
IPv6 CIDR Block
External Expandabl...
Group Broadcast
Subnet
Network ACL
Route Table
CVM
Project
Default VPC
Action
vpc
None
0
1
-
No
Modify Extended CID...
Edit IPv4 CIDR
Release IPv6 Address
Delete

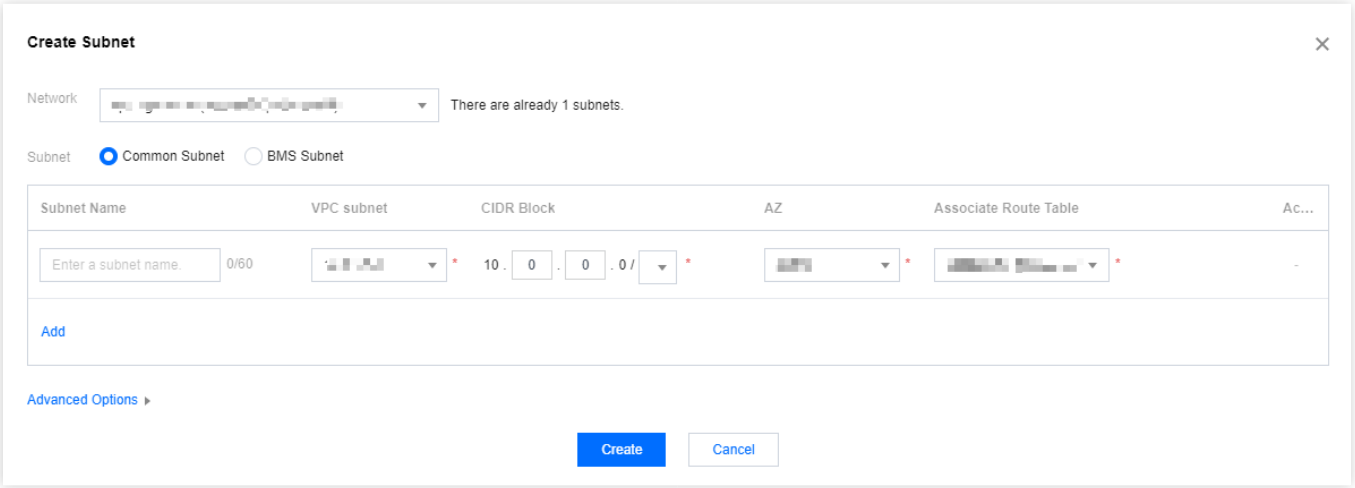
Managing Subnets

In the absence of subnets, when you purchase instances such as CVMs, the system will create a default subnet for you in the corresponding region. The default subnet can help you deploy your business more quickly and save time.
The default subnet has exactly the same features as the subnet you create yourself, and the default subnet does not occupy your quota in a region. If you no longer need the default subnet, you can delete it yourself.

Create a subnet

Users can create one or more subnets at the same time.

1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click Create and configure the subnet parameters in the pop-up Create Subnet dialog box.



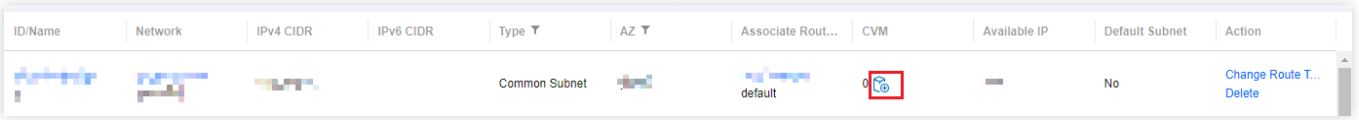
- Network: The VPC where the subnet resides.
- Subnet Name: Enter a custom subnet name within 60 characters.
- VPC subnet: The CIDR block of the selected VPC will be automatically displayed.
- CIDR Block: Set the CIDR block of the subnet (If there are auxiliary CIDRs under the VPC, auxiliary CIDRs can be used to create subnets.). The CIDR of a subnet must be part of the VPC CIDR block and cannot overlap with the CIDR block of other existing subnets under the VPC.
- AZ: Select an availability zone where the subnet resides.
- Associate Route Table: Select a route table to be associated. The subnet must be associated with a route table to control outbound traffic. The default route table of the VPC will be associated by default to ensure private network interconnection in the VPC. You can also select another route table within the VPC.
- Add a Line: Users can create one or more subnets. Click Add a Line to create multiple subnets at a time.

- Advanced Options: You can optionally set tags for the subnet to better manage subnet resources. Click Add to set multiple tags at a time. To delete, click the Delete icon.

4. After completing the configurations, click Create. Then subnets that have been successfully created will be displayed in the list.

Adding a CVM to the Subnet

1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Select the target subnet, and click the icon in the CVM column to add a CVM.

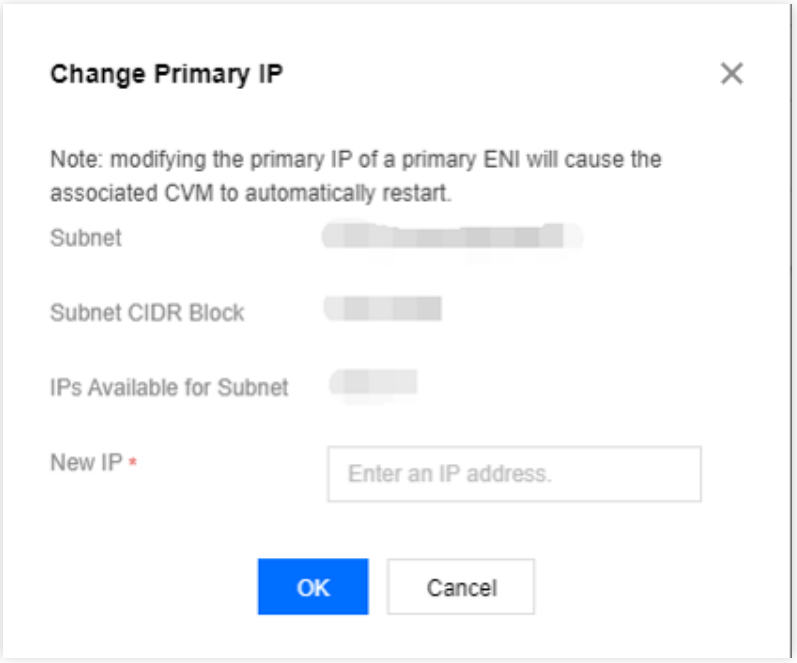


4. Complete the addition of the CVM instance as instructed on the page.

Modifying the Primary Private IP Addresses of the CVM

You can modify the primary private IP address of the primary ENI, but not that of secondary ENIs. The modification steps are as follows:

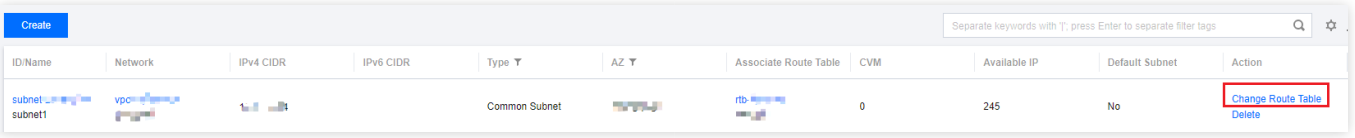
1. Log in to the Cloud Virtual Machine (CVM) console.
2. Click CVM in the left sidebar to enter the CVM Management page.
3. In the list, locate the target CVM, click the instance ID, and enter the Details page.
4. Select the ENI tab and click to expand the primary ENI.
5. In the Action column of the targeted primary private IP addresses, click Modify Primary IP.
6. In the pop-up box, enter a new IP address and click OK.



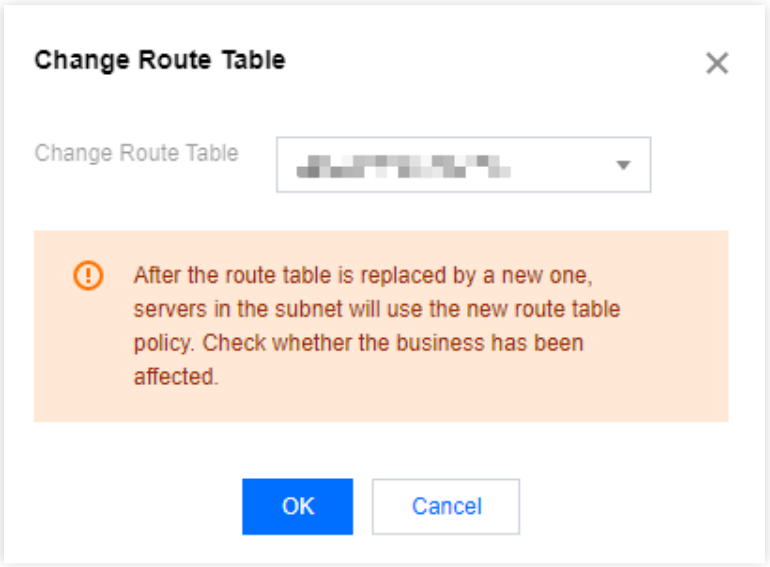
Changing the Subnet Route Table

Each subnet must be associated with a route table to specify the outbound route for the subnet. You can change the route table associated with a subnet in real-time. If you need to create a new route table, see Creating Custom Route Tables.

1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click Change Route Table in the Action column on the right side of the subnet that needs to change the route table.



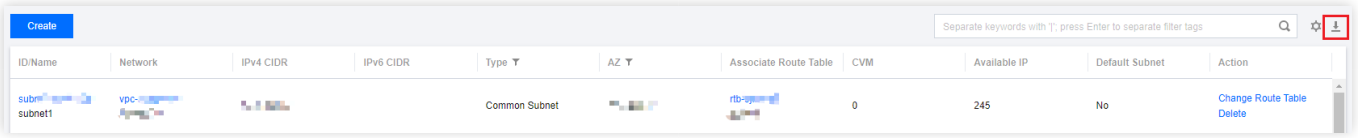
4. In the dropdown list, select the route table you want to change to and click OK.



Exporting Subnet Lists

VPC subnets support list export.

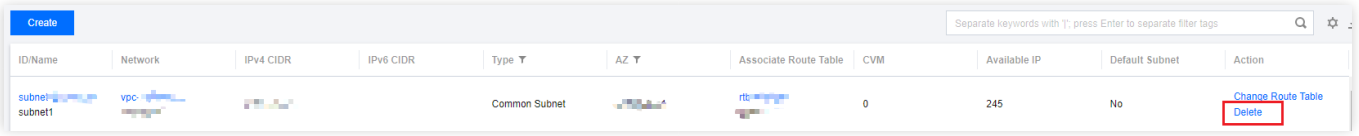
1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click the export icon in the upper right corner of the page to download the subnet list in CSV format to the local device.



Delete a subnet

> Note:
>
> Before deleting a subnet, make sure that the IPs in the subnet are not occupied and that there are no resources (such as CVMs and CDBs) in the subnet.

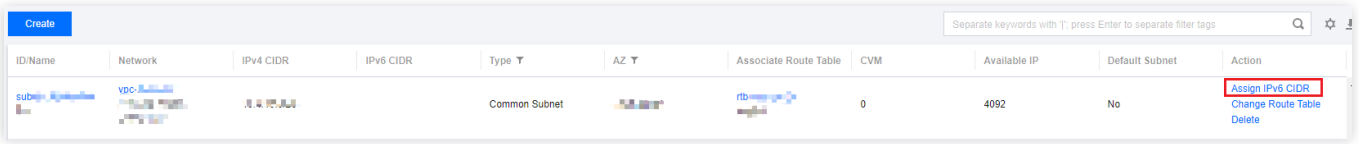
1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. In the list, locate the target subnet, click Delete in the Action column, and confirm the operation.



Allocating and Releasing IPv6 CIDR for a Subnet

Note: The premise for allocating the IPv6 CIDR to a subnet is that the VPC has obtained the IPv6 CIDR.

1. Log in to the Virtual Private Cloud console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Select a subnet and click Assign IPv6 CIDR. The system will allocate one /64 IPv6 CIDR.



4. Select a subnet from which you want to release the IPv6 CIDR, click Release IPv6 CIDR, and confirm the operation. The system will reclaim the IPv6 CIDR of the subnet.

Enabling or Disabling Multicast

Multicast is a mode of one-to-many communication, which can save businesses on the network bandwidth and reduce network load through point-to-multipoint efficient data transmission.

- Multicast: Cloud Platform supports multicast on the VPC dimension.

Overview

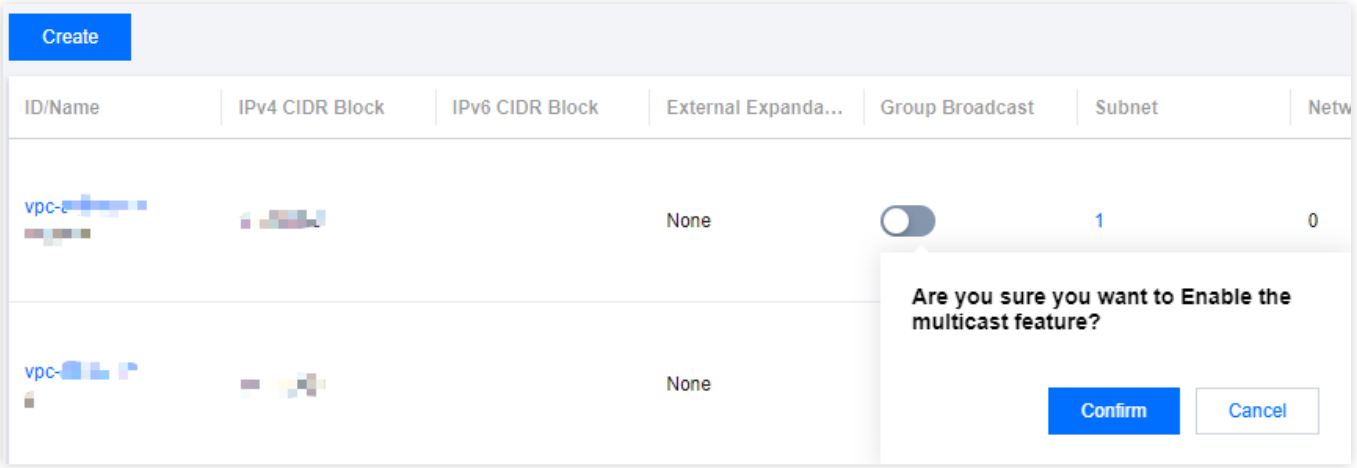
Multicast is mostly used in the financial and game industries:

- For the game industry, multicast is mainly used for heartbeat holding between multiple servers.
  In the unicast mode, the initiating server sends data to N servers separately. In the multicast mode, the server sends the same data to N servers at once, which reduces the server resource consumption and also the bandwidth resource of the backbone network.

Enabling or Disabling Multicast

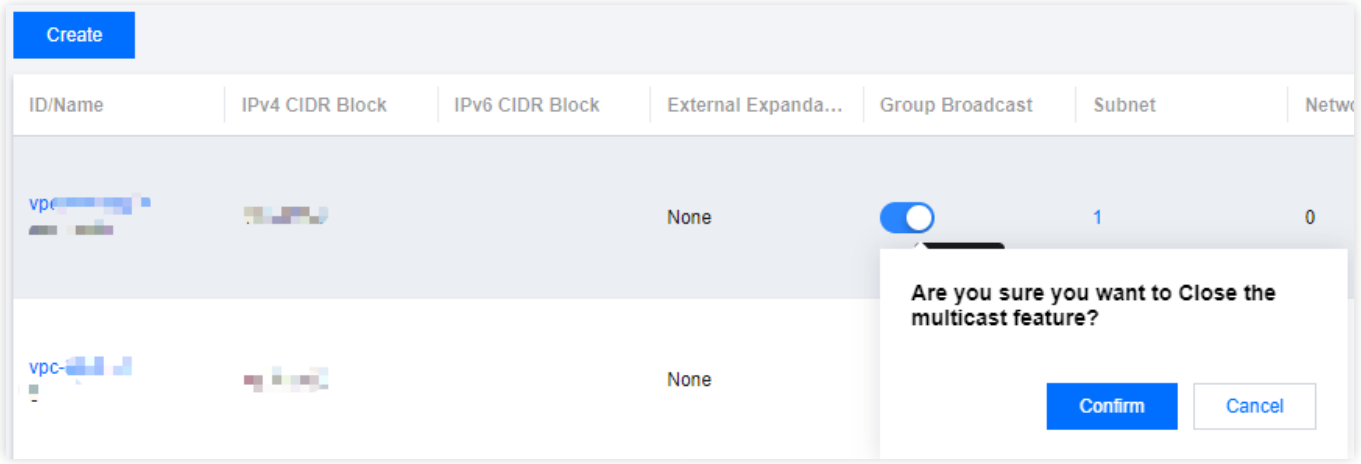
Enabling Multicast

1. Log in to the Virtual Private Cloud console.
2. In the list, locate the row of the VPC where you want to enable the Group Broadcast feature, click the button under Group Broadcast and confirm the operation.



Disabling Multicast

1. Log in to the Virtual Private Cloud console.
2. In the list, locate the row of the VPC where you want to disable the Group Broadcast feature, click the button under Group Broadcast and confirm the operation.


Create
ID/Name
IPv4 CIDR Block
IPv6 CIDR Block
External Expanda...
Group Broadcast
Subnet
None
1
0
None
Are you sure you want to Close the multicast feature?
Confirm
Cancel

Route Tables Overview

A route table consists of multiple routing policies that control the outbound traffic direction of subnets in the VPC. Each subnet can only be associated with one route table, while each route table can be associated with multiple subnets. You can create multiple route tables for subnets with different traffic routes.

Type

There are two types of route tables: default and custom.

- Default route table: When you create a VPC, the system automatically generates a default route table, which will be associated with subnets created later if no custom route table is selected. You cannot delete the default route table, but you can add, delete, and modify routing policies in it.
- Custom route table: You can create or delete a custom route table in the VPC. This custom route table can be associated with all the subnets to apply the same routing policy.

> Note:
>
> You can associate a route table when creating a subnet, or changing the route table after a subnet is created.

Routing Policies

A route table controls traffic routes by using routing policies. A routing policy consists of the destination, next hop type, and next hop:

- Destination: Specifies the destination IP range to which you want to forward the traffic. It should be an IP range. If you want to enter a single IP address, set the mask to 32 (for example, 172.16.1.1/32). The destination cannot be an IP range of the VPC where the route table resides, because the local route already allows private network interconnection in this VPC.
- Next hop type: Indicates the egress of data packets for the VPC. The next hop type of VPC supports NAT Gateway, Peering Connection, VPN Gateway, Direct Connect Gateway, CVM, and others.
- Next hop: Specifies the next hop instance (identified by the next hop ID) to which the traffic is forwarded, such as a NAT gateway in the VPC.

Routing Policy Priority

When there are multiple routing policies in a route table, the following routing priority applies, from high to low:

- Traffic within the VPC: Traffic within the VPC is matched first.
- Exact match route (the longest prefix match): When there are multiple routes in the route table that can match the destination IP, the route with the longest (exact) mask is matched to determine the next hop.
- Public IP address: If no routing policy is matched, a CVM instance can access the internet through its public IP address.

Priority of NAT Gateway and EIP

When a subnet is associated with a NAT gateway, and the CVM instance in the subnet has a public IP address (or EIP), the CVM instance accesses the internet through the NAT gateway by default (Because the priority of the exact match route is higher than that of the public IP address.). However, you can set a routing policy to allow the CVM instance to access the internet through its public IP address. For more information, see Adjusting the Priorities of NAT Gateways and EIPs.

Restrictions

Usage Limitations

- The default route table for each VPC cannot be deleted.
- After a VPC is created, the system automatically adds a default route to the route table, indicating resource interconnection in this VPC. This routing policy cannot be modified or deleted.

Destination	Next Hop Type	Next Hop
Local	Local	Local

- Dynamic routing protocols such as BGP and OSPF are not supported.

Quota Limitation

Resource	Limitation (Unit: count)
Number of route tables in each VPC	10
Number of route tables associated with each subnet	1
Number of routing policies per route table	50

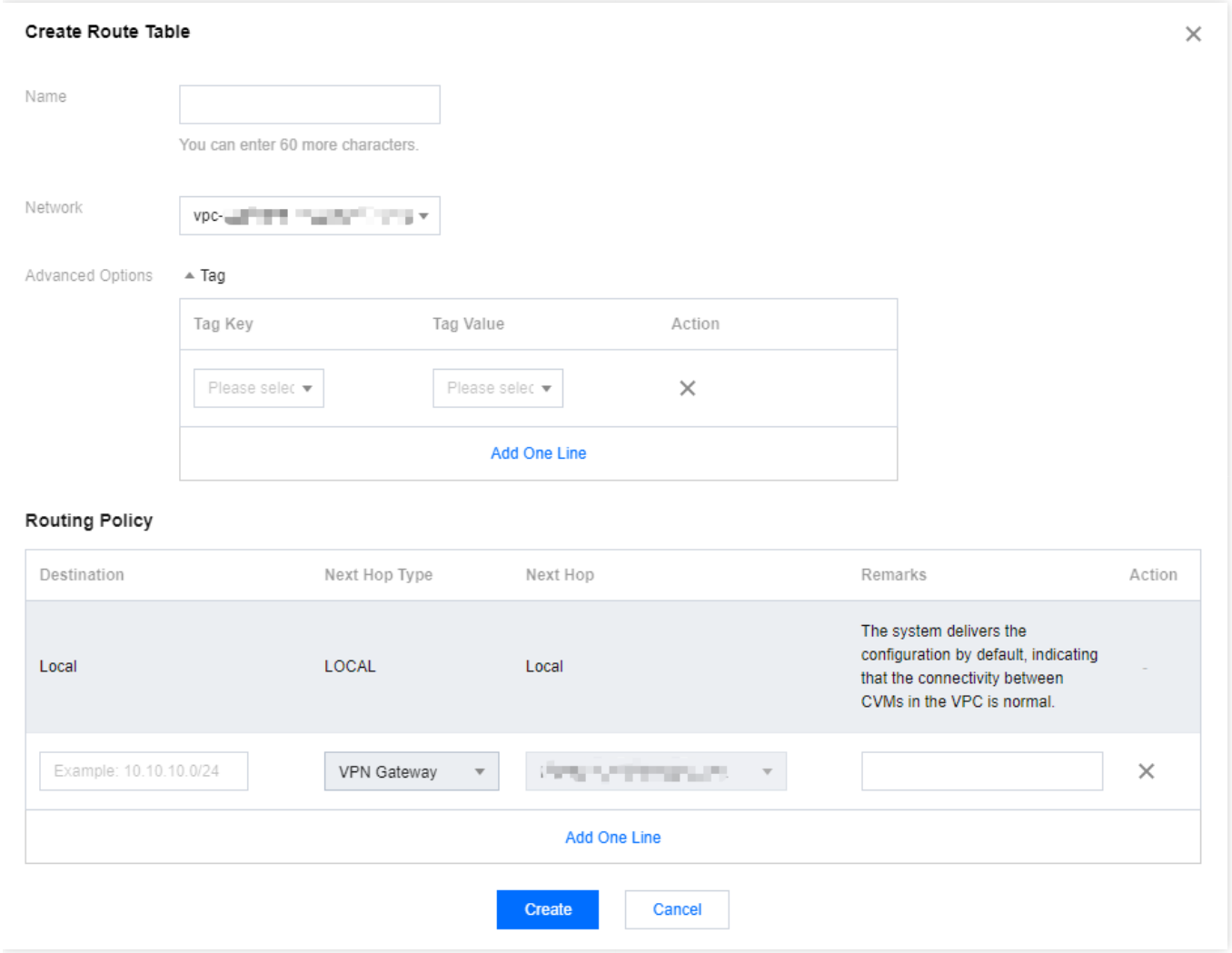
Managing Route Tables

Creating Custom Route Tables

In addition to the default route table automatically generated by the system, you can also create new custom route tables.

1. Log in to the VPC Console.
2. Click Route Table in the left sidebar to go to the route table management page.
3. Click Create.
4. In the pop-up window, enter the route table name, select the VPC to which the route table belongs, configure a routing policy, and click Create.

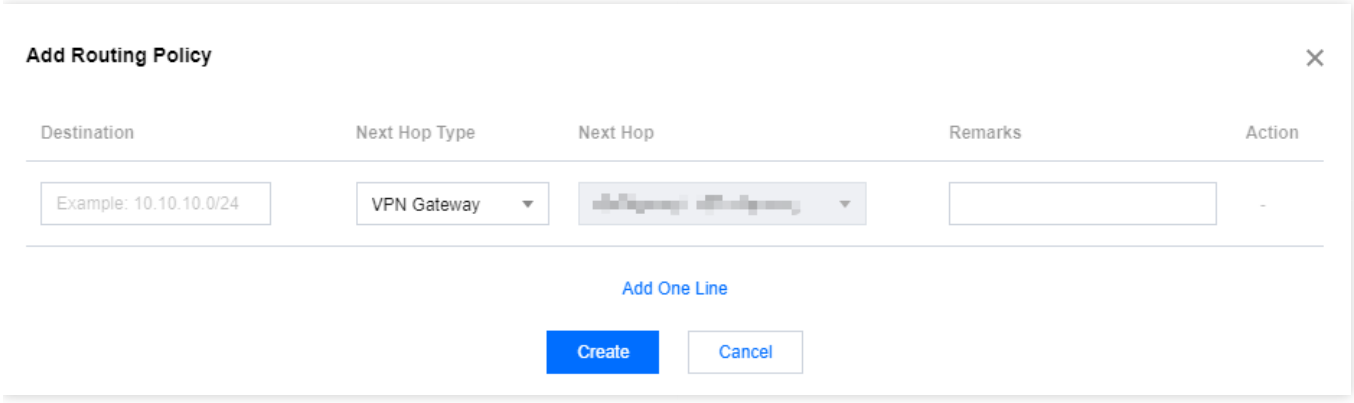
> Note:
>
> When the next hop is Peering Connection or Direct Connect Gateway, you can enter an IPv6 address.



Configuring Routing Policies

1. Log in to the VPC Console.
2. Click Route Table in the left sidebar to go to the route table management page.
3. In the list, click the route table ID that needs to be modified to enter the details page.
4. Click Add Routing Policy to add a route policy.
5. In the pop-up box, enter the destination IP range and select the next hop type (Public Network Gateway, VPN Gateway, Direct Connect Gateway, etc.) and the next hop ID.

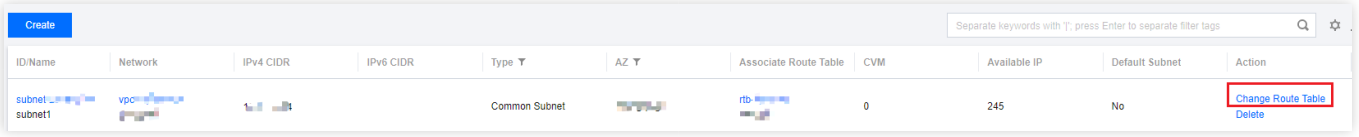
Configuration	Description
Destination	Specify the destination IP range to which you want to forward traffic.
Next Hop Type	Indicates the egress of data packets for the VPC. Supported types: - VPN Gateway: The traffic directed to a destination IP range is forwarded to a VPN Gateway. - Direct Connect Gateway: The traffic directed to a destination IP range is forwarded to a direct connect gateway. - Peering connections: The traffic directed to a destination IP range is forwarded to the VPC peer of a peering connection. - NAT Gateway: The traffic directed to a destination IP range is forwarded to a NAT Gateway. - CVM: The traffic directed to a destination IP range is forwarded to a public network gateway in the VPC (a CVM instance with forwarding enabled). - Public IP of CVM: The traffic directed to a destination IP range is forwarded to the public IP address (including EIPs) of a CVM instance in the VPC.
Next Hop	Specify the next hop instance to which the traffic is redirected, such as a gateway or CVM IP.



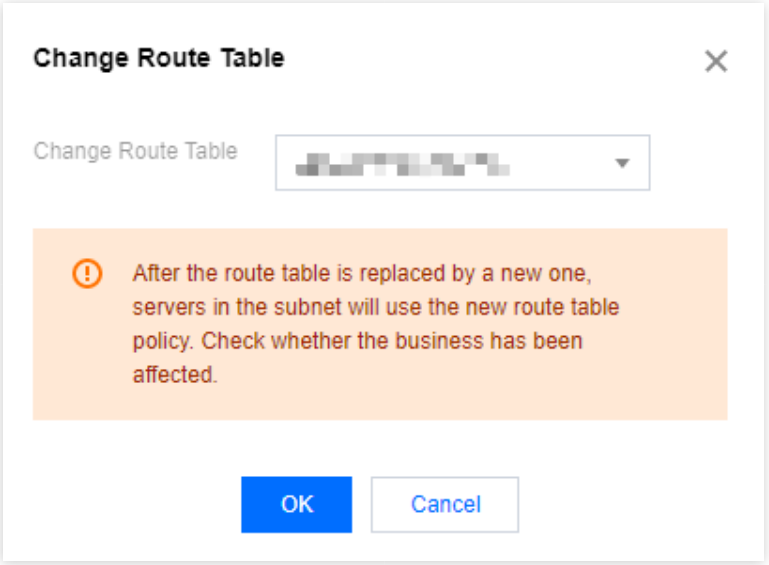
6. Click OK and the routing policy takes effect immediately.
7. (Optional) After adding a custom routing policy, you can click Edit or Delete in the routing policy operation column to modify or delete the routing policy.

Changing the Subnet Route Table

1. Log in to the VPC Console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click Change Route Table in the Operation column on the right side of the subnet that needs to change the route table.



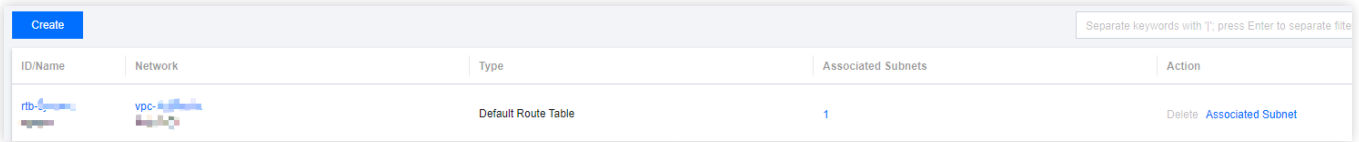
4. In the pop-up window, select the new route table and click OK.



Deleting Custom Route Tables

The system-generated default route table cannot be deleted, but custom route tables can be created, modified, and deleted.

1. Log in to the VPC Console.
2. Click Route Table in the left sidebar to go to the route table management page.
3. Click Delete in the Operation column on the right side of the route table that you want to delete.



IP and Network Interface
Elastic Public IP (EIP)

Elastic Public IP Address (EIP), also known as an Elastic IP address or Elastic IP. With EIP, you can quickly map an address to another instance (or NAT gateway instance) in your account for failure isolation. With EIP, you can quickly map an address to another instance (or NAT gateway instance) in your account for failure isolation.

You can keep an EIP in your account until you release it. Unlike common public IPs, which are tied to cloud servers and follow their lifecycle, elastic public IPs can be decoupled from cloud servers and operated on as standalone cloud resources. For example, if you need to retain a public IP address that is strongly related to your business, convert it to an EIP and keep it in your account.

Managing ENI

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be freely migrated among multiple CVMs. ENIs are very helpful in configuring and managing networks and building highly reliable network solutions.

You can bind multiple ENIs to a CVM to implement a high-availability network solution(Only ENIs in the same availability zone can be bound, and the specific number that can be bound is determined by the server specification.). You can also bind multiple private IP addresses to an ENI to deploy a single host with multiple IPs.

HAVIP
Overview

A high availability virtual IP (HAVIP) is a private IP address assigned from the CIDR block of a VPC subnet. It is usually used together with high-availability software, such as Keepalived and Windows Server Failover Cluster, to build a highly available primary/secondary cluster.

> Note:
>
> - To guarantee the CVM high availability in a primary/secondary cluster, we recommend assigning CVMs to different host machines using placement groups.
> - The high availability software should support sending ARP messages.

Features

- You can apply for multiple HAVIP addresses in the console for each VPC.
- You must bind the HAVIP in CVM's configuration file.
- The HAVIP is subnet-specific and can only be bound to a server under the same subnet through announcement.

Architecture and Principle

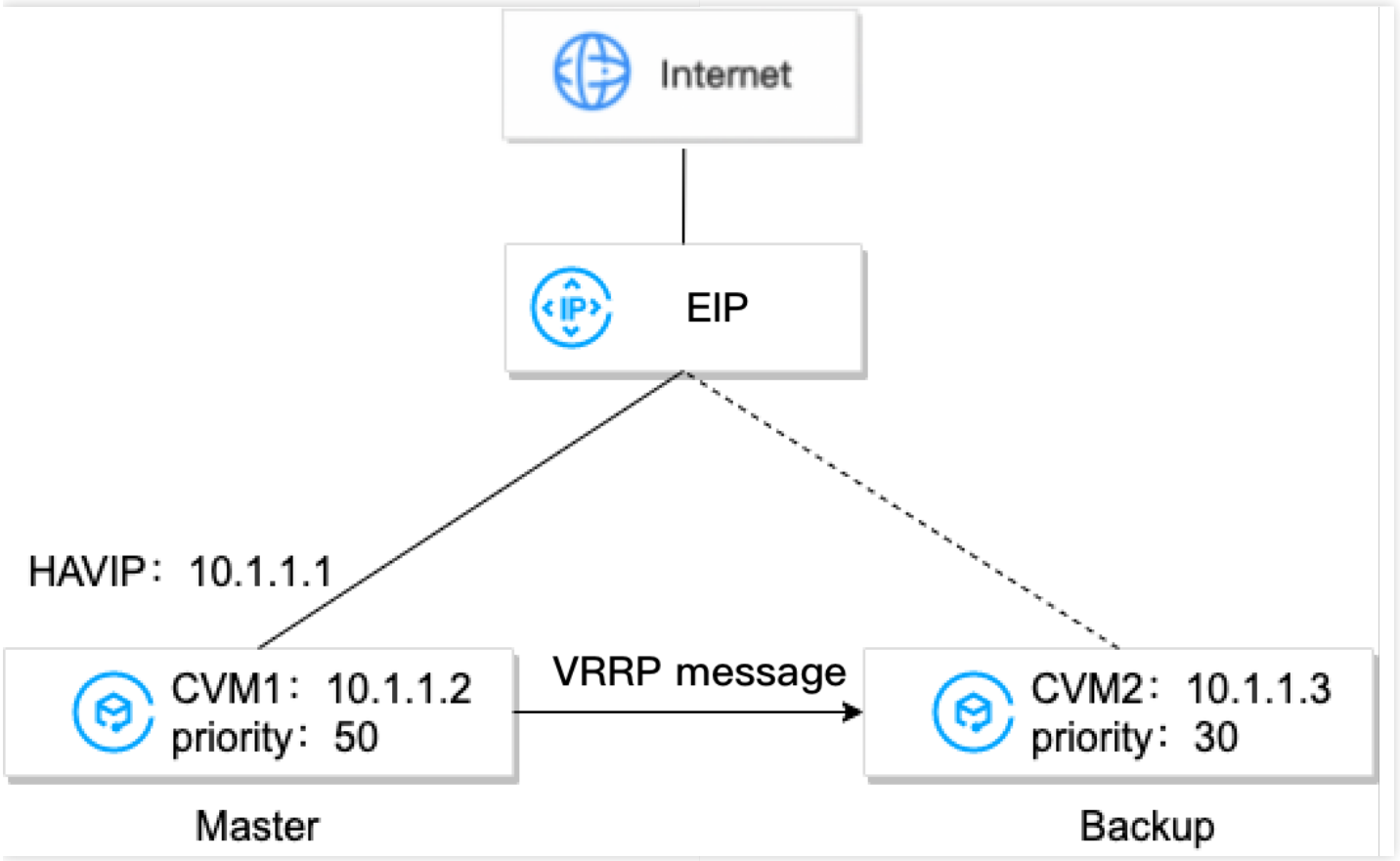
Typically, a high availability primary/secondary cluster consists of 2 servers: an active primary server and a standby secondary server. The two servers share the same VIP (virtual IP). The VIP can only work on one primary server at the same time. When the primary device fails, the secondary server will take over the VIP to continue providing services.

- In traditional physical networks, Keepalived's VRRP protocol can be used to negotiate the primary/secondary status. The principle is that the primary device periodically sends free ARP packets to refresh the MAC table of the up-link switch or terminal ARP table, triggering the migration of the VIP to the primary device.
- In a VPC, a high availability primary/secondary cluster can also be implemented by deploying Keepalived on CVMs. However, a CVM instance usually cannot obtain a private IP address through ARP announcement due to security reasons such as ARP spoofing. The VIP must be a HAVIP applied from Cloud Platform, which is subnet-specific. Therefore, a HAVIP can only be bound to a server under the same subnet through announcement.

  > Note:

> Keepalived is a VRRP-based high availability software. To use Keepalived, first complete its configuration in the Keepalived.conf file.

The following figure shows the HAVIP architecture.



According to the example figure, CVM1 and CVM2 can be built into a high availability primary/secondary cluster with the following steps:

1. Install Keepalived on both CVM1 and CVM2, configure HAVIP as VRRP VIP, and set the priorities of the primary and secondary servers. Larger values represent higher priorities.
2. Keepalived uses the VRRP protocol to compare the initial priorities of CVM1 and CVM2 and determines the Master server. In this case, CVM1 is the Master server and CVM2 is the Backup server.
3. The Master server sends out ARP messages, announces the VIP (a HAVIP), and updates VIP to mac mappings. In this case, the CVM1 is the Master server and provides services by using the private IP address (HAVIP) for communication. You can see the HAVIP is bound to the Master server CVM1 in the HAVIP console.
4. (Optional) Bind an EIP to the HAVIP in the console to implement communication over the public network.
5. The Master server periodically sends VRRP messages to the Backup server. If the Master server fails to send VRRP messages within a certain period, the Backup server will be set as Master and send out ARP update messages that carry its MAC address. In this case, CVM2 becomes the Master server to

provide communication services and handle external access requests. You will see that the CVM bound to the HAVIP changes to CVM2 in the HAVIP console.

Common Use Cases

- Cloud Load Balancer HA
  To deploy Cloud Load Balancers (CLB), you will generally take HA between CLB instances and configure real servers as a cluster. Therefore, you must deploy and use HAVIP as a virtual IP between two CLB servers.
- Relational Database Primary/Secondary
  If Keepalived or Windows Server Failover Cluster are used between two databases to build a highly available primary/secondary cluster, use HAVIP as a virtual IP.

FAQs

Why should I use HAVIP along with Keepalived in a VPC?

Some public cloud vendors do not support binding a private IP address to CVM through ARP announcement due to security reasons such as ARP spoofing. If you directly use a private IP address as virtual IP in the Keepalived.conf file, Keepalived will not be able to update the IP to MAC mapping during the primary/secondary server virtual IP switch. In this case, you have to call an API to switch the IP. Using Keepalived configuration as an example, the IP configurations are as follows:
Using Keepalived configuration as an example, the IP configurations are as follows:

```
vrrp_instance VI_1 {
    state BACKUP          #Backup
    interface eth0        #ENI name
    virtual_router_id 51
    nopreempt               #Non-preempt mode
    #preempt_delay 10
    priority 80
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.17.16.7   #Private IP address of the local device
    unicast_peer {
        172.17.16.13          #IP address of the peer device. For example: 10.0.0.1
    }
```

```
    virtual_ipaddress {

        172.17.16.3  #Enter the HAVIP address you have applied for in the console.

    }

    garp_master_delay 1
    garp_master_refresh 5

    track_interface {
        eth0
    }

    track_script {
        checkhaproxy
    }
}
```

If there is no HAVIP, the following section of the configuration file will be invalid.

```
    virtual_ipaddress {
      172.17.16.3 #Enter the HAVIP address you have applied for in the console.
    }
```

Restrictions

Usage Limitations

- The occupation of an HAVIP can be declared by the backend CVM, but you cannot manually bind HAVIPs to a specified server in the console (The experience is consistent with that of a traditional physical machine.).
- The backend RS but not the HAVIP determines whether to migrate based on the configuration file negotiation.
- Only supports VPC.
- Heartbeat detection must be done by an application on the CVM, but not by the HAVIP, which serves only as a floating IP address declared by ARP (The experience is consistent with that of a traditional physical machine.).

Quota Limitations

Resources	Limitation
Default HAVIP quota in each VPC	200

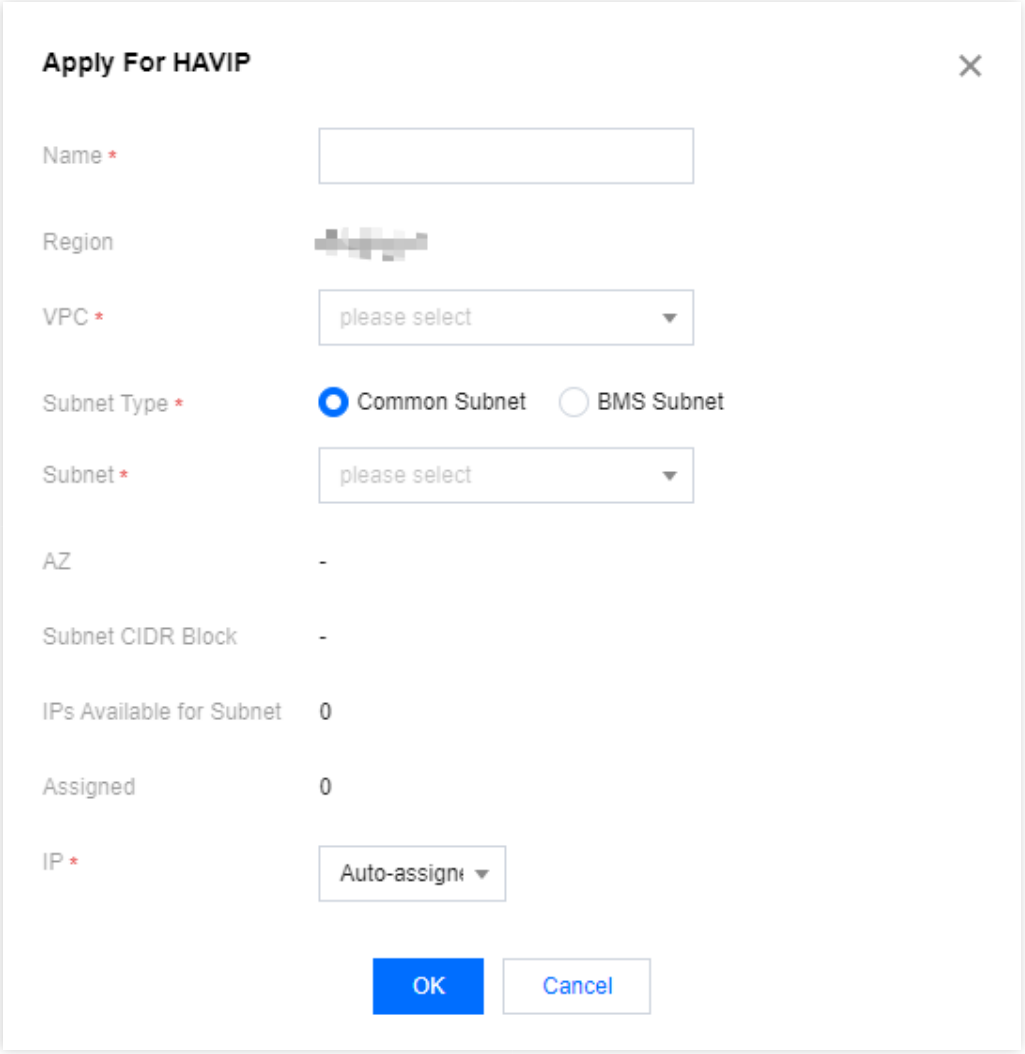
Creating a High Availability Virtual IP

This section explains how to create a High Availability Virtual IP (HAVIP) in the console and subsequent operations such as configuration in third-party software.

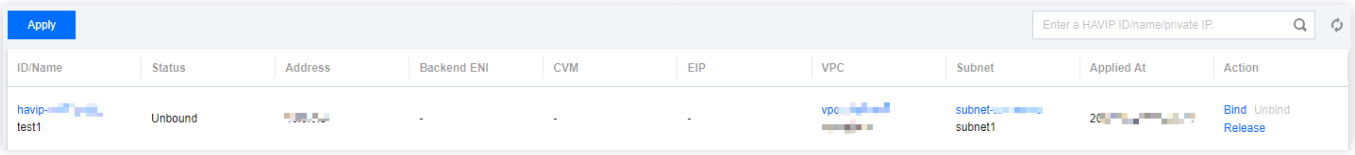
Directions

1. Log in to the VPC console, and in the left navigation pane, select IP & Network Interfaces > High Availability Virtual IP.
2. On the HAVIP Management page, click Apply.
3. In the Apply for High Availability Virtual IP dialog box that appears, configure the parameters of the HAVIP.

- Name: Enter the name of the HAVIP.
- VPC: Select the private network where the HAVIP will be created.
- Subnet: HAVIP has subnet properties, so select the subnet.
- IP Address: Supports auto-allocation and manual input. If you choose auto-allocation, the system will assign an IP address from the subnet; if you choose manual input, you need to provide an available IP address within the subnet IP range and avoid system-reserved IPs. For example, if the subnet range is 10.0.0.0/24, the available intranet IP range would be 10.0.0.2 - 10.0.0.254.

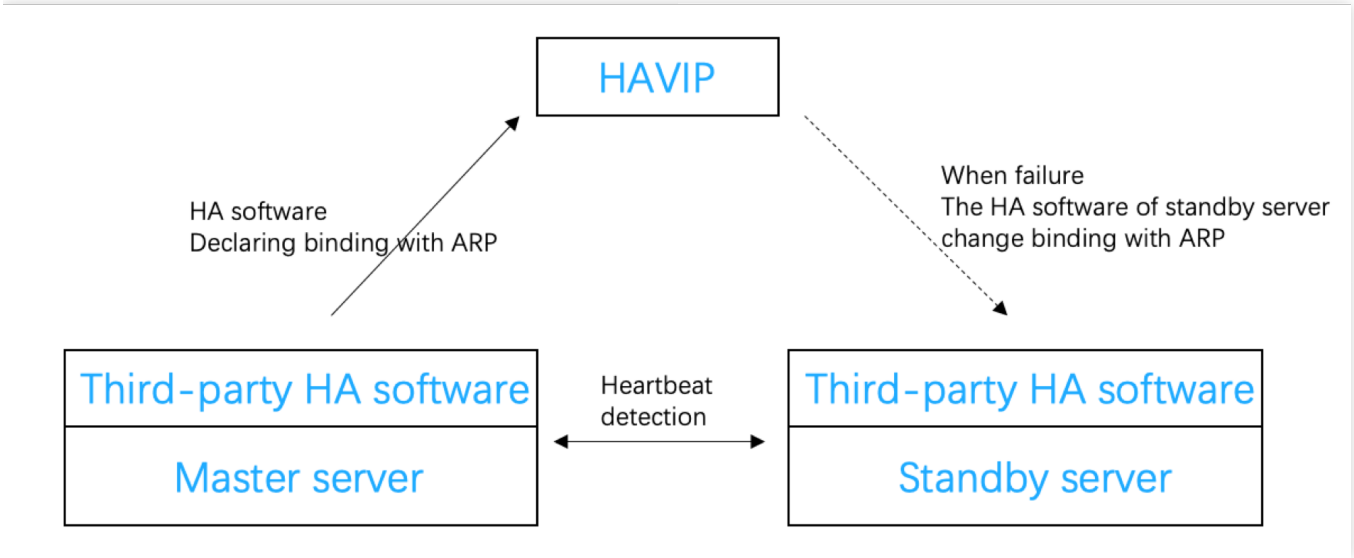


4. Click OK to create the HAVIP, which will be displayed in the list with a status of Unbound.



Subsequent Operations

HAVIP is used in conjunction with third-party HA software. After creation, further configuration is required in the third-party HA software. HAVIP is merely an object to be operated on, serving as a declare-bindable private IP. The binding and unbinding operations are initiated by the third-party HA software, not from the HAVIP console. To specify, in third-party HA software, designate HAVIP as a floating VIP (Virtual IP Address), then the third-party HA software specifies the network card to be bound through the ARP protocol. An illustration is as follows:



In a traditional physical device environment, all private IP addresses can be bound to the NIC through the ARP protocol by default and designated as floating IPs in the HA software. However, in a cloud environment, ARP protocol is prohibited for ordinary private IPs. Attempting to designate an ordinary private IP as a floating IP in the HA software will result in a drift failure. Therefore, in the HA software within the CVM, HAVIP needs to be specified as a floating VIP. This operation is exactly the same as the third-party HA software on non-cloud platforms.

> Note: Common HA software programs include: Linux HeartBeat, Keepalived, Pacemaker, and Windows MSCS.

When specifying a VIP in the configuration file of the HA software, you only need to enter the HAVIP that you created:

```
vrrp_instanceVI_1 {
# Select proper parameters for the primary and secondary CVMs.
    state MASTER #Set the initial status to Backup.
    state MASTER              #The ENI such as `eth0` used to bind a VIP
    virtual_router_id 51 #The virtual_router_id value for the cluster
        virtual_router_id 51       #Set to non-preempt mode
        preempt_delay 10          #Set the preempt delay to 10 minutes.
    priority 100              #Set the priority. The larger the value, the higher the priority.
    advert_int 1              #Check interval. The default value is 1 second.
    authentication {          #Set authentication
        auth_type PASS         #Authentication method
        auth_pass 1111         #Authentication password
    }
        unicast_src_ip 172.16.16.5 #Set the private IP address of the local device.
        unicast_peer{
        172.16.16.6              #IP address of the peer device
        }
    virtual_ipaddress {
```

```
    172.16.16.12            # <font color="red">Set the HAVIP as a floating IP</font>
}
}
```

After HAVIP is configured in the HA software of CVM, the HAVIP status will change to Bound with CVM in the console.

For common configuration examples, please refer to:

- Best Practices-Building High Availability Primary/Secondary Cluster by Using HAVIP + Keepalived
- Best Practices-Creating a High-availability Database by Using HAVIP + Windows Server Failover Cluster

Documentation

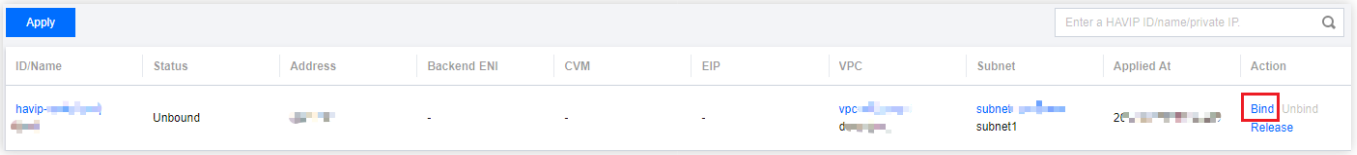
Similar to a private IP address, an HAVIP can also be bound with or unbound from an EIP in the VPC console. If you need public network communication, see Binding or Unbinding EIP. If not, you do not need to bind EIPs.

Binding or Unbinding EIP

High Availability Virtual IP (HAVIP), similar to regular internal IPs, supports binding or unbinding an Elastic IP (EIP) via the console. If you have a need for public network communication, you can refer to this document to bind an EIP. If you do not have a requirement for public network communication, you can skip this section.

Binding EIP

1. Log in to the VPC console, and in the left navigation pane, select IP & Network Interfaces > High Availability Virtual IP.
2. On the HAVIP management page, select the HAVIP to which you want to bind the EIP, and click Bind in the right-hand operation column.



3. In the Bind EIP dialog box that appears, click on the EIP you want to bind.

> Note:
>
> - If there are no available EIPs, please create an EIP in the EIP console before performing the binding operation. One HAVIP can only bind to one EIP.
> - If the HAVIP is not bound to a cloud server instance, the EIP bound to this HAVIP will be in an Idle state, and idle resource fees will be charged by the system. For common configuration examples, please refer to:
>   - Best Practice - Build High Availability Active/Standby Clusters with HAVIP + Keepalived
>   - Best Practice - Build High Availability DB with HAVIP + Windows Server Failover Cluster

4. Click Confirm to complete the EIP binding.

Unbinding EIP

1. Log in to the VPC console, and in the left navigation pane, select IP & Network Interfaces > High Availability Virtual IP.
2. On the HAVIP management page, select the HAVIP from which you want to unbind the EIP, and click Unbind in the right-hand operation column.
3. In the Unbind Elastic Public IP dialog box that appears, please be aware of the following risks, confirm them, and then click Confirm to complete the unbinding of the EIP.

   > Note:

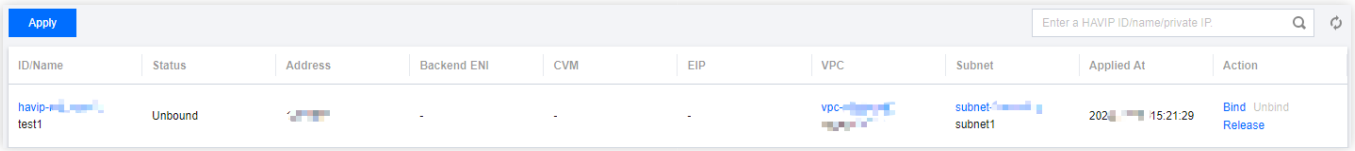
- Unbinding an EIP will affect public network services. Please assess the impact on your business and make necessary preparations.
- After unbinding, the EIP will enter an idle state, and the system will charge idle resource fees. If not needed, you can release the EIP directly.

Querying Highly Available Virtual IP

In the HAVIP console, you can view detailed information about all HAVIPs in the specified region.

Directions

1. Log in to the VPC console.
2. Select IP And Network Card > HAVIP from the left navigation pane to enter the Highly Available Virtual IP interface.
3. View detailed information on all HAVIPs that have been applied for in this region.



The fields are defined as follows:

- ID/Name: After HAVIP creation, the system automatically generates an ID. Clicking the ID allows access to the basic information interface of the HAVIP. The name is a user-defined name during creation.
- Status: Indicate whether the HAVIP has been specified as a migratable VIP in the HA software configuration file of the cloud server. If configured successfully, the status displays as Bound to Cloud Server. If not configured or configuration fails, the status displays as Unbound.
- Address: HAVIP address.
- Backend ENI: The Elastic Network Interface (ENI) ID of the cloud server bound to the HAVIP. If the HAVIP is not bound to a cloud server, this field displays as -.
- CVM: The cloud server ID bound to the HAVIP. If the HAVIP is not bound to a cloud server, this field displays as -.
- EIP: The Elastic IP (EIP) bound to the HAVIP. If the HAVIP is not bound to an EIP, this field displays as -.
- VPC: The VPC where the HAVIP is located.
- Subnet: The subnet where the HAVIP is located.
- Applied At: The time when the HAVIP was applied for.
- Action: Operations that can be performed on the HAVIP, including Binding, Unbinding, and Releasing.
    - Binding: Used to bind an EIP.
    - Unbinding: Used to unbind an EIP.
    - Releasing: Used to release the HAVIP.

4. In the search box on the right side, you can enter the ID, name, or internal IP address for quick search.
5. Click the refresh icon in the upper right corner to refresh the interface.

Releasing Highly Available Virtual IP

If HAVIP is no longer needed, you can release it directly in the console according to this document.

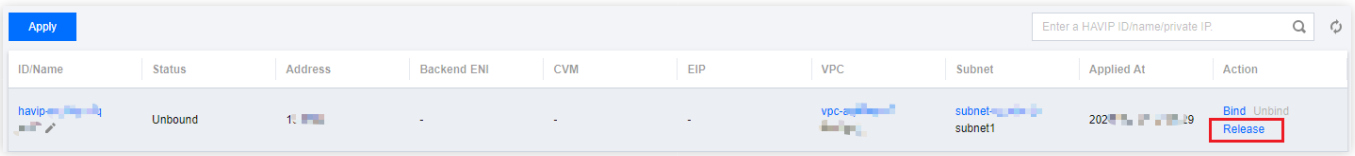
Prerequisites

Only HAVIPs that are not bound to cloud servers can be released.

> Note:
>
> For HAVIPs that are already bound to cloud servers, if you need to release them, please first unbind the HAVIP in the third-party HA software configuration file on the cloud server, and then you can release it in the console.

Directions

1. Log in to the VPC console.
2. In the left navigation pane, choose IP And Network Card > HAVIP, and find the HAVIP that needs to be released in the list.
3. Click Release in the action bar.



4. In the confirmation dialog box that appears, click Confirm to complete the release of the HAVIP.

VPC Connection Overview

Connect to the public network

You can use the following products or features to achieve access between VPC and the public network.

Product	Features	Features
Ordinary Public IP	Support cloud servers accessing the internet or users accessing cloud servers from the public network.	Only available when purchasing cloud servers; if not assigned during purchase, you can use EIP or NAT Gateway.
Elastic Public IP (EIP)	A single cloud server can bind one or more EIPs to access the internet or be accessed from the public network.	A type of IP resource that can be independently purchased and owned. Can be dynamically bound and unbound with cloud servers and NAT gateways. You can adjust the bandwidth limit of EIP according to your business needs.
NAT Gateway	SNAT: Supports multiple cloud servers under the same VPC to access the internet through the same public IP. DNAT: Maps the private IP, protocol, and port of cloud servers within the VPC to external IP, protocol, and port, enabling services on cloud servers to be accessed from the public network.	NAT Gateway can be used for multiple cloud servers to access the internet. You can adjust the bandwidth limit of NAT Gateway according to your business needs.
Cloud Load Balancer (CLB)	By evenly distributing access traffic to multiple cloud servers to provide services externally.	Provides layer-4 and layer-7 CLB features based on ports, supporting users to access CVMs from the Internet through CLB (CLB). It eliminates single points of failure and improves the availability of application systems.
Public Gateway	A type of cloud server with forwarding capabilities enabled. Cloud servers without public IP addresses can access the internet through public gateways located in different subnets.	Unlike cloud servers with regular public IP addresses, public gateways can forward traffic from other subnet cloud servers to the internet, while cloud servers with regular public IP addresses can only meet their own internet access needs. If you need to use it, you need to refer to the Configure Cloud Server as Public Gateway page for self-

Product	Features	Features
		configuration.

Connect to other VPCs

You can use the following products or features to achieve communication between VPCs and one-way access to VPCs.

Product	Features	Features
Peering connection	Used for intra-network communication between two VPCs.	The CIDRs of the two VPCs must not overlap. Manual configuration of routes is required. Support communication between VPCs in different accounts and regions.
Private Connection	Used for one-way service access between two VPCs.	It supports sharing application services deployed in VPC with other VPCs in the same account or across accounts through private connections.

Connect to local data centers

You can use the following products or features to interconnect VPC with an on-premises data center.

Product	Features	Features
VPN Connection	Establish a connection between the on-premises data center and VPC through an encrypted channel over the internet.	Network quality depends on the public internet. Network transmission is encrypted based on IKE protocol with pre-shared keys.
Direct Connect	Connects VPC and the on-premises data center using a physical dedicated connection.	Provide reliable network latency. Exclusive network link with high security. Supports configuring network address translation services on the gateway to resolve address conflicts.

Connect to the classic network

You can use the following products or features to interconnect VPC with the classic network.

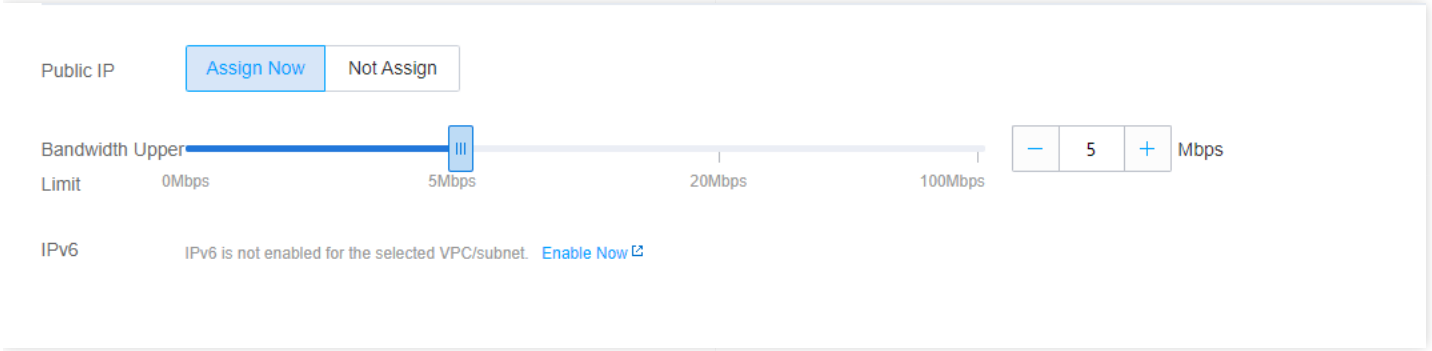
Product	Features	Features
Classic Network Interconnection	Associates cloud servers in the classic network with a specified VPC, allowing cloud servers in the classic network to communicate with cloud servers, databases, and other cloud services in the VPC.	Cloud servers in the classic network can access cloud resources such as cloud servers, cloud databases, internal load balancers, and cloud caches in the VPC. Cloud servers in the VPC can only access interconnected cloud servers in the classic network and cannot access other computing resources in the classic network.
Terminal Connection	Enable instances in the VPC to communicate with non-cloud server instances in the classic network through the intranet.	Support basic network products for connection include: CLB, MySQL, Memcached, Redis®, and MongoDB. Terminal connections do not support cross-region or cross-account connections. If you need to establish a terminal connection, please submit a ticket for assistance.

Connecting to the Public Network

You can interact with the internet using common public IP addresses, elastic public IP addresses, NAT gateways, and load balancers.

Normal Public IP

When creating a cloud server instance, you can choose to allocate a common public IP address to the instance. The system will assign an IP address to your cloud server, allowing it to access and be accessed from the internet.
Common public IPs cannot be dynamically bound or unbound with resources like CVMs. However, you can convert a common public IP to an elastic public IP.



Elastic Public IP (EIP)

An EIP is an independently owned IP resource. Unlike common public IPs, which are tied to cloud servers and follow their lifecycle, elastic public IPs can be decoupled from cloud servers and operated on as standalone cloud resources.
For operations such as application, binding, and release of elastic public IPs, see EIP - Operation Steps.
EIP has the following advantages:

- Independently Held Resources
  EIPs can be independent resources in your account, eliminating the need to purchase them in conjunction with cloud servers. They can be operated on as standalone cloud resources.
- Elastic Binding and Unbinding of Resources
  Elastic public IPs can be dynamically bound and unbound with cloud servers and other resources, offering flexibility and high availability.

NAT Gateway

If you have multiple cloud servers that need to access the internet through a single public IP, NAT gateway can meet your requirements. NAT Gateway provides SNAT and DNAT functions for cloud servers within private networks, facilitating the setup of public network egress and service provision.
For configuration operations related to NAT gateway, please refer to NAT Gateway.
NAT Gateway has the following advantages:

- Secure Public Network Access
  NAT Gateway provides SNAT and DNAT functions, allowing communication with the internet while hiding the IP addresses of hosts within the VPC, thus ensuring security.
- High Availability
  NAT Gateway features dual-machine hot standby and automatic hot switch, supporting up to 5Gbps forwarding capacity, providing robust support for large-scale public network applications.
- Flexible Configuration
  You can modify the specifications of the NAT Gateway according to your needs, allowing for flexible configuration.

Cloud Load Balancer (CLB)

Cloud Load Balancer (CLB) is a service for distributing traffic among multiple cloud servers. Cloud Load Balancer can expand the service capacity of application systems externally through traffic distribution and enhance the availability of application systems by eliminating single points of failure.
For purchasing and configuring a load balancer, please refer to Cloud Load Balancer - Quick Start Guide.
Cloud Load Balancer has the following advantages:

- High Performance of Single Cluster
  A set of CLB clusters consists of multiple physical servers, with availability reaching up to 99.95%. The cluster system also features the functions of removing faulty instances and selecting healthy instances to ensure the normal operation of backend server businesses.
- Safety and Stability
  CLB relies on the Great Wall distributed defense system to defend against the vast majority of network attacks (such as DDoS attacks), achieving second-level cleansing for traffic attacks, greatly avoiding situations such as IP blocking and bandwidth saturation.

Public Gateway

A public gateway is a cloud server with forwarding capabilities enabled. Cloud servers in a private network

without public IPs can access the internet through public gateways located in different subnets. The public gateway server performs source address translation for public network traffic. All traffic from other cloud servers accessing the internet passes through the public gateway, with their IP addresses being converted to the IP address of the public gateway server.

For configuring the public gateway, please refer to Configure Public Gateway.

Connecting to Other VPCs

You can establish connectivity between different VPCs through peering connections.

Peering connection

Peering Connections facilitate bidirectional communication between two VPCs, supporting both intra-account and inter-account peering.

- Intra-Account Peering Connection Creation
- Inter-Account Peering Connection Creation

Private Connection

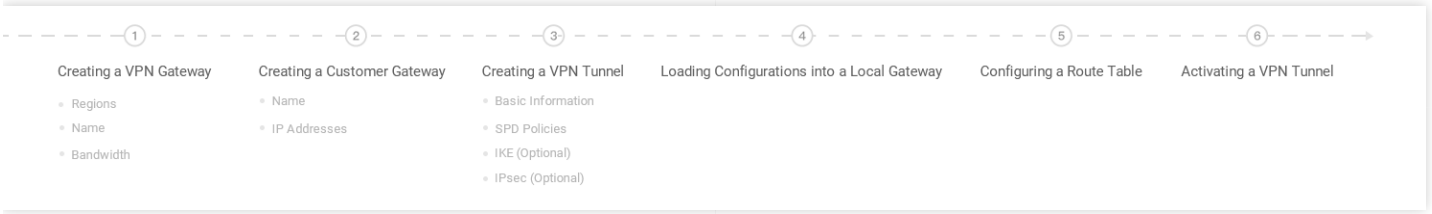
You can share application services deployed in VPC with other VPCs within the same or across different accounts through Private Link.
Share Services Across Different Accounts Using Private Link

Connecting to Local Data Centers

You can realize the communication between the VPC and the local data center through VPN connection and DC access.

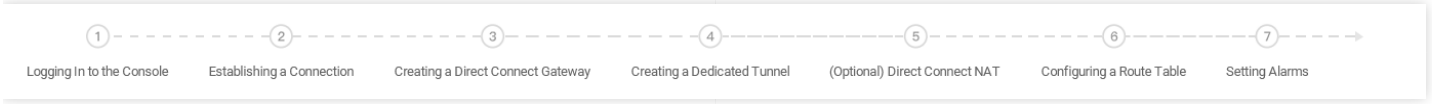
VPN Connection

The VPN connection is a way to connect your local data center and VPC through an encrypted public network channel. A VPN connection consists of three components: VPN gateway, peer gateway, and VPN tunnel.
Each VPN gateway can establish multiple VPN tunnels, with each tunnel connecting to a local data center.



Direct Connect

Direct Connect establishes a physical connection between VPC and your local data center. Direct Connect comprises three components: physical line, dedicated channel, and dedicated gateway.
Users can connect Converge Cloud computing resources across multiple regions using a single physical connection, enabling flexible and reliable hybrid cloud deployment.



For detailed operations, please refer to Dedicated Connection - Quick Start Guide.

VPC Terminal Nodes Overview

Scenarios and Advantages

Private Link enables a VPC to access resources in other VPCs over the private network, supporting connectivity between VPCs in the same account or across different accounts. Compared with public network services, it can save public network bandwidth, offer higher security, and significantly simplify the network architecture.
With Private Link, you can establish secure and stable private connections between VPCs and cloud services, simplifying the network architecture and avoiding potential security risks associated with accessing services via the public network.

Product Components

Private Link involves two important product entities:

- Terminal node services: Terminal node services are services that can be accessed by other VPCs through the creation of terminal nodes to establish private network connections. Terminal node services are created and managed by service providers.
- Terminal nodes: Terminal nodes can be associated with terminal node services to establish network connections for accessing external services via VPC private networks. Terminal nodes are created and managed by service users.

Restrictions

Quotas for Terminal Node Services

Resources	Limitation
The quantity of Terminal Node Services per single account.	100
The quantity of Terminal Nodes that can be added to a single Terminal Node Service.	500

Resources	Limitation
Supported resource types for the backend service of an Terminal Node Service.	Application-type Layer-4 CLB in the internal network; each Terminal Node Service is associated with 1 CLB and can be associated with multiple listeners.
Traffic supported by Terminal Node Service	- IPv4 traffic - IPv6 traffic
Protocols supported by "Terminal Node Service"	TCP protocol, UDP protocol, and HTTP protocol

Quotas for "Terminal Node"

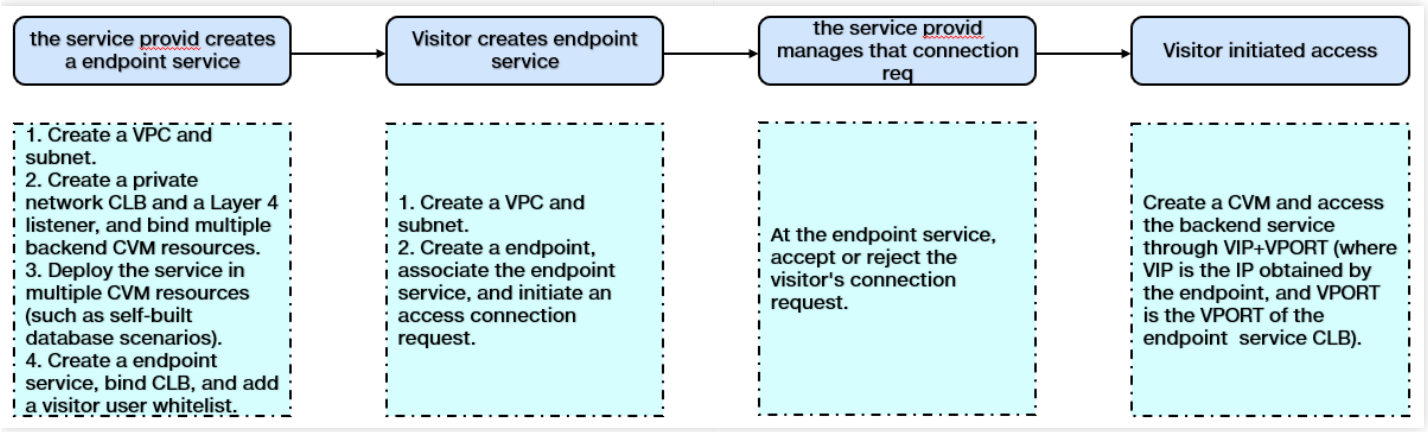
Resources	Limitation
Quantity of Terminal Nodes that can be created per single VPC.	50
Quantity of Terminal Node Services that can be associated with a single Terminal Node.	1
Traffic supported by Terminal Node.	- IPv4 traffic - IPv6 traffic
Protocols supported by Terminal Node.	TCP protocol, UDP protocol, and HTTP protocol

Billing description

- No instance fees are charged for Terminal Nodes and Terminal Node Services.
- No traffic communication fees are charged for Terminal Nodes and Terminal Node Services.
- No fees are charged for internal network CLB instances

Directions

Private Link enables the connectivity between VPCs. The operation steps are as follows.



Note:

- If it's cross-account, the CLB's vport information needs to be provided by the service provider to the requester, while the requester's user account UIN information needs to be provided to the service provider.
- CLB needs to create a Layer-4 CLB listener, and Layer-7 CLB listeners are not supported.

Endpoint Service

The Endpoint Service is created and maintained by the service provider and can be accessed by other VPCs through creating terminal nodes to establish private network connections.

Creating Endpoint Service

This section provides guidance on creating endpoint services.

Prerequisites

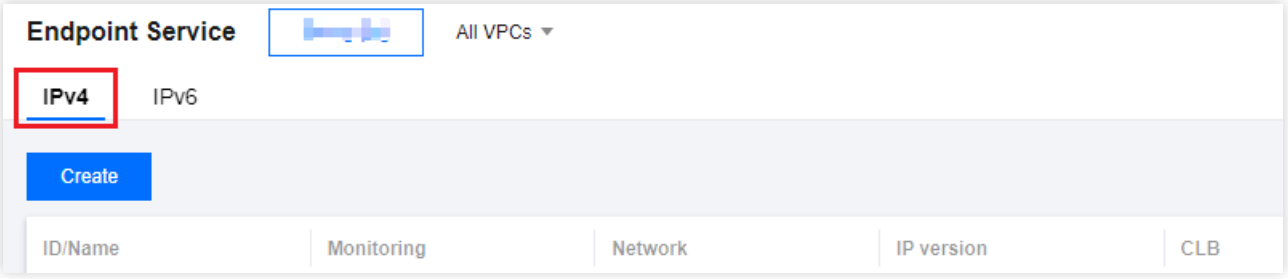
VPC, subnet, and application-type Layer-4 internal CLB have been created.

Operation Guide

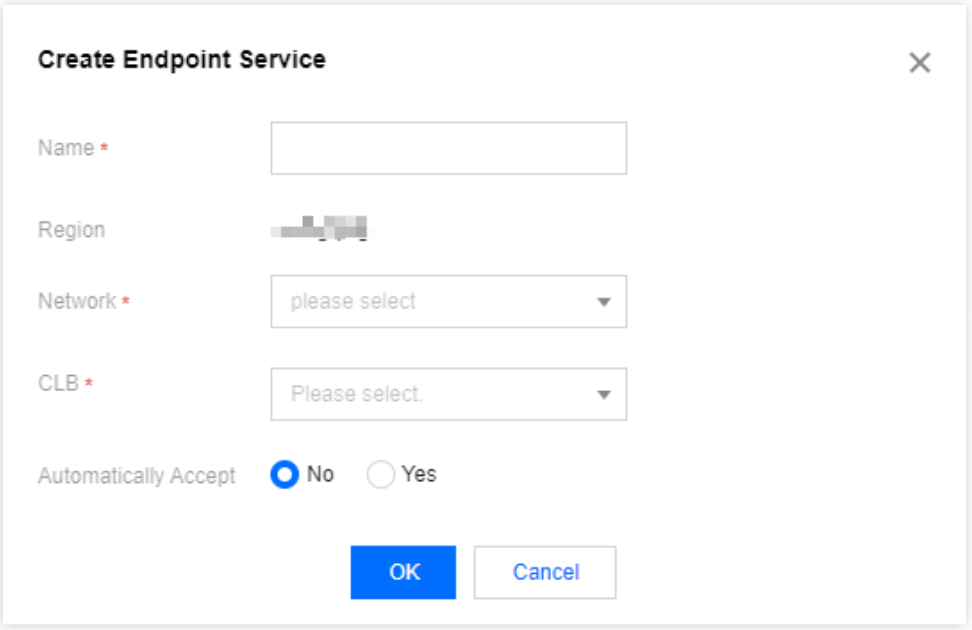
1. Log in to the VPC console.
2. In the left navigation pane, click on VPC Endpoint > Endpoint Service.
3. Terminal node services support both IPv4 and IPv6 scenarios.

- IPv4

  i. On the IPv4 tab, click Create.



  ii. In the pop-up Create Endpoint Service interface, configure the relevant parameters.



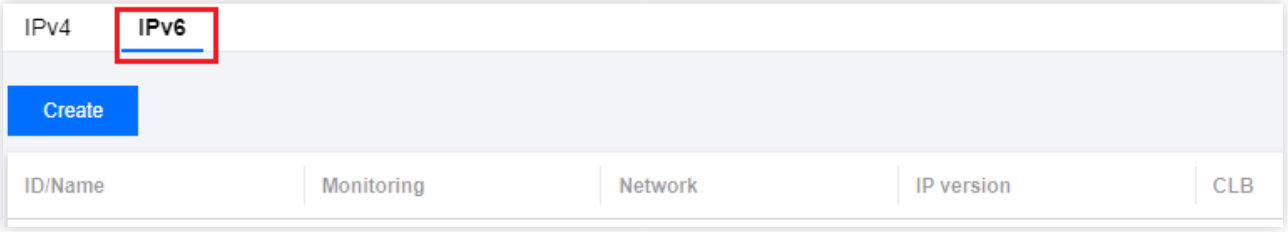
Parameter description:

- Service name: custom the name of endpoint service.
- Region: region where the terminal node service is located.
- VPC: Select the associated VPC.
- Load Balancer: Choose the CLB (Cloud Load Balancer) already created in the VPC; replacement is allowed.
- Auto Accept: Specifies whether the terminal node service automatically accepts connection requests initiated by terminal nodes. By default, it is set to No and can be changed.
  - If it is the same account, then Auto Accept is available.
  - If it is a cross-account, when select Auto Accept and the endpoint is in the user allowlist, then the endpoint is available upon successful creation.
  - If it is cross-account and Auto Accept is not selected, the initial status of the successfully created endpoint is Pending Acceptance, and it needs to be accepted by the server-side to become available.

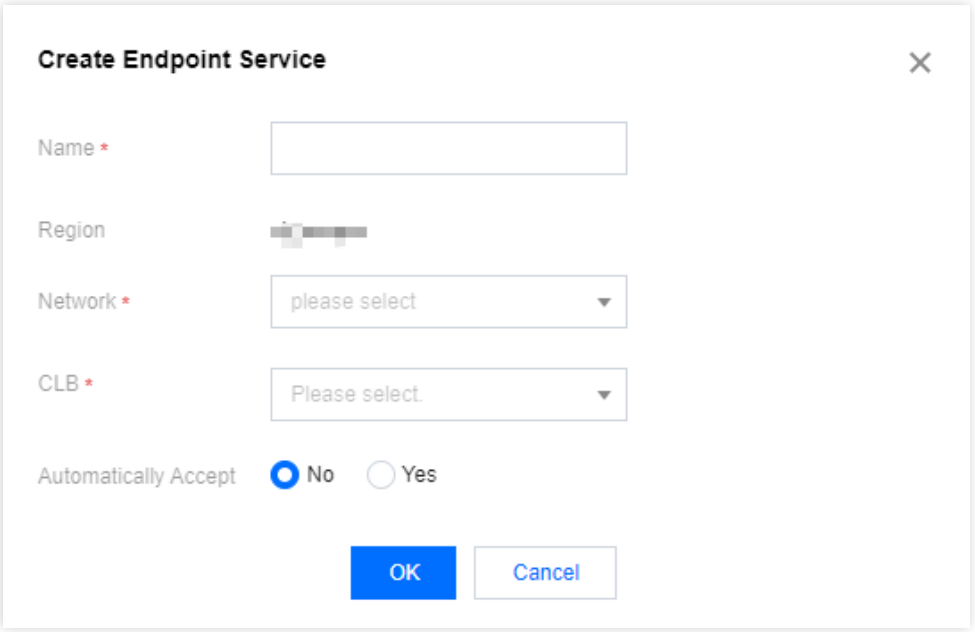
iii. After completing the parameter settings, click Confirm to complete the creation of the IPv4 terminal node service.

- IPv6

iv. On the IPv6 tab, click Create.



v. In the pop-up Create Endpoint Service interface, configure the relevant parameters.



Parameter description:

- Service name: custom the name of endpoint service.
- Region: region where the terminal node service is located.
- VPC: Select the associated VPC.
- Load Balancer: Choose the CLB (Cloud Load Balancer) already created in the VPC; replacement is allowed.
- Auto Accept: Specifies whether the terminal node service automatically accepts connection requests initiated by terminal nodes. By default, it is set to No and can be changed.
  - If it is the same account, then Auto Accept is available.
  - If it is a cross-account, when select Auto Accept and the endpoint is in the user allowlist, then the endpoint is available upon successful creation.
  - If it is cross-account and Auto Accept is not selected, the initial status of the successfully created endpoint is Pending Acceptance, and it needs to be accepted by the server-side to become available.

vi. After completing the parameter settings, click Confirm to complete the creation of the IPv4 terminal node service.

Managing User Allowlist

Used to manage the accounts allowed to access the terminal node service.

Allowlist management follows the following principles:

- When the terminal node service is set to auto-accept, users in the allowlist will be automatically accepted when creating terminal nodes, and the terminal nodes will be available as soon as they are created.
- If it is across accounts and the UIN of the terminal node is not in the allowlist of the target terminal node service, the creation will fail directly with an error, indicating that the terminal node service does not allow the connection.

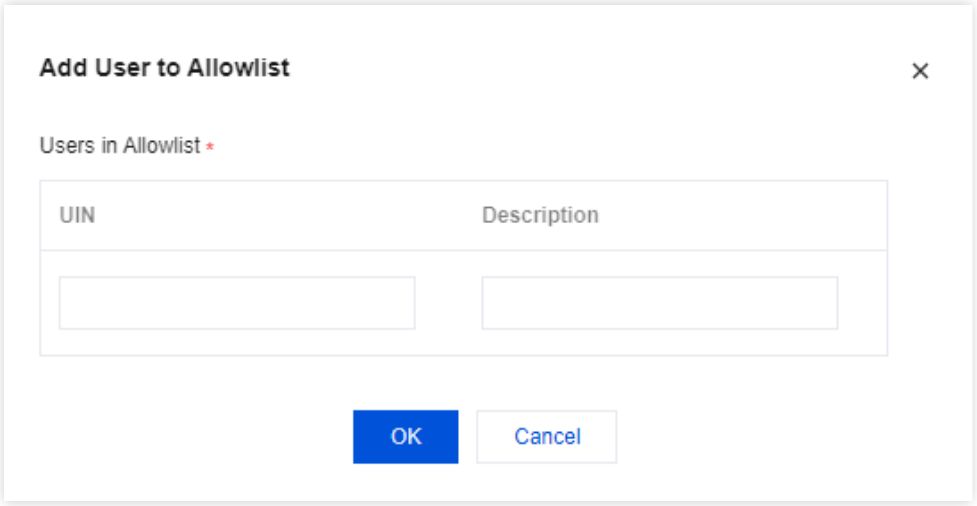
- If it is across accounts and the UIN of the terminal node is in the allowlist of the target terminal node service, the initial state of the successfully created terminal node will be pending acceptance. It will become available after being accepted by the server.
- Within the same account, auto-accept turns into available.

Prerequisites

Have obtained the user account information for the terminal node.

Directions

1. Click on the ID of the created terminal node service to access the details page.
2. click Allowlist tab to enter the User Allowlist Management interface.
3. Click Add to enter the Add Users to Allowlist interface.



4. Enter the user's UIN and description. After adding the user to the allowlist, click OK. The successfully added allowlist will be displayed in the list.

Managing Endpoint Connections

Users manage connection requests initiated by terminal nodes.

Directions

1. Click on the ID of the created terminal node service to access the details page.
2. Click the Endpoint Connection tab to enter the Endpoint Connection Management interface.
3. Handle the status connection requests of the terminal nodes based on the actual situation.
   Endpoint connections have three statuses: Pending Acceptance, Available, and Denied.
   - For connections in the Denied state, you can perform the Acceptance operation. After execution, the status becomes Available.
   - For connections in the Available state, you can perform the Deny operation. After execution, the status becomes Denied.
   - For connection requests in the Pending Acceptance state, you can perform Acceptance or Deny, and after

execution, the status becomes Available or Denied, respectively.

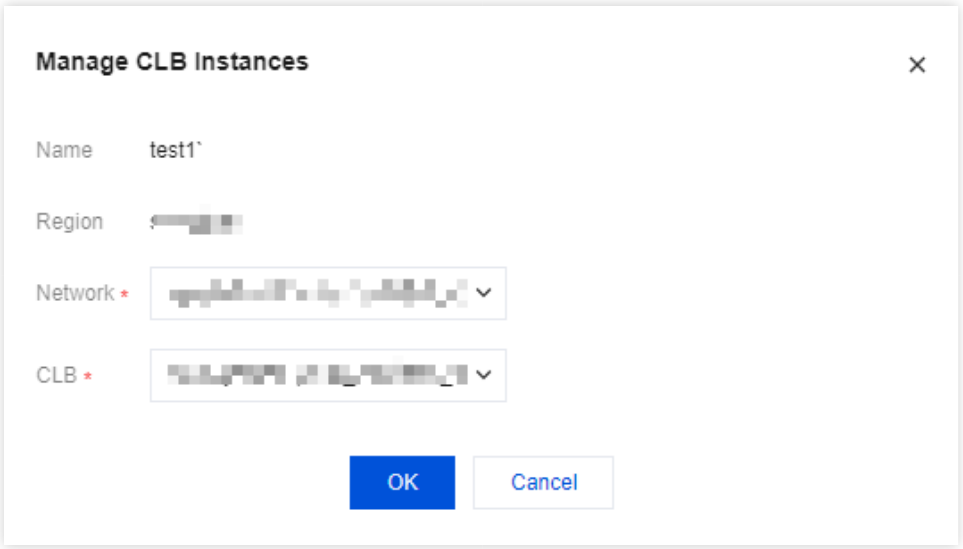
Note: The endpoint service can be connected by multiple endpoint. The status of the endpoint service refers to the status of each connection, not the status of the endpoint service alone.

Manage CLB Instances

Users manage the CLB of the endpoint service. When the endpoint service has no available connection status, changing the CLB is supported.

Directions

1. In the list, find the endpoint service to be processed, click More > Manage CLB Instances in the Action column, and a Manage CLB Instances dialog box will pop up.



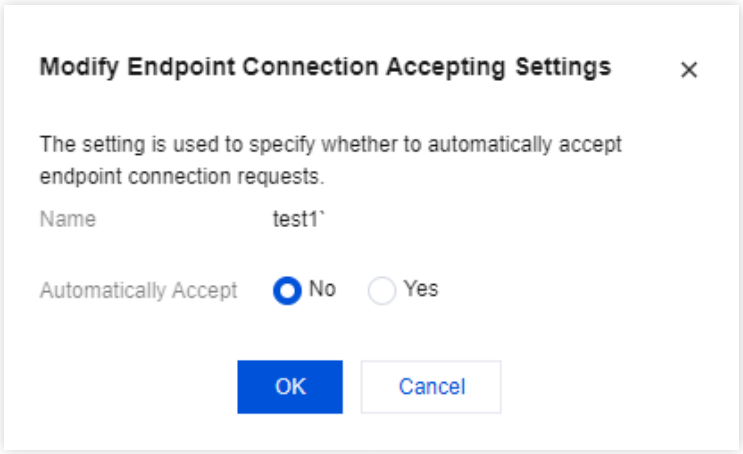
2. In the dialog box, select the network and CLB, and click [OK].

Modify Endpoint Connection Accepting Settings

Users can set whether the endpoint service needs to automatically accept connection requests.

Directions

1. In the list, find the endpoint service to be processed, click More > Modify Endpoint Connection Accepting Settings in the Action column, and a Modify Endpoint Connection Accepting Settings dialog box will pop up.



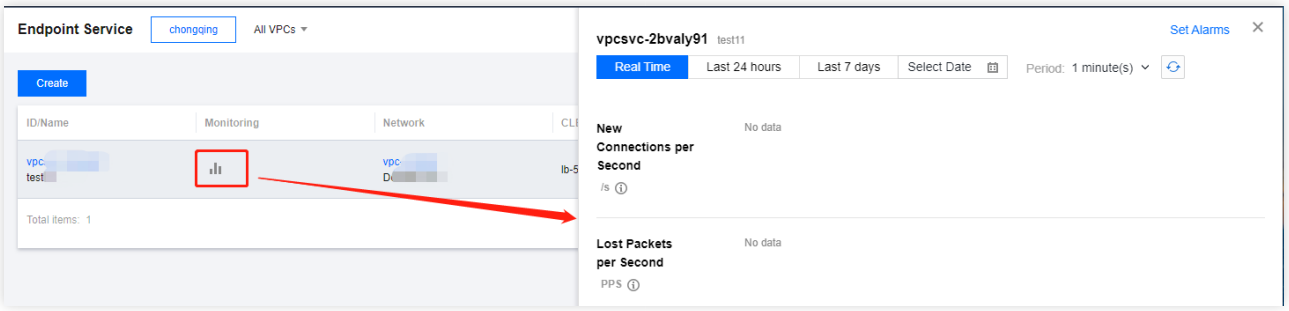
2. In the popup, select "Yes" or "No", then click OK.

Monitoring

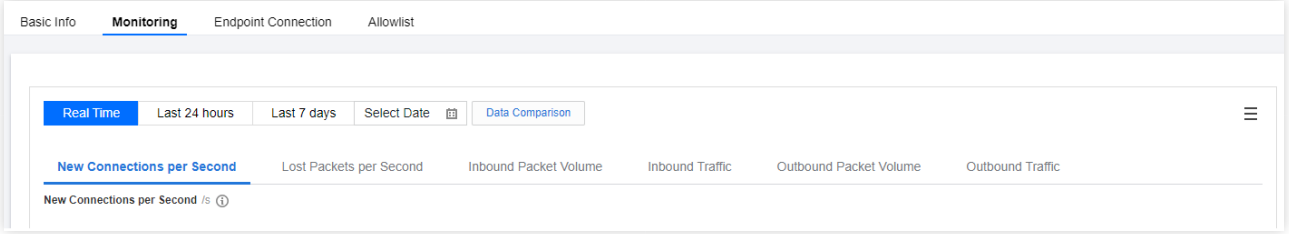
Metric monitoring helps you understand the real-time status of your services. If any anomalies occur, you can detect and address them promptly, thus improving operational efficiency.

Directions

1. Click on the monitoring icon in the endpoint service monitoring column to access the metric monitoring interface of the terminal node service.



2. Alternatively, you can click on the terminal node service ID to enter the details page and then click on the Monitoring tab to view the metric information.



3. For monitoring metrics, you can perform operations such as data comparison, data export, and exporting images as needed.

Endpoint

As a service user, endpoints are associated with endpoint services, establishing network connections for accessing external services through VPC private links.

Create Terminal Node

This section provides guidance on creating terminal nodes.

Prerequisites

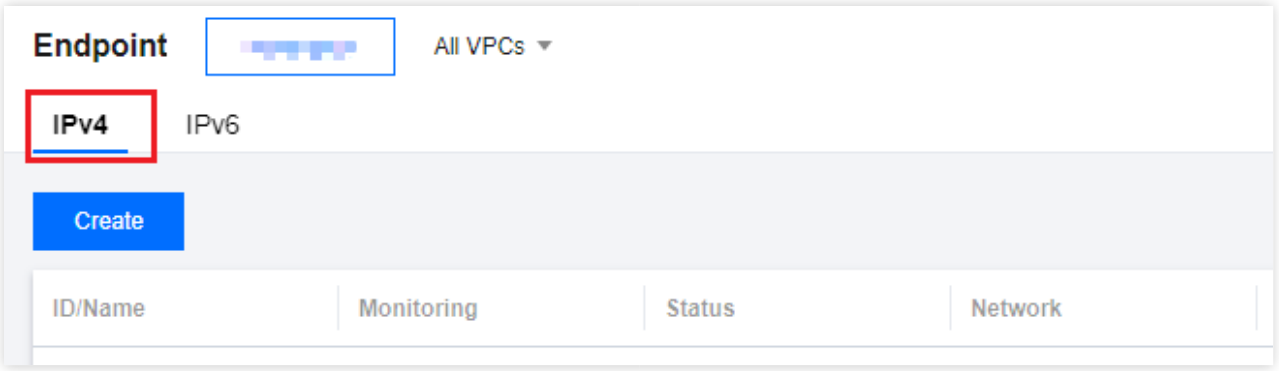
VPC, subnet, and CVM have been created.

Operation Guide

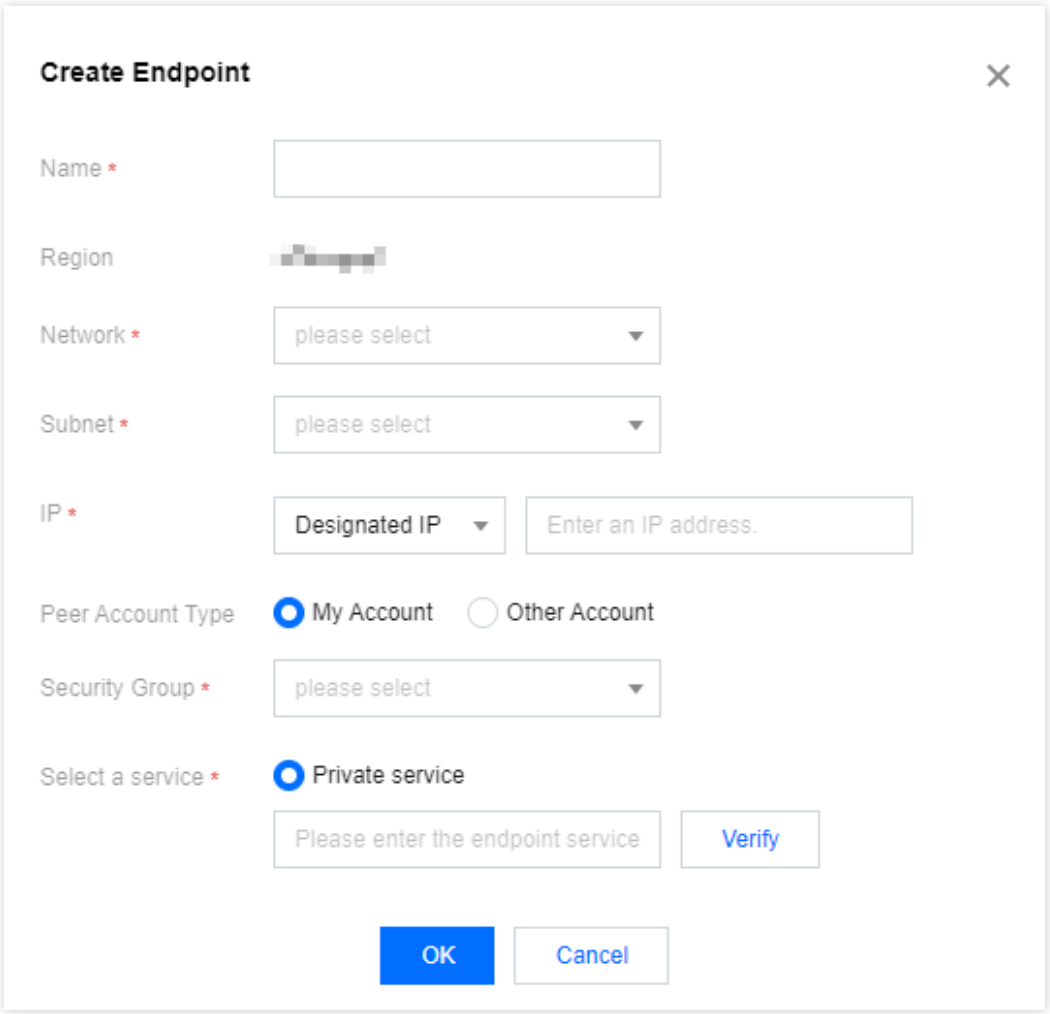
1. Log in to the VPC console.
2. Click VPC Endpoint > Endpoint on the left sidebar.
3. Terminal node support both IPv4 and IPv6 scenarios.

- IPv4

  i. On the IPv4 tab, click on Create.



  ii. In the pop-up dialog box for Create Endpoint, configure the terminal node parameters.



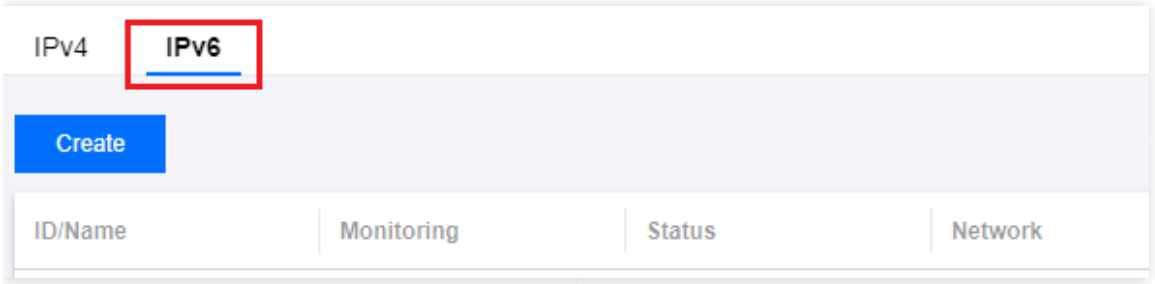
Parameter description:

- Name: custom the name of the endpoint.
- Region: The region where the endpoint is located.
- Network: Select the VPC where the endpoint is located.
- Subnet: Select the subnet where the endpoint is located.
- IP: the IP address of the endpoint. You can specify an IP address, which should be a private IP address within the VPC, or opt for automatic IP assignment.
- Peer account type: Select the owning account of the VPC that needs access. My Account indicates access within the same account VPC, while Other Accounts signifies cross-account VPC access. For cross-account access, it is necessary to inform the peer account of your account number, and after initiating a connection request, server-side acceptance is required for connectivity.
- Select a service: Enter the ID of the endpoint service and click Verify. Only services that have passed verification can be connected.

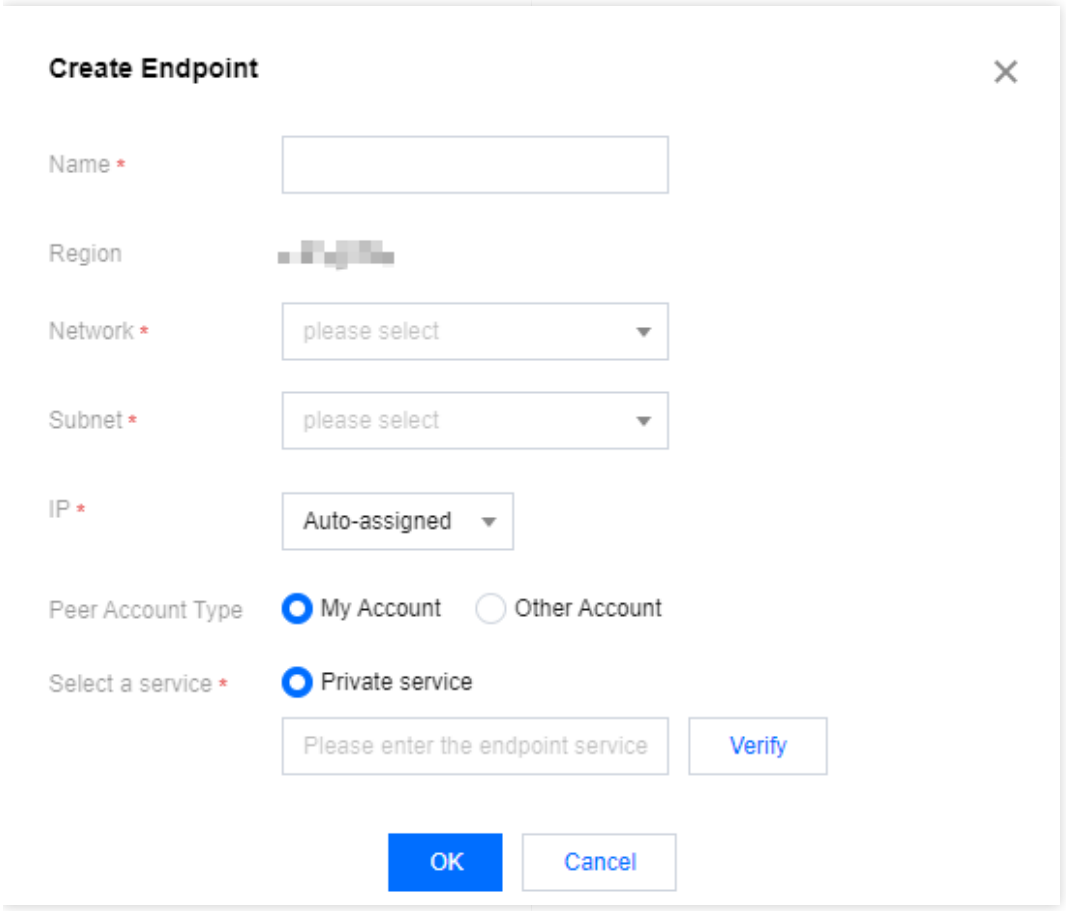
iii. After the parameter settings are completed, click OK.

- IPv6

iv. On the IPv6 tab, click Create.



5. In the pop-up dialog box for Create Endpoint, configure the terminal node parameters.



Parameter description:
- Name: custom the name of the endpoint.
- Region: The region where the endpoint is located.
- Network: Select the VPC where the endpoint is located.
- Subnet: Select the subnet where the endpoint is located.
- IP: the IP address of the endpoint. You can specify an IP address, which should be a private IP address within the VPC, or opt for automatic IP assignment.
- Peer account type: Select the owning account of the VPC that needs access. My Account indicates access within the same account VPC, while Other Accounts signifies cross-account VPC access. For cross-account access, it is necessary to inform the peer account of your account number, and after initiating a connection request, server-side acceptance is required for connectivity.

- Select a service: Enter the ID of the endpoint service and click Verify. Only services that have passed verification can be connected.
6. After the parameter settings are completed, click OK.

Bind/Unbind Security Groups

Bind a security group to the endpoint to control the inbound traffic, and improve the security of business access.

Operation Guide

1. Log in to the Security Group Console, create a security group and set its rules.
2. On the security groups tab in the endpoint details page, you can bind or unbind security groups to the endpoint, as well as adjust the priority of the security groups.

Data Verification

Obtain the VIP and vport of the CLB for the terminal node service provider, and access it in CVM according to the access method of the service provider, such as MySQL client, IE browser, etc.

Monitoring

Metric monitoring helps you understand the real-time status of your services. If any anomalies occur, you can detect and address them promptly, thus improving operational efficiency.

Directions

1. Click the monitoring icon in the Endpoint Monitoring column to enter the metric monitoring interface for endpoint services.
2. You can also click the Endpoint Service ID to enter the details page, then click the [Monitoring] tab to view the metrics.
3. For monitoring metrics, you can perform operations such as data comparison, data export, and exporting images as needed.

Security Management
Security Groups
Overview of Security Groups

A security group is a virtual firewall with stateful packet filtering capabilities used to set network access controls for instances such as cloud servers, load balancers, and cloud databases. It controls inbound and outbound traffic at the instance level and is an important means of network security isolation.
You can configure security group rules to allow or deny inbound and outbound traffic for instances within the security group.

Features

- A security group is a logical grouping where you can add instances such as cloud servers, elastic network interfaces, and cloud databases that have the same network security isolation requirements within the same region.
- Instances associated with the same security group do not communicate by default, and you need to add corresponding allow rules.
- Security groups are stateful; for inbound traffic that you have allowed, outbound traffic is automatically allowed, and vice versa.
- You can modify security group rules at any time, and new rules take effect immediately.

Security group rules

Components

Security group rules include the following components:

- Source: the source data (inbound) or destination data (outbound) IP.
- Protocol type and protocol port: Protocol types such as TCP, UDP, HTTP, etc.
- Policy: Allow or deny.

Rule Priority

- Rules within a security group have priorities. Rules within a security group have priorities. Rule priority is represented by the position of the rule in the list, with the highest priority rule at the top of the list and the lowest at the bottom.
- If there is a rule conflict, the rule with the higher priority will prevail by default.

- When traffic enters/exits an instance bind to a security group, it matches rules from the top to the bottom of the security group rule list. If a rule is successfully matched and allowed to pass, the subsequent rules will not be matched.

Multiple security groups

An instance can be bind to one or more security groups. When an instance is bind to multiple security groups, the rules of multiple security groups are executed sequentially from top to bottom, and you can adjust the priority of security groups at any time.

Security group template

When creating a new security group, you can choose from two security group templates provided by Converge Cloud:

- Allow all port templates: All inbound and outbound traffic will be allowed.
- Allow Common Ports Template: TCP port 22 (Linux SSH login), ports 80 and 443 (Web services), port 3389 (Windows remote log in), ICMP protocol (Ping), and internal network traffic will be allowed.

  > Note:
  >
  > - If the provided security group templates do not meet your actual needs, you can also create a custom security group.
  > - If you have security protection requirements at the application layer (HTTP/HTTPS), you can separately purchase Web Application Firewall (WAF). WAF provides application layer web security protection against web vulnerability attacks, malicious crawlers, and CC attacks, safeguarding websites and web applications.

Usage Limitations

For usage limitations and quotas regarding security groups, please refer to Limitation notes.

Directions

The usage process for security groups is illustrated in the following diagram.



Creating Security Group

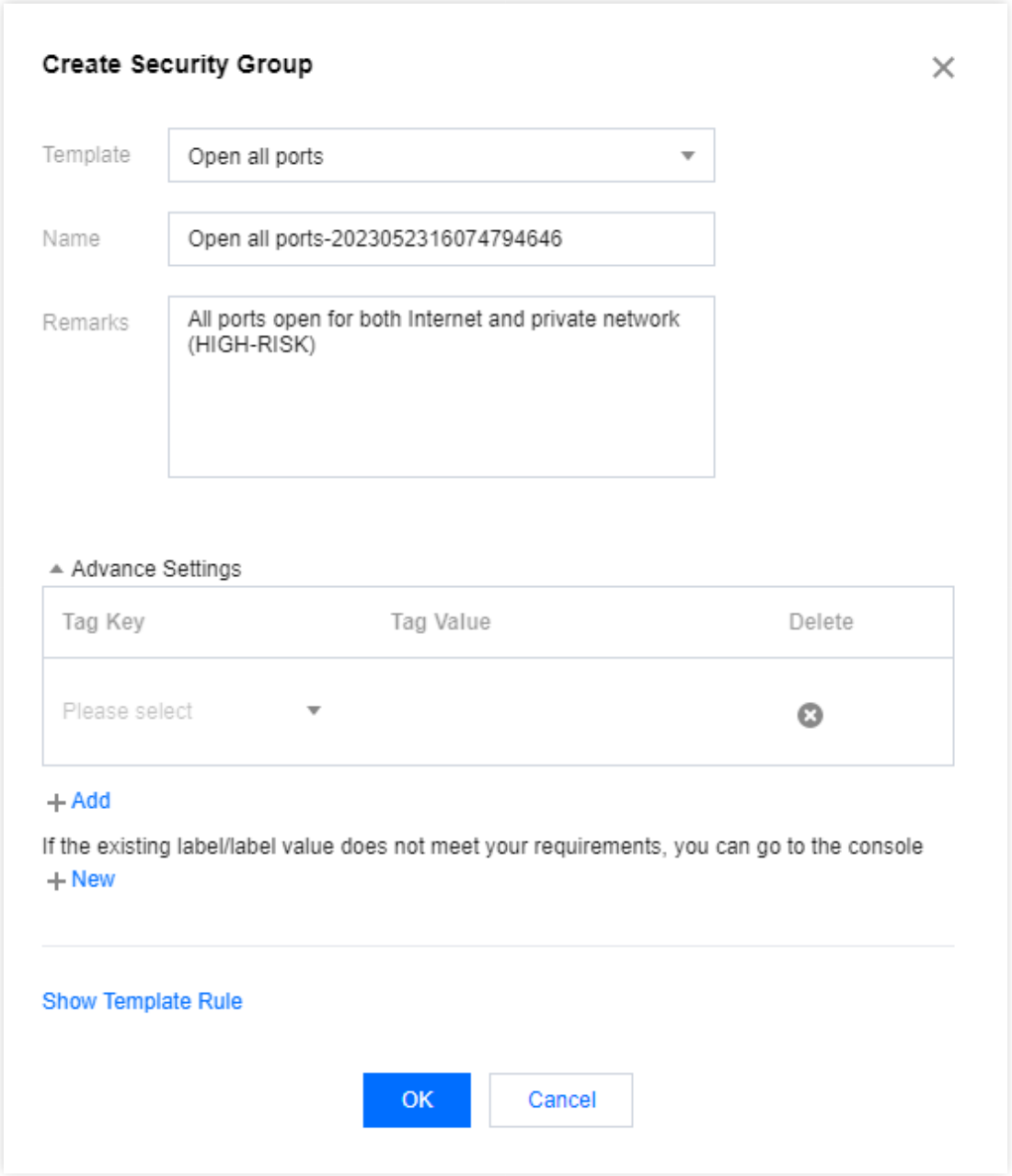
Overview

Security groups are the virtual firewalls of Cloud Virtual Machine instances, and each Cloud Virtual Machine instance must belong to at least one security group. When you create a Cloud Virtual Machine instance, if you have not created a security group yet, the cloud platform provides two templates: Open All Ports and Open Ports 22, 80, 443, 3389 and ICMP Protocol to create a default security group.

If you do not want Cloud Virtual Machine instances to be added to the default security group, you can also create your own security groups as described in this document. This document introduces to create a security group on the Cloud Virtual Machine console.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and click +Create.
4. In the Create Security Group pop-up window, complete the parameter configuration. See the figure below:



- Template: based on the services to be deployed for the Cloud Virtual Machine instances in the security group, select an appropriate template to simplify security group rule configuration. As shown below:

Template	Description	Scene
Open All Ports	All ports are opened to the public network and private network by default, which has certain security risks.	-
Open Ports 22, 80, 443 and 3389 and ICMP Protocol.	By default, ports 22, 80, 443, 3389 and the ICMP protocol are opened. The private network is fully opened.	Instances in the security group need to be deployed with Web services.

Template	Description	Scene
Custom	After the security group is successfully created, add the security group rules as required.	-

- Name: customize the security group name.
- Remarks: Custom, and a short description of the security group for easier management.
- Advance Settings: Set tag information. If there is no tag, you can click Create to create tag information; click Add to add a tag, and click Delete to delete it.

5. Click OK to complete the creation of the security group.
   If you selected the Custom template when creating a new security group, you can click Set Rules Now to Add Security Group Rules.

Adding Security Group Rule

Overview

Security groups are used to manage whether access requests from the public network or private network are allowed. For security reasons, the inbound direction of security groups often adopts a deny access policy. If you select Open All Ports template or Open 22, 80, 443, 3389 Ports and ICMP Protocol template when creating a security group, the system will automatically add security group rules for some communication ports based on the selected template type.

This document describes how to add security group rules to allow or forbid Cloud Virtual Machine instances in the security group to access the public network or private network.

Notes

- Security group rules support IPv4 security group rules and IPv6 security group rules.
- Open all ports already includes IPv4 and IPv6 security group rules.

Prerequisites

- You have created a security group. For detailed operations, see Create Security Group.
- You already know which public network or private network access requests need to be allowed or denied for the Cloud Virtual Machine instance.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be set.
4. In the row of the security group where rules need to be set, click Modify Rules in the Operation column.
5. On the Security Group Rules page, click Inbound Rules and select any of the following methods to complete the operation according to actual needs.
   The following operation uses Method 2: adding rules as an example.
   - Method 1: open all ports, is applicable to scenarios where ICMP protocol rules do not need to

be set and operations can be completed through ports 22, 3389, ICMP, 80, 443, 20, 21.
- Method 2: adding a rule, is applicable to scenarios where multiple communication protocols need to be set, such as the ICMP protocol.

6. In the Add Inbound pop-up window, set the rules.
   The main parameters for adding a rule are as follows:
   - Type: the default value is Custom. You can also select other system rule templates, such as Windows log-in, Linux log-in, Ping, HTTP(80), or HTTPS(443).
   - Source: the source (inbound rule) or destination (outbound rule) of traffic, specify one of the following options:

Specified Source/ Destination	Description
Single IPv4 address or IPv4 address range	Notation in CIDR (such as 203.0.113.0, 203.0.113.0/24 or 0.0.0.0/130618222416261120, where 0.0.0.0/130618222416261120 represents matching all IPv4 addresses)
Single IPv6 address or IPv6 address range	Notation in CIDR (such as FF05::B5, FF05:B5::/60, ::/130618222416261120 or 0::0/130618222416261120, where: ::/130618222416261120 or 0::0/130618222416261120 represents matching all IPv6 addresses).
Refer to the security group ID. You can reference the ID of following security groups: - current security group - other security group	- The current security group represents the security group ID associated with the Cloud Virtual Machine. - The other security group represents another security group ID under the same item in the same area. Note: - Referencing a security group ID is an advanced feature that you can choose to use. The rules of the referenced security group will not be added to the current security group. - When configuring the security group rules, if you enter a security group ID in source/destination, it means that only the private network IP address of the Cloud Virtual Machine instance and Elastic Network Interface bound to this security group ID is used as the source/destination, excluding the public network IP address.
Reference an IP address object or IP address group object in the parameter template	-

- Protocol Port: Enter the protocol type and port range or you can also reference the protocol port or protocol port group in the parameter template.
- Policy: the default value is Allow.

    - Allow: Access requests of this port are allowed.
    - Reject: Data packets will be discarded without any response.
- Notes: Custom, and a short description of the rule for easier management.

7. Click Finish to complete adding the security group inbound rule.
8. On the Security Group Rules page, click "Outbound Rules" and refer to Step 5 - Step 7 to complete adding outbound rules for the security group.

Restrictions

Usage Limitations

- Security groups are divided by region. A Cloud Virtual Machine (CVM) can be bind only to security groups in the same region.
- The security group are applicable to any Cloud Virtual Machine instance in the network environment.
- Each user can set up to 50 security groups under each project in each region.
- A maximum of 100 inbound or outbound access rules can be set for each security group.
- One Cloud Virtual Machine can join multiple security groups, and one security group can be associated with multiple Cloud Virtual Machines at the same time.

Quota Limitations

Description	Limitation
Number of Security Groups	50/region
Number of Security Group Rules	100/inbound, 100/outbound
Number of Cloud Virtual Machine instances associated with a single security group	100
Number of security groups a Cloud Virtual Machine can be associated with	5
Number of rule entries for each security group that references the security group IDs	10 entries

Managing Security Group
Viewing Security Group

View all security groups

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region to view all security groups under this region.

View specified security groups

You can also view the security groups you want to view through the search feature on the Security Groups Management page.

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region.
4. At the top right of the security group list under this region, click the search text box and select any one of the following methods to query the security groups you want to view.

- Select Security Group ID, enter the security group ID, and press  to query the corresponding security group of this security group ID.

- Select Security Group Name, enter the security group name, and press  to query the corresponding security group of this security group name.

Remove from Security Group

You can remove Cloud Virtual Machine instances from the security group based on your business needs.

Prerequisites

The Cloud Virtual Machine instance has joined two or more security groups.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security groups whose instances need to be removed.
4. In the row of the security group whose instance need to be removed, click Manage Instances in the Operation column to enter the Associated Instance page.
5. On the Associated Instance page, select the instance to be removed and click Remove from Security Group.
6. Click OK in the pop-up window.

Clone Security Group

Overview

You may need to clone a security group in the following scenarios:

- Assume that you have created a security group sg-A in region A and need to use the exact same rules as those for instances in region B. In this case, you can directly clone sg-A into region B instead of creating security groups from scratch in region B.
- If your business needs to execute a new security group rule, you can clone the original security group for backup.

Notes

- By default, only the inbound/outbound rules of this security group are cloned, but not the instances associated with the security group.
- Security groups can be cloned between projects or regions.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group to be cloned.
4. In the row of the security group to be cloned, click More > Clone in the Operation column.
5. In the Clone Security Group pop-up window, select Target Project and Target Region for the clone, enter the New Name of security group, and click OK.

Delete Security Group

If your business has no longer required one or more security groups, you can delete the security group. After deletion, all rules within the security group will be deleted simultaneously.

Prerequisites

Make sure that the security group to be deleted has no associated instances. If there are associated instances, remove those instances from the security group first; otherwise, the operation to delete the security group cannot be executed.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group to be deleted.
4. In the row of the security group to be deleted, click More > Delete in the Operation column.
5. Click OK in the pop-up window.

Associated Instances

> Note:
>
> Security groups support association with CVMs, secondary Elastic Network Interfaces, and Cloud Load Balancers. This document uses the association with Cloud Virtual Machine as an example.

Overview

Security groups are used to set the network access control for single or multiple Cloud Virtual Machine instances, which is an important means of network security isolation. You can associate Cloud Virtual Machine instances with one or more security groups based on business needs. Here's how to associate a Cloud Virtual Machine instance with a security group in the console.

Prerequisites

A Cloud Virtual Machine instance has been created.

Directions

1. Log in to the VPC Console.
2. In the left sidebar, click Security > Security Groups to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be set.
4. In the row of the security group whose rules need to be set, click Manage Instances in the Operation column to enter the Associated Instance page.
5. On the Associated Instance Page, click Add Association.
6. In the Add Instance Association pop-up window, select the instances you want to bind to the security group, and click OK.
7. Click the Download icon in the upper right corner to download the list of associated instances to the local device.

Subsequent Operations

- If you want to view all the security groups you have created in a certain region, you can query the Security Group List.

- If you do not want your Cloud Virtual Machine instance to belong to one or more security groups, you can remove the Cloud Virtual Machine instance from the security group.
- If your business no longer requires one or more security groups, you can delete the security group. After deletion, all rules within the security group will be deleted simultaneously.

Managing Security Group Rule
View Security Group Rules

Overview

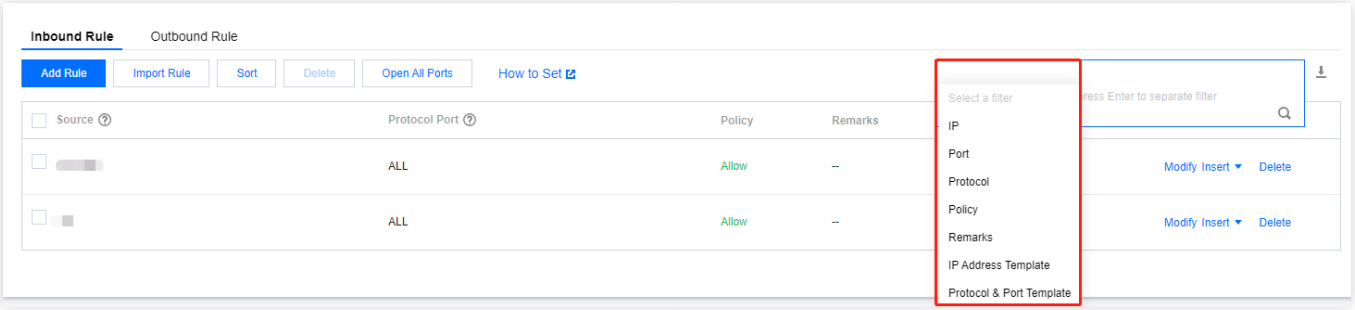
After adding a security group rule, you can view the details of the security group rule in the console.

Prerequisites

A security group has been created and security group rules have been added to it.
For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.

Directions

1. Log in to the VPC Console.
2. In the left sidebar, select Security > Security Groups to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be viewed.
4. Click the security group ID/name of the rule to be viewed to enter the Security Group Rules page.
5. On the Security Group Rules page, click the Inbound Rule or Outbound Rule tab to view the inbound/ outbound security group rules.
6. Click the search column on the right to quickly search by different latitudes.



Modify Security Group Rule

Overview

Improper security group rules (for example, those that do not restrict access to specified ports) can incur severe security risks. In this case, you can modify these unreasonable security group rules in a security group to ensure the network security of CVM instances.

Prerequisites

A security group has been created and security group rules have been added to it.
For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be modified.
4. In the row of the security group whose rules need to be modified, click Modify Rules in the Operation column to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be modified (Inbound/Outbound), click the Inbound/Outbound Rules tab.
6. Find the security group rule to be modified, and click Edit in the Operation column to modify the existing rules.

Delete Security Group Rule

Overview

If you no longer need a security group rule, you can delete it.

Prerequisites

- A security group has been created and security group rules have been added to it.
  For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.
- It is confirmed that the CVM instance does not need to permit/forbid public network access or private network access.

Directions

1. Log in to the Cloud Virtual Machine Console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be deleted.
4. In the row of the security group whose rules need to be deleted, click Modify Rules in the Operation column to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be deleted (Inbound/Outbound), click the Inbound/Outbound Rules tab.
6. Find the security group rule that needs to be deleted and click Delete in the Operation column.
7. Click OK in the pop-up window.

Import security group rules

Overview

Security group rules can be imported. You can import the exported security group rule file into a security group to quickly create or recover security group rules.

Directions

1. Log in to the VPC Console.
2. In the left sidebar, select Security > Security Groups to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be imported.
4. Click the security group ID/name of the rule to be imported to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be imported (Inbound/Outbound), click the Inbound/Outbound Rules tab.
6. On the Inbound/Outbound Rule tab, click Import Rules.
7. In the Batch Import - Inbound/Outbound Rules pop-up window, select the edited template file for inbound/outbound rules, and click Start Importing.

> Note:
>
> - If there are security group rules under the security groups that need to be imported, it is recommended that you export the existing rules first. Otherwise, when importing new rules, the original rules will be overwritten.
> - If there is no security group rule under the security group that needs to import rules, it is recommended that you download the template first and then import the file after editing the template file.

Export Security Group Rule

Overview

Security group rules can be exported. You can export the security group rules of a security groups for local backup.

Directions

1. Log in to the VPC Console.
2. In the left sidebar, select Security > Security Groups to enter the Security Group Management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be exported.
4. Click the security group ID/name of the rule to be exported to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be exported (Inbound/ Outbound), click the Inbound/Outbound Rules tab.
6. Under the Inbound/Outbound Rules tab, click the Download icon  at the top right to download and save the security group rule file to your local device.

Security Group Use Cases

Security group settings are used to manage whether the Cloud Virtual Machine can be accessed. You can configure the inbound and outbound rules of the security group to set whether your server can be accessed and can access other network resources.
By default, the inbound and outbound rules for security groups are as follows:

- To ensure the data security, the input rules for security groups are set to a denial policy, prohibiting remote access from external networks. If you need your Cloud Virtual Machine to be accessible from the outside, you need to open the appropriate ports for inbound rules.
- The outbound rules for security groups are used to determine whether your Cloud Virtual Machine can access external network resources. If you select Open All Ports or Open 22, 80, 443, 3389 Ports and ICMP Protocol, the outbound rules for the security groups are fully open. If you opt for custom security group rules, the default outbound rule is to deny all, requiring you to open the relevant ports for outbound rules to access external network resources.

Common Use Cases

This document describes several common use cases for security groups. If any of the following scenarios meet your requirements, you can set your security groups according to the configuration recommended for the corresponding use case.

Scenario 1: remotely connecting to a Linux CVM through SSH

Example: You have created a Linux CVM and wish to connect to the CVM remotely via SSH.
Solution: When adding an inbound rule, select "Linux login" in the "Type", open port 22, and allow Linux SSH login.
You can also, based on actual requirements, allow all IPs or specified IPs (IP segments) to configure IP sources that can remotely connect to the CVM via SSH.

Direction	Type	Source	Protocol Port	Policies
Inbound	Linux log in	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP range you specify	TCP:22	Allow

Scenario 2: remotely connecting to a Windows CVM through RDP

Example: You have created a Windows CVM and wish to connect to the CVM remotely via RDP.
Solution: When adding an inbound rule, select "Windows login" in the "Type", open port 3389, and allow

Windows remote login.
You can also, based on actual requirements, allow all IPs or specified IPs (IP segments) to configure IP sources that can remotely connect to the CVM via RDP.

Direction	Type	Source	Protocol Port	Policies
Inbound	Windows login	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP range you specify	TCP:3389	Allow

Scenario 3: pinging a CVM from the public network

Example: You created a CVM and wish to test whether the communication between this CVM and other CVMs is normal.
Solution: Use the ping program for testing. When adding an inbound rule, select "Ping" in the "Type", open the ICMP protocol port, and allow other CVMs to access this CVM through the ICMP protocol.
You can also, based on actual requirements, allow all IPs or specified IPs (IP segments) to configure IP sources that can access this CVM via the ICMP protocol.

Direction	Type	Source	Protocol Port	Policies
Inbound	Ping	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP range you specify	ICMP	Allow

Scenario 4: Telnet remote log-in

Example: You wish to log in to the CVM remotely via Telnet.
Solution: To log in to the CVM remotely via Telnet, you need to configure the following security group rules when adding an inbound rule:

Direction	Type	Source	Protocol Port	Policies
Inbound	Custom	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP range you specify	TCP:23	Allow

Scenario 5: allowing Web Service HTTP or HTTPS Access

Example: You have set up a website and wish users to access the website via HTTP or HTTPS.
Solution: To allow access to the website via HTTP or HTTPS, you need to configure the following security group rules based on actual requirements when adding an inbound rule:

- Allow all IPs on the public network to access the website

Direction	Type	Source	Protocol Port	Policies
Inbound	HTTP (80)	0.0.0.0/0	TCP:80	Allow
Inbound	HTTP (80)	0.0.0.0/0	TCP:80	Allow

- Allow some IPs on the public network to access the website

Direction	Type	Source	Protocol Port	Policies
Inbound	HTTP (80)	IPs or IP address ranges allowed to access your website	TCP:80	Allow
Inbound	HTTPS(443)	IPs or IP address ranges allowed to access your website	TCP:80	Allow

Scenario 6: allowing external IPs to access the specified port

Example: After deploying the service, you want the specified business port (e.g., 1101) to be accessible from the outside.
Solution: When adding inbound rules, select Custom in Type and open protocol port 1101, allowing external access to the specified business port IP. You can also open all IPs or specified IPs (IP range) according to actual needs, allowing access from IPs to the specified business port.

Direction	Type	Source	Protocol Port	Policies
Inbound	Custom	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP address range you specify	TCP:1101	Allow

Scenario 7: denying external IPs to access the specified port

Example: After deploying the service, you do not want the specified business port (e.g., 1102) to be accessible from the outside.
Solution: When adding inbound rules, select Custom in Type, configure protocol port 1102, and set the Policy to Deny to deny external access to the specified business port.

Direction	Type	Source	Protocol Port	Policies

Direction	Type	Source	Protocol Port	Policies
Inbound	Custom	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP address range you specify	TCP:1102	Allow

Scenario 8: allowing a Cloud Virtual Machine access to a specified external IP only

Example: You want your CVM to access only specific external IP addresses.
Solution: Refer to the following configuration and add the following two outbound security group rules.

- Allow instances to access specific public IP addresses
- Prohibit the instance from accessing all public IP addresses with any protocol

> The rule that permits access should have a higher priority than the rule that denies access.

Direction	Type	Source	Protocol Port	Policies
Outbound	Custom	The specified public IP address that can be accessed by the CVM	The required protocol and port	Allow
Outbound	Custom	0.0.0.0/0	ALL	Deny

Scenario 9: denying a Cloud Virtual Machine access to a specified external IP

Example: You do not want your CVM to access specific external IP addresses.
Solution: Refer to the following configuration and add security group rules.

Direction	Type	Source	Protocol Port	Policies
Outbound	Custom	The specified public IP address that you do not want to be accessed by the CVM	ALL	Deny

Scenario 10: using FTP to upload or download files

Example: You need to use FTP software to upload or download files to/from the Cloud Virtual Machine.
Solution: Refer to the following configuration and add security group rules.

Direction	Type	Source	Protocol Port	Policies
Inbound	Custom	0.0.0.0/0	TCP:20-21	Allow

Combination of Multiple Scenarios

In practical scenarios, you may need to configure multiple security group rules based on business needs. For instance, setting up both inbound and outbound rules. One Cloud Virtual Machine can be bind to one or more security groups. When a Cloud Virtual Machine is bind to multiple security groups, these groups will be matched and executed in order from top to bottom. You can adjust the priority of the security groups at any time. For an explanation of the priority of security group rules, see Rule Priority Explanation.

Common Server Ports

The following describes the common server ports. For more information on service application ports for Windows, refer to the Microsoft Official Documentation (Overview of Windows Services and Network Port Requirements).

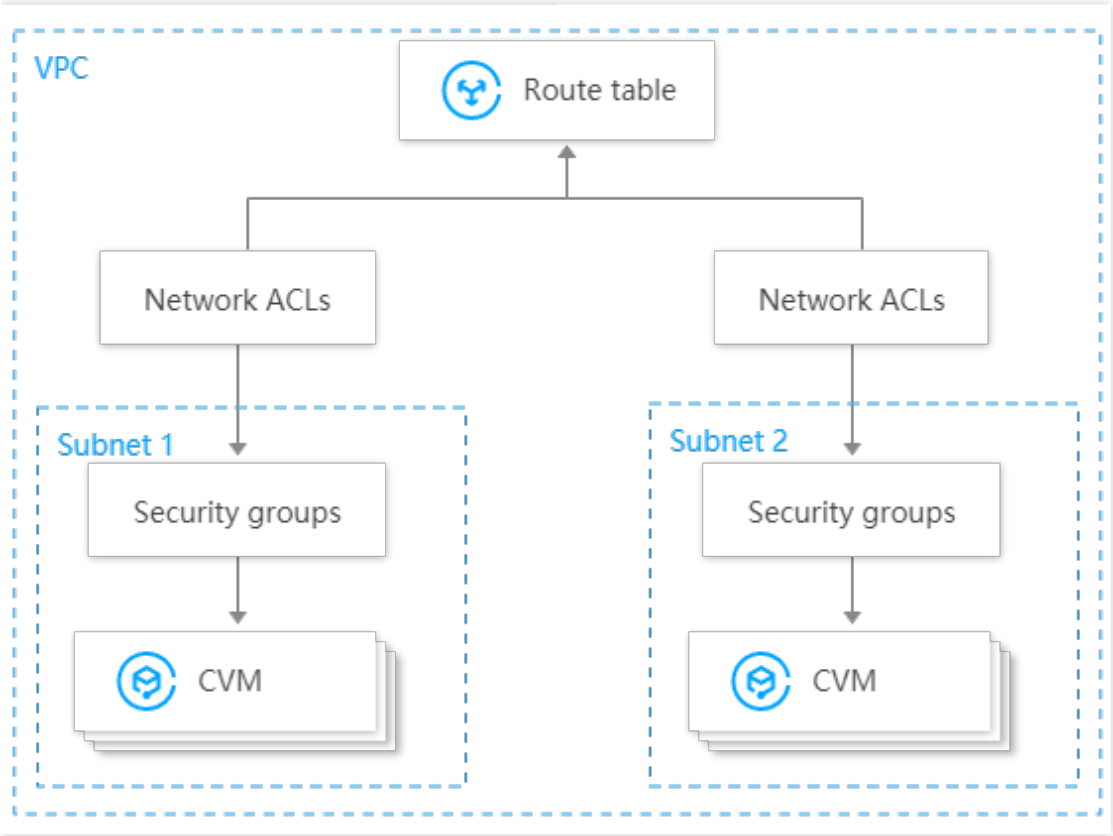
Port	Service	Description
21	FTP	Port opened by the FTP server. It is for uploading and downloading.
22	SSH	Port 22 is the SSH port used to remotely connect Linux system servers via command-line mode.
25	SMTP	Port opened by the FTP server. It is for sending mail.
80	HTTP	It is used to provide external access for website services such as IIS, Apache, and Nginx.
110	POP3	Port 110 is open for POP3 (mail protocol 3) services.
137,138,139	NETBIOS Protocol	Among them, 137 and 138 are UDP ports, which are used when transferring files through the network neighborhood. Port 139: Connections coming through this port attempt to get NetBIOS/SMB services. This protocol is used for Windows file and printer sharing and SAMBA.
143	IMAP	Port 143 is mainly used for Internet Message Access Protocol v2 (IMAP). Like POP3, it is a protocol for receiving emails.
443	HTTPS	A web browsing port and another type of HTTP that provides encryption and transmission through secure ports.
1433	SQL Server	Port 1433 is the default port of the SQL Server, which uses two ports: TCP-1433 and UDP-1434. Port 1433 is used for SQL Server to provide external services, whereas port 1434 is used to respond to the requester regarding which TCP/IP port is being used by SQL Server.
3306	MySQL	Port 3306, the default port of MySQL database, is used for MySQL to provide external services.
3389	Windows Server Remote Desktop Services	Port 3389 is the service port for Windows 2000 (2003) Server remote desktop, which allows connection to a remote server using the Remote Desktop connection tool.

Port	Service	Description
8080	Proxy Port	Similar to port 80, port 8080 is used for the WWW proxy service for web browsing. The port number extension ":8080" is often appended to the URL when users visit a website or use a proxy server. In addition, after the Apache Tomcat web server is installed, the default service port is port 8080.

Network ACL
Rule Overview

Rule Overview

The network access control list (ACL) is an optional security layer at the subnet level, which is used to control the data flow entering and leaving the subnet and can be accurate to the protocol and port granularity.



Use Cases

You can associate the same network ACL for subnets with the same network traffic control and precisely control the traffic entering and leaving the subnet by setting outbound and inbound rules.
For example, suppose you host multi-layer web applications in the VPC of the cloud platform and create different subnets to deploy web layer, logical layer, and data layer services, respectively, through the network ACL. In that case, you can control access between these three subnets so that the web layer subnet and the data layer subnet cannot access each other. Still, only the logical layer can access the web layer and

the data layer subnet.

ACL Rules

When you add or delete a rule in the network ACL, it is automatically applied to the network flow control of its associated subnet.
Network ACL rules include inbound and outbound rules, which are composed of the following:

- Source/Destination IP: source/destination IP of traffic. If it is an inbound rule, you need to enter the source IP; if it is an outbound rule, you need to enter the destination IP. Both source and destination IPs support the following format:
  - Single IP address: 192.168.0.1 or FF05::B5
  - CIDR: 192.168.1.0/24 or FF05:B5::/60
  - All IPv4 addresses: 0.0.0.0/130618222416261120
  - All IPv6 addresses: 0::0/130618222416261120 or ::/130618222416261120
- Protocol type: Select the protocol type allowed/denied by ACL rules, such as TCP and UDP.
- Port: source/destination port of traffic. The port supports the following formats:
  - Single port: e.g. 22 or 80
  - Continuous port: e.g. 1-65535 or 100-20000
  - All ports: ALL
- Policy: Allow or deny.

Default Rules

Once created, every network ACL has two default rules that cannot be modified or deleted, with the lowest priority.

- Default Inbound Rule

Protocol type	Port	Source IP	Policies	Description
ALL	ALL	0.0.0.0/130618222416261120	Deny	Deny all inbound traffic.

- Default Outbound Rule.

Protocol type	Port	Source IP	Policies	Description
ALL	ALL	0.0.0.0/130618222416261120	Deny	Deny all outbound traffic.

Rule Priority

- The priority of network ACL rules is indicated by the position of the rule in the list. The rule at the top of the list has the highest priority and is applied first, while that at the bottom of the list has the lowest priority.
- If there is a rule conflict, the rule with the higher priority will prevail by default.
- When traffic enters or leaves a subnet bound to a network ACL, it matches against the rules from the top of the network ACL list to the last. If a rule is successfully matched and allows passage, subsequent rules are not matched.

Application Example

Example: To allow all source IPs to access all ports on the CVM within the ACL-associated subnet while denying HTTP service access on port 80 from the server source IP 192.168.200.11/24 , you can add the following two network ACL inbound rules:

Protocol type	Port	Source IP	Policies	Description
HTTP	80	192.168.200.11/24	Deny	Deny the HTTP service of this IP address to access port 80.
ALL	ALL	0.0.0.0/130618222416261120	Allow	Allow all source IPs to access all ports.

Difference Between Security Group and Network ACL

Comparison Item	Security Group	Network ACL
Traffic Control	Traffic control at the instance level of CVM and database.	Traffic control at the instance level of subnet.
Rule	Allowing and denying rules are supported.	Allowing and denying rules are supported.
With or Without Status	With status: Returning data flow is automatically allowed, regardless of any rules.	Without status: Returning data flow must be explicitly allowed by the rule.
Effective Time	The rules are only applied to the instance when security groups are specified during the creation of instances, such as CVM and CDB, or when security groups are associated after the instance is created.	After the ACL is created and bound to the subnet, the ACL will be automatically applied to all CVM, CDB, and other instances in the associated subnet.

Comparison Item	Security Group	Network ACL
Rule Priority	If there is a rule conflict, the rule with the higher priority will prevail by default.	If there is a rule conflict, the rule with the higher priority will prevail by default.

Restrictions

Usage Limitations

- One network ACL can be bound to multiple subnets.
- The network ACL does not have any status; you need to set the outbound and inbound rules separately.
- The network ACL does not affect the private network interoperability between CVM instances within the associated subnet.

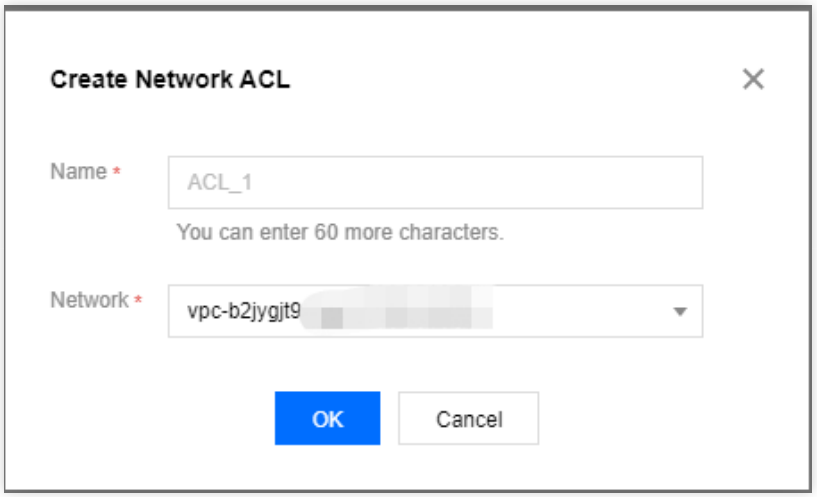
Quota Limitations

Resources	Limitation
Number of Network ACLs per VPC	50
Number of Rules per Network ACL	Number of inbound directions: 20 Number of outbound directions: 20
Number of Network ACLs Associated with Each Subnet	1

Managing Network ACL

Creating Network ACL

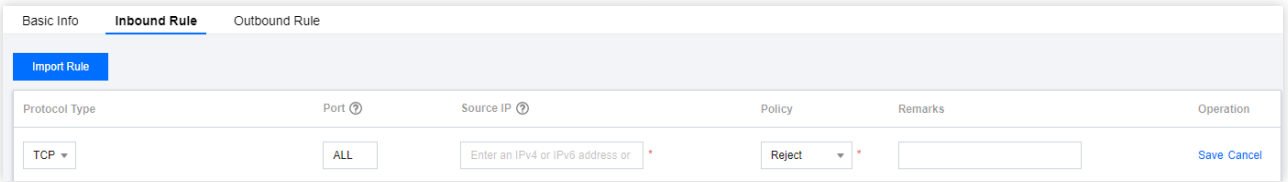
1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. At the top of the list, select the region and VPC, then click on +Create.
4. In the pop-up box, enter the name, select the VPC to which it belongs, and click on OK.



5. On the list page, click the corresponding ACL ID to enter the details page where you can add ACL rules and associated subnets.

Adding Network ACL Rules

1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. In the list, find the network ACL to be modified and click its ID. The details page is displayed.
4. To add an outbound/inbound rule, click on Outbound Rule or Inbound Rule > Edit > Add A Row. Select the protocol type, enter the port and source IP address, and select policy. You can also click on Import Rules to import rules in batches.
    - Protocol type: Select the protocol type allowed/denied by ACL rules, such as TCP and UDP.
    - Port: the source port of traffic, supporting a single port or port segment, such as 80 or 90-100.
    - Source IP: source IP or source IP range of traffic, supporting IP or CIDR, such as 10.20.3.0 or 10.0.0.2/24 .
    - Policy: Allow or deny.



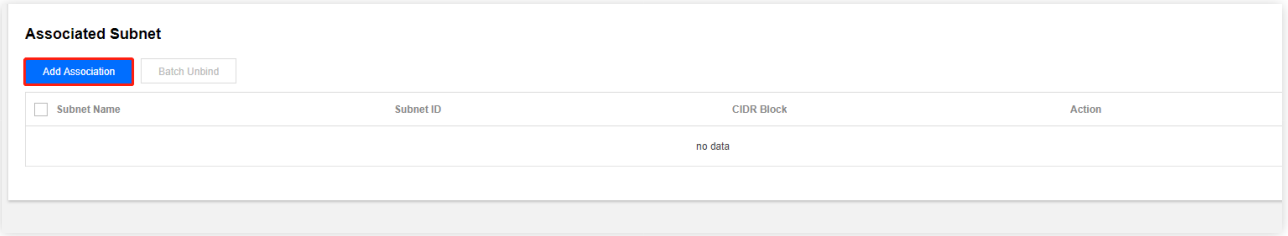
5. Click on Save.

Deleting Network ACL Rules

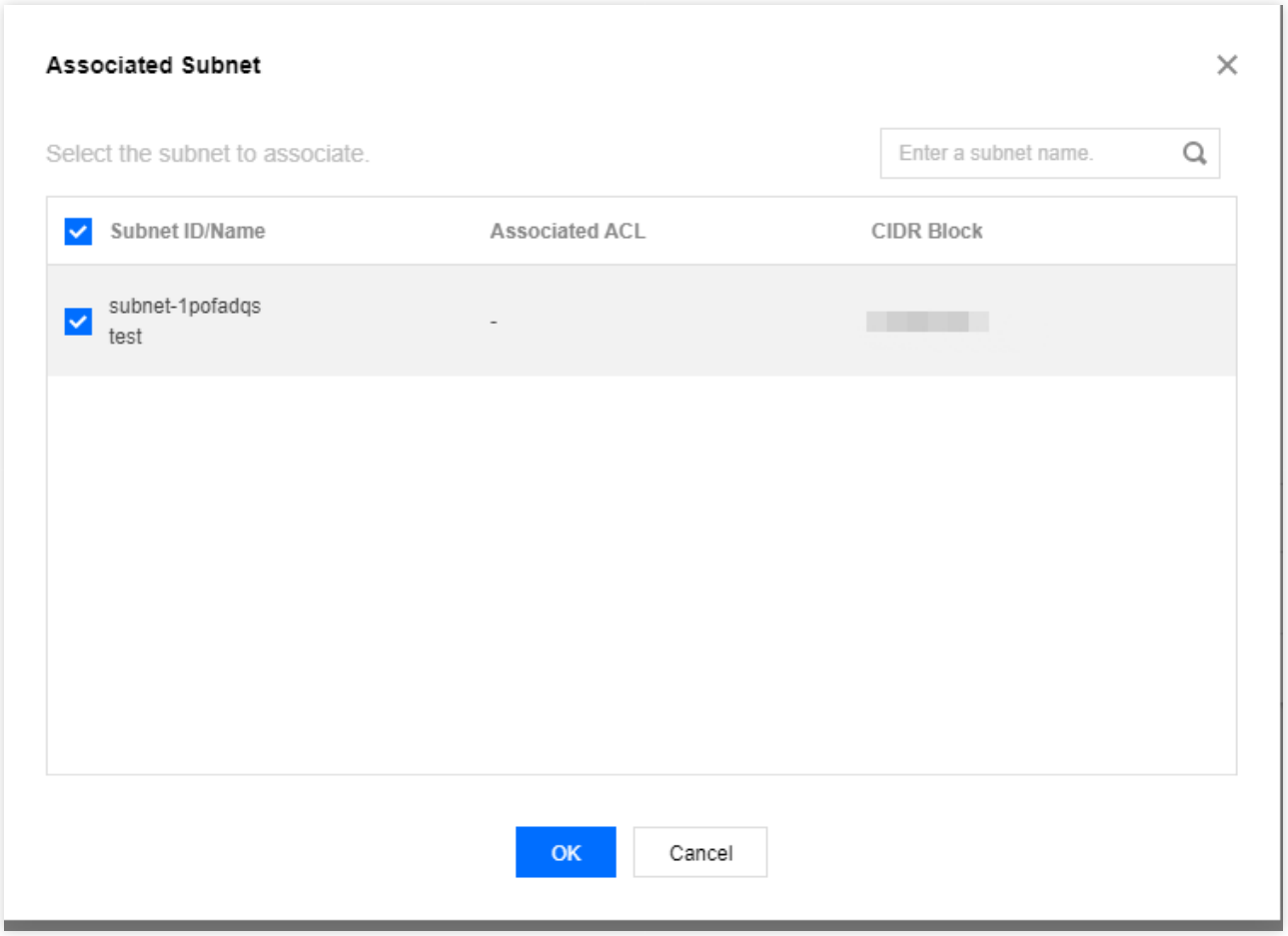
1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. In the list, find the network ACL to be deleted and click its ID. The Basic Information page is displayed.
4. Click on the Inbound Rules or Outbound Rules tab to enter the Rule List page.
5. Click on Edit to delete the inbound rules in the same steps as that of deleting the outbound rules. This document takes the deletion of inbound rules as an example.
6. In the list, find the row of the rule you wish to delete, then click on Delete under the operation column.
   At this time, the ACL rule is grayed out. If this deletion is an incorrect operation, you can click on Restore Deletion under the operation column to restore it.
7. Click on Save to save the above operations.
   The deletion or restoration of ACL rules will take effect only after being saved.

Associating Subnet to Network ACL

1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. In the list, find the network ACL to be associated with and click its ID. The details page is displayed.
4. On the Basic Information page, in the Associated Subnets module, click on Add Association.

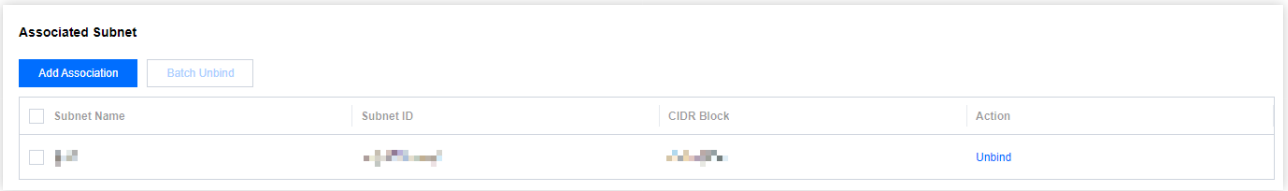


5. In the pop-up window, select the subnet you want to associate with, and then click on OK.



Disassociating Subnet from Network ACL

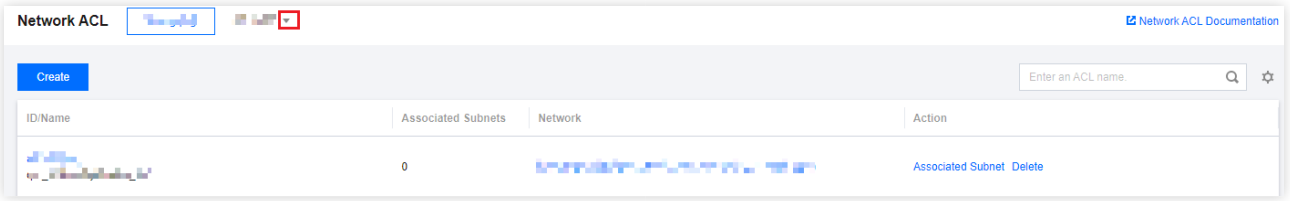
1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. In the list, find the network ACL to be disassociated and click its ID. The details page is displayed.
4. There are the following methods to disassociate subnets:
   - Method 1: In the Associate Subnet module on the Basic Information page, find the subnet to be disassociated and click on Unbind.



   - Method 2: In the Associated Subnet module on the Basic Information page, check all subnets that need to be disassociated and click on Batch Unbind.
5. Click on OK in the pop-up window.

Deleting Network ACL

1. Log in to the VPC console.
2. In the left directory, click on Security > Network ACL to go to the management page.
3. Select the region and the VPC.
4. In the list, find the network ACL to be deleted and click its ID. The details page is displayed.
5. Click on Delete and confirm the operation to delete this network ACL and all its rules.
   If Delete is grayed out, as shown for network ACL testEg in the image below, it means the network ACL is currently associated with a subnet. You need to disassociate it from the subnet before you can proceed with the deletion.



Parameter Template Restrictions

Usage Limitations

- Formats supported by the IP address template are as follows:
- Single IP, such as 10.0.0.1 .
- Consecutive IP, such as 10.0.0.1 - 10.0.0.100 .
- IP range, such as 10.0.1.0/24 .
- Formats supported by the port template are as follows:
- Single port, such as TCP:80 .
- Multiple discrete ports, such as TCP:80, 443 .
- Consecutive ports, such as TCP:3306-20000 .
- All ports, such as TCP: ALL .

Quota Limitation

Instance	Limitation (Unit: count)
IP Address Objects (ipm)	Maximum 1,000 per tenant
IP Address Group Objects (ipmg)	Maximum 1,000 per tenant
Protocol Port Objects (ppm)	Maximum 1,000 per tenant
Protocol Port Group Objects (ppmg)	Maximum 1,000 per tenant
IP Address Members in An IP Address Object (ipm)	Maximum 20 per tenant
IP Address Object Members (ipm) in An IP Address Group Object (ipmg)	Maximum 20 per tenant
Protocol Port Members Within A Protocol Port Group Object (ppm)	Maximum 20 per tenant
Protocol Port Object Members (ppm) in A Protocol Port Group Object (ppmg)	Maximum 20 per tenant

Instance	Limitation (Unit: count)
The Number of IP Address Group Objects (ipmg) that Can Reference the Same IP Address Objects (ipms)	Maximum 50 per tenant
The Number of Protocol Port Group Objects (ppmg) that Can Reference the Same Protocol Port Object (ppm)	Maximum 50 per tenant

> Note:
>
> The parameter template can be referenced by security groups. Once a security group references a parameter template feature, the IPs/ports within the parameter template will be expanded into multiple security group rules. Note that the totals of rule entries for each security group cannot exceed 2,000 after expansion.

Managing Parameter Templates

A parameter template is a collection of parameters that support saving IP addresses and protocol ports as templates. It can be directly referenced when adding security group rules.Converge Cloud supports the following four types of parameter templates:
Converge Cloud supports the following four types of parameter templates:

- IP address (ipm): Supports single IP, CIDR, and IP range.
- IP address group (ipmg): a collection of multiple IP address objects.
- Protocol port (ppm): Supports single port, multiple ports, consecutive ports, and all ports, with the protocol supporting TCP, UDP, ICMP, and GRE protocol.
- Protocol port group (ppmg): a collection of multiple protocol port objects.

Overview

Operation scenarios of the parameter template are as follows:

- Manage multiple IP addresses or protocol port groups with the same requirements.
- Manage multiple IP addresses or protocol port groups with frequent editing requirements.

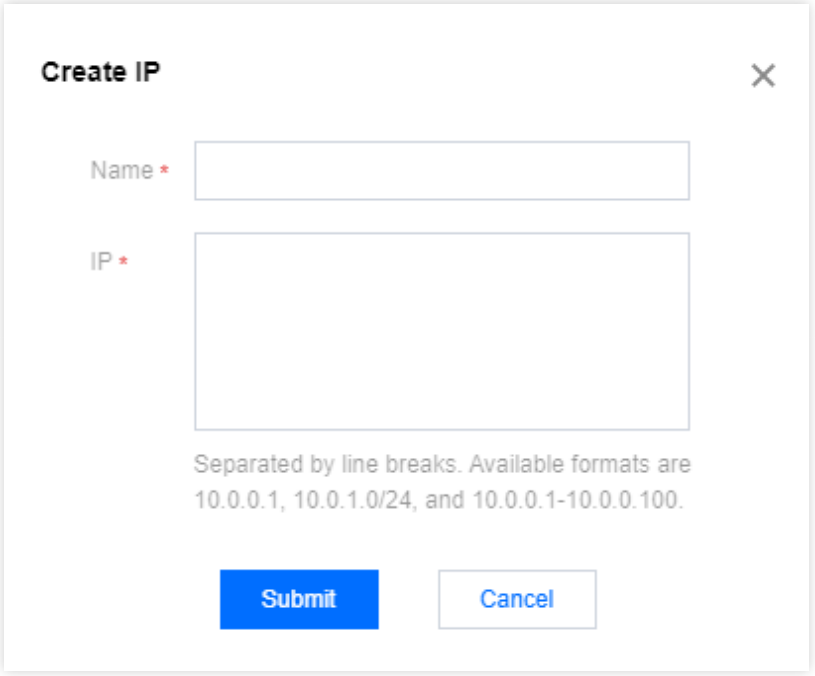
Step 1: Create a parameter template

1. Creating An IP Address Parameter Template

Add the IPs with the same requirements or frequent editing requirements to the IP address object.

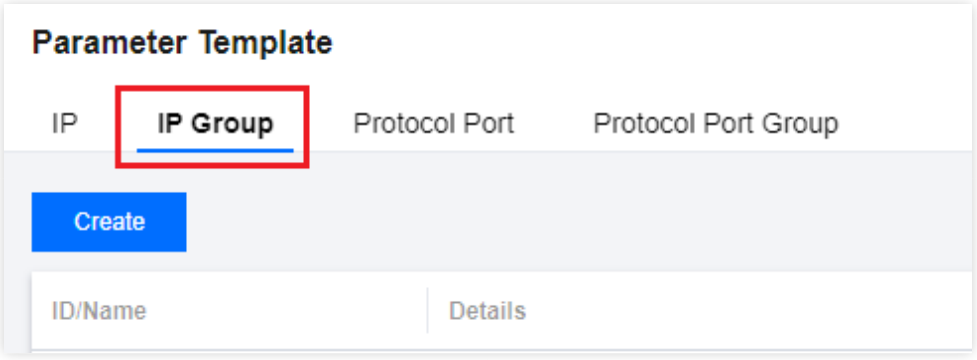
1. Log in to the VPC console.
2. Click on Security > Parameter Template in the left sidebar to enter the management page.
3. On the IP Address tag page, click on +Create.
4. In the pop-up window, fill in the name and IP address, then click on Submit.
   To add multiple IP addresses, separate them with a new line. The supported IP address formats are as follows:

- Single IP, such as 10.0.0.1 .
- IP range, such as 10.0.1.0/24 .
- Consecutive IP, such as 10.0.0.1 - 10.0.0.100 .

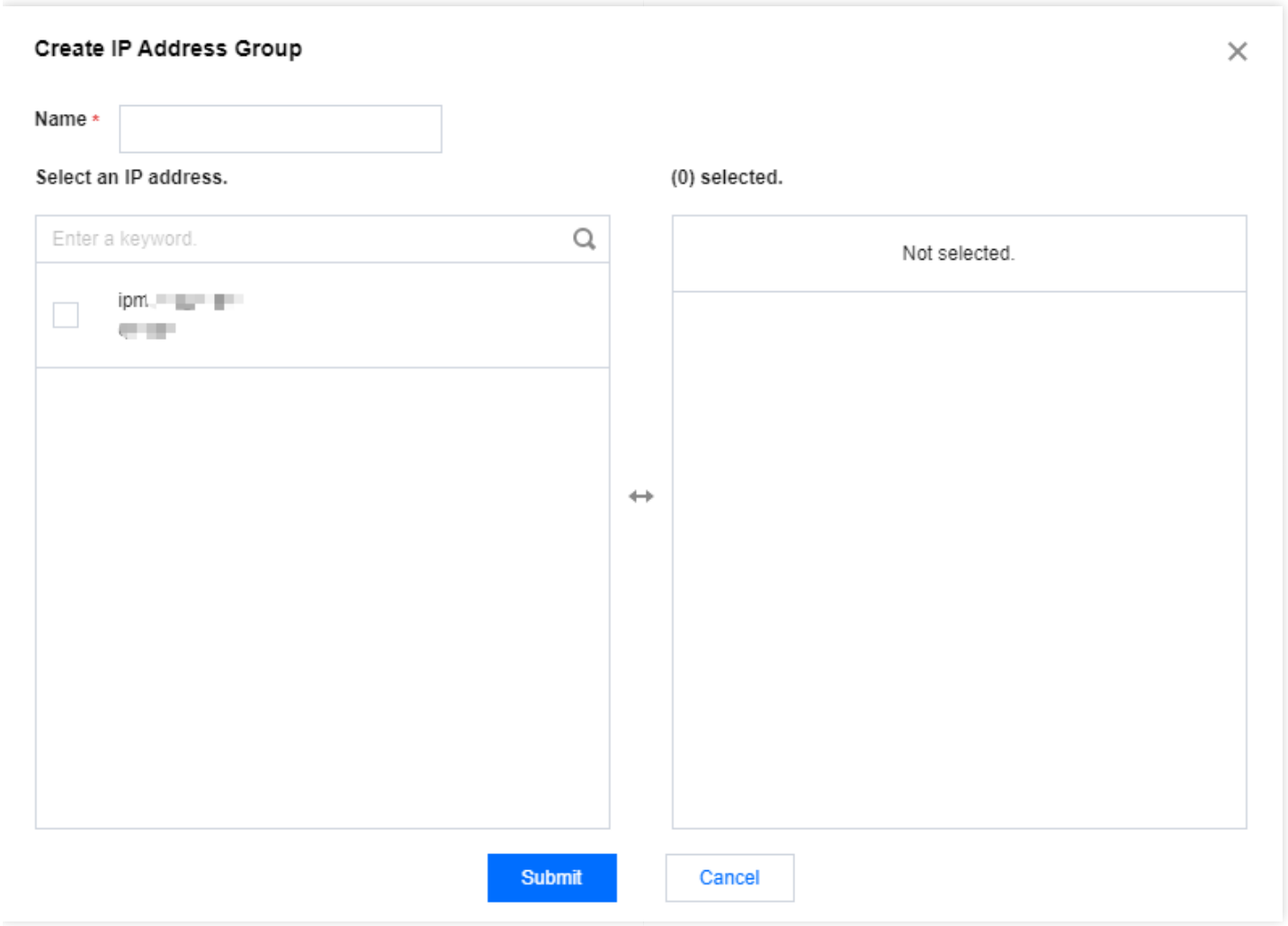


5. (Optional) You can add several created IP addresses to an IP address group, making it an IP address group.

6. Select the IP Address Group tag page to enter the management page, then click on +Create.



7. In the pop-up window, fill in the name and select the IP addresses to be added, then click on Submit.

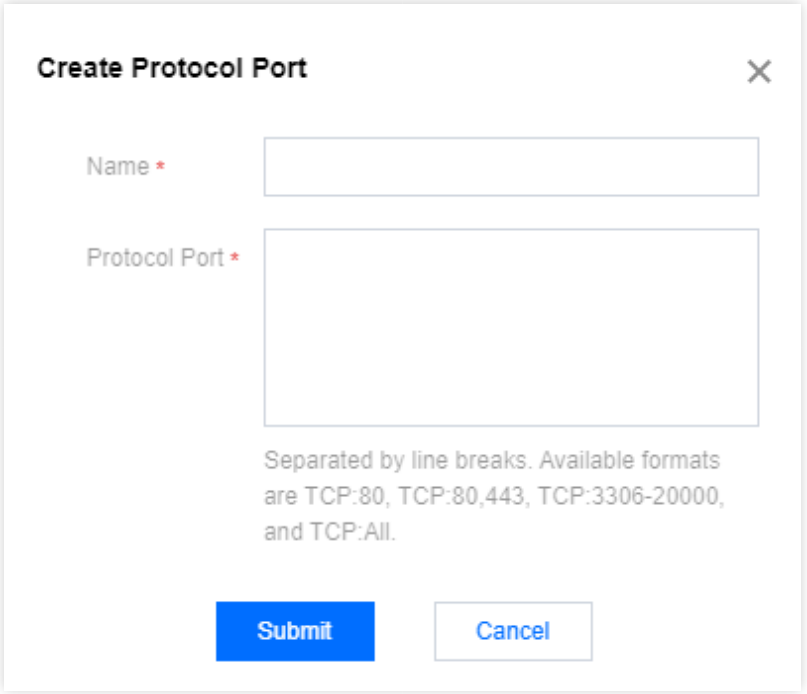


2. Creating A Protocol Port Parameter Template

Add protocol ports with the same requirements or frequent editing requirements to the protocol port object.

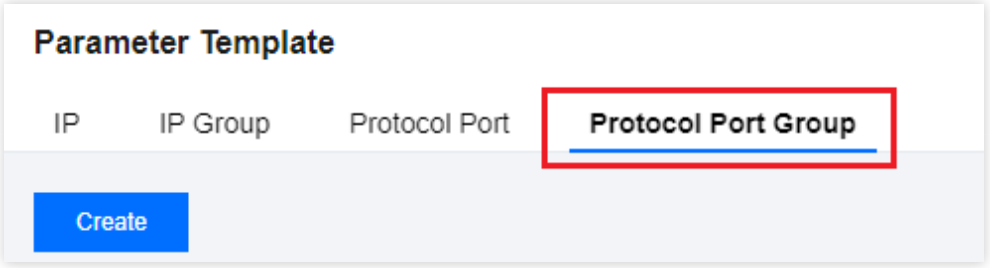
1. Log in to the VPC console.
2. Click on Security > Parameter Template in the left sidebar to enter the management page.
3. Click on the Protocol Port tab, enter the Protocol Port tag page, and click on +Create.
4. In the pop-up window, fill in the name and protocol port, then click on Submit.
   To add multiple protocol ports, separate them with a new line. The protocol ports support the following formats:

- Single port, such as TCP:80 .
- Multiple discrete ports, such as TCP:80,443 .
- Consecutive ports, such as TCP:3306-20000 .
- All ports, such as TCP: ALL .

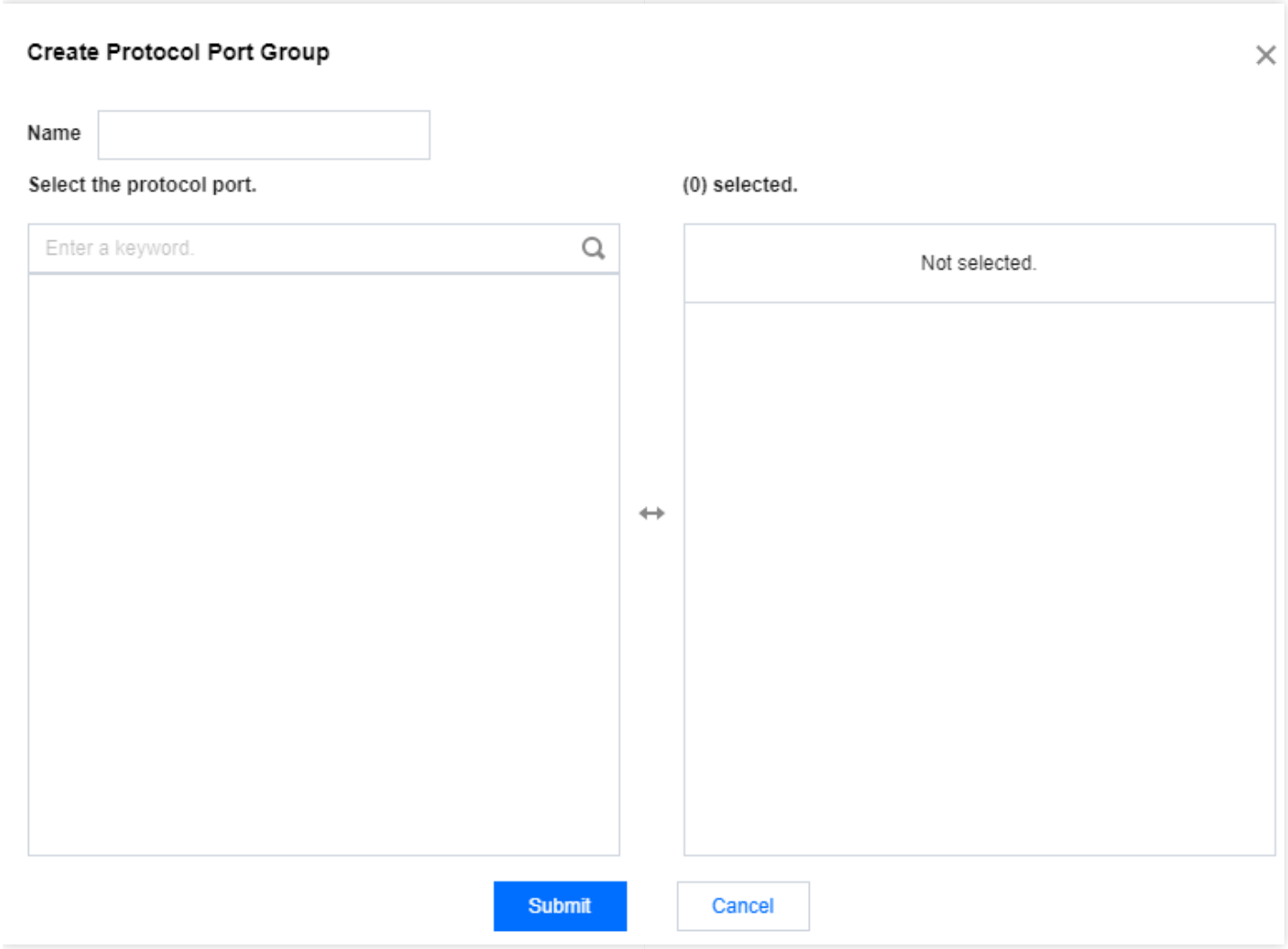


5. (Optional) You can add the created multiple protocol ports to a protocol port group at the same time, as a protocol port group.

6. Select the Protocol Port Group tag page to enter the management page, then click on +Create.

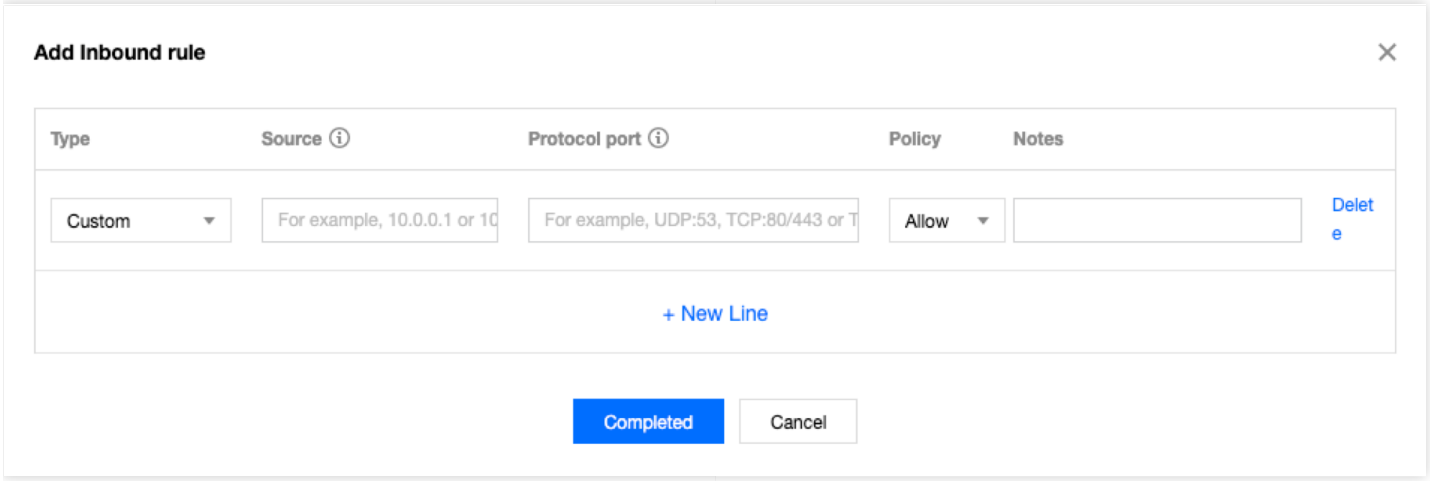


7. In the pop-up window, fill in the name and select the protocol ports to be added, then click on Submit.



Step 2: Refer to the parameter template in the security group

1. Log in to the VPC console.
2. Click on Security > Security Group in the left sidebar to enter the management page.
3. In the list, find the security group that needs to reference the parameter template and click its ID to enter the details page.
4. In the inbound/outbound rule tag page, click on Add Rules.
5. In the pop-up window for sources and protocol ports, select the corresponding parameter template. For detailed steps on adding inbound/outbound rules, refer to Adding a Security Group Rule. > If you need to add a new IP address or protocol port in the future, you only need to add it to the corresponding IP address group or protocol port group, and there is no need to modify the security group rules or create another security group.


Add Inbound rule
Type
Source
Protocol port
Policy
Notes
Custom
For example, 10.0.0.1 or 10
For example, UDP:53, TCP:80/443 or T
Allow
Delet
e
+ New Line
Completed
Cancel

Cloud Access Management
CAM Overview

If you use services such as VPC, CVM, and databases in Converge Cloud, and these services are managed by different people but share your cloud account key, the following problems may arise:

- Your key is shared by multiple people and the risk of leakage is high.
- The access of other users is not under control, which can introduce security risks caused by misoperations.
  To prevent these problems, you can use sub-accounts to allow different users to manage different services. By default, a sub-account has no permission to use CVM or CVM-related resources. Therefore, we need to create policies to allow sub-accounts to use the resources or permissions they need.

Overview

Cloud Access Management (CAM) is a set of web services provided by Converge Cloud. It primarily helps customers securely manage access permissions to resources under the Converge Cloud account. With CAM, you can create, manage, and terminate users (groups), and control who can use which Converge Cloud resources through identity and policy management.

You can use CAM to bind a user or user group to a policy that allows or denies them access to specified resources to complete specified tasks.

- For more basic information on CAM policies, refer to Syntax Logic.
- For more use information on CAM policies, refer to Policy.
  Skip this chapter if you don't need cloud access management of VPC resources for sub-accounts. Skipping this chapter does not affect your understanding and use of the rest of the document.

Getting Started

The CAM policy allows or denies one or more VPC operations. You must also specify the resources that can be used for the operation (it can be all resources, or some operations can be partial resources). The policy can also contain the conditions set by the operation resources.

Some VPC API operations support resource-level permissions. That is, you cannot specify a specific resource for these API operations. Instead, you must specify all the operations resources.

Task	Link
Basic Policy Structure	Policy Syntax
Defining Operations in A Policy	VPC Operations
Defining Resources in A Policy	VPC Resource Paths
Resource-level Permissions Supported by VPC	Resource-level Permissions Supported by VPC
Console Example	Console Example

Authorizable Resource Type

Policy Syntax

CAM policy:

```
{
       "version":"2.0",
       "statement":
       [
         {
           "effect":"effect",
           "action":["action"],
           "resource":["resource"],
            "condition": {"key":{"value"}}
         }
      ]
}
```

- The version is required, currently only allowing a value of "2.0".
- Statement is used to describe the detailed information of one or more permissions. This element includes the permissions or permission sets of multiple other elements such as effect, action, resource, and condition. A policy has one and only one statement element.

1. action used to describe the operations that are allowed or denied. Operations can be APIs (described with a name prefix) or feature sets (a specific set of APIs described with a permid prefix). This element is required.
2. resource describes the detailed data authorized. Resources are described using six paragraphs. The resource definition details will vary for each product. For information on how to specify resources, please refer to the product documentation corresponding to the resource declaration you have written. This element is required.
3. conditions describes the constraints under which the policy takes effect. Conditions consist of operators, operation keys, and operation values. Condition values can include information such as time and IP address. Some services allow you to specify additional values in the condition. This element is optional.
4. effect describes whether the statement produces an "allow" or "explicit deny" result. It includes allow and deny. This element is required.

VPC Operations

In the CAM policy statement, you can specify any API operation from any service that supports CAM. For VPC, use APIs prefixed with name/vpc:. For example, name/vpc:Describe or name/vpc:CreateRoute.
If you want to specify multiple actions in a single statement, separate them with commas as follows:

```
"action":["name/vpc:action1","name/vpc:action2"]
```

You can also use wildcard characters to specify multiple actions. For example, you can specify all actions whose names begin with the word Describe as follows:

```
"action":["name/vpc:Describe*"]
```

To specify all operations in a VPC, use a wildcard (*) as follows:

```
"action":["name/vpc:*"]
```

VPC Resource Paths

Each CAM policy statement has its own resources that apply to it.
The general format of resource paths is as follows:

```
**qcs:project_id:service_type:region:account:resource**
```

- project_id: Describe the project information. It is only for compatibility with early CAM logic and does not need to be filled in.
- service_type: the product abbreviation, such as VPC.
- region: regional information, such as bj.
- account: the root account information of the resource owner, such as uin/164256472.
- resource: the specific resource details of each product, such as vpc/vpc_id1 or vpc/*.
  For example, you can specify an instance (vpc-d08sl2zr in this case) in the statement, as shown below:

```
"resource":[ "qcs::vpc:bj:uin/164256472:instance/vpc-d08sl2zr"]
```

You can also use the * wildcard character to specify all instances belonging to a specific account, as follows:

```
"resource":[ "qcs::vpc:bj:uin/164256472:instance/*"]
```

If you want to specify all resources, or if a specific API operation does not support resource-level permissions, use the * wildcard in the Resource element as shown:

```
"resource": ["*"]
```

To specify multiple resources in one instruction, separate them with a comma. The following is an example of specifying two resources:

```
"resource":["resource1","resource2"]
```

The following table describes the resources that can be used by VPC and the corresponding methods of describing these resources.

In the following table, words prefixed with $ are aliases.

- Here, project refers to the Project ID.
- Here, region refers to the Region.
- Here, account refers to the Account ID.

Resources	Resource description method in authorization policy
VPC	qcs::vpc:$region:$account:vpc/$vpcId
Subnet	qcs::vpc:$region:$account:subnet/$subnetId
Security Group	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

VPC CAM Policy Examples

Full Read-Write Policy of VPC

The following policy allows you to create and manage VPC. You can associate this policy with a group of network administrators. The Action element specifies all VPC-related APIs.

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Read-only Policy of VPC

The following policy allows you to query your VPC and relevant resources. However, you cannot create, update, or delete them with this policy.
In the console, the premise of operating a resource is that it can be viewed, so it is recommended you open VPC read-only permissions for users.

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
```

```
}
```

Only sub-accounts are allowed to manage a single VPC

The following policies allow users to see all VPCs but only operate VPC A (assuming that the ID of A is vpc-d08sl2zr) and network resources under A (such as subnets and routing tables, excluding CVM and databases) and do not allow users to manage other VPCs.
This version does not support Only Allowing Users to View A, which will be supported in subsequent versions.

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "name/vpc:*",
            "resource": "*",
            "effect": "allow",
            "condition": {
                "string_equal_if_exist": {
                    "vpc:vpc": [
                    "vpc-d08sl2zr"
                    ],
                    "vpc:accepter_vpc": [
                     "vpc-d08sl2zr"
                    ],
                     "vpc:requester_vpc": [
                     "vpc-d08sl2zr"
                    ]
                }
            }
        }
    ]
}
```

Users are allowed to manage VPC but cannot operate routing table

The following policies allow users to read and write the VPC and its related resources but do not allow users to perform related operations on routing tables.

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "name/vpc:AssociateRouteTable",
                "name/vpc:CreateRoute",
                "name/vpc:CreateRouteTable",
                "name/vpc:DeleteRoute",
                "name/vpc:DeleteRouteTable",
                "name/vpc:ModifyRouteTableAttribute"
            ],
            "resource": "*",
            "effect": "deny"
        }
    ]
}
```

Users are allowed to manage VPC resources

This policy allows users to view all VPC resources but only allows them to add, delete, modify, and check VPNs.

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "name/vpc:Describe*",
                "name/vpc:Inquiry*",
                "name/vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
```

```
            "action": [
                "name/vpc:*Vpn*",
                "name/vpc:*UserGw*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

Resource-level Permissions Supported by VPC API Operations

In CAM, the following API operations can be performed on VPC resources. The corresponding relationship between resources and conditions supported by specific APIs is as follows:

> Note: If the VPC API does not support resource-level permissions in the table, you can grant users access to VPC APIs that are not in this list but must specify * for resource elements of policy statements.

API Operation	Resources	Condition	Remarks
AcceptVpcPeeringConnection	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc:region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc:$region: $account:pcx/ $peeringConnectionId</	vpc:accepter_vpc vpc:region vpc:requester_vpc	The value of vpc: accepter_vpcq is the accepter VPC. vpc: Region indicates the region where it is located. The value of vpc: requester_vpc is the requester VPC.
—	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId (accepter vpcId)	vpc:region	vpc: Region indicates the region where the VPC is located.
AcceptVpcPeeringConnectionEx	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc: $region:$account:pcx/ $peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: accepter_vpc_region indicates the accepter region. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: requester_vpc_region indicates the requester region.
—	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
AddVpnConnEx	VPC resources qcs::vpc:$region:	vpc:region	vpc: Region indicates the region where the VPC is

API Operation	Resources	Condition	Remarks
	$account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId		located.
—	VPN gateway resources qcs::vpc:$region: $account:vpngw/* qcs::vpc:$region: $account:vpngw/ $vpnGwId	vpc:vpc vpc:region	vpc:vpc represents the developer's VPC. vpc:region represents the region of the vpc.
—	Customer gateway resources qcs::vpc:$region: $account:cgw/*	vpc:region	vpc: Region indicates the region where the VPC is located.
—	VPN channel resources qcs::vpc:$region: $account:vpnx/*	vpc:vpc vpc:vpngw vpc:region	vpc: vpc indicates the developer's VPC. vpc:vpngw indicates the VPN gateway under the developer. vpc: Region indicates the region where the VPC is located.
AssignPrivateIpAddresses	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
AssociateVip	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region vpc:vpc	
AssociateRouteTable	Subnet resource qcs::vpc:$region: $account:subnet/* qcs::vpc:$region: $account:subnet/ $subnetId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
—	Routing table resources qcs::vpc:$region: $account:rtb/* qcs::vpc:$region: $account:rtb/ $routeTableId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
AttachClassicLinkVpc	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	CVM resources qcs::cvm:$region:	cvm:region	cvm: region indicates the area where the CVM is

API Operation	Resources	Condition	Remarks
	$account:instance/* qcs::cvm:$region: $account:instance/ $instanceId		located.
AttachNetworkInterface	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
—	CVM resources qcs::cvm:$region: $account:instance/* qcs::cvm:$region: $account:instance/ $instanceId	cvm:region	cvm: region indicates the area where the CVM is located
CreateAndAttachNetworkInterface	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	CVM resources qcs::cvm:$region: $account:instance/* qcs::cvm:$region: $account:instance/ $instanceId	cvm:region	cvm: region indicates the area where the CVM is located
—	ENI resources qcs::vpc:$region: $account:eni/*	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
CreateDirectConnectGateway	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Direct connect gateway resources qcs::vpc:$region: $account:dcg/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
CreateLocalDestinationIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateLocalIPTranslationAclRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateLocalIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateLocalSourceIPPortTranslationAclRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateLocalSourceIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreatePeerIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateNatGateway	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	NAT gateway resources qcs::vpc:$region:$account:nat/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
CreateNetworkAcl	VPC resource qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Network ACL resources qcs::vpc:$region:$account:acl/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateNetworkInterface	VPC Resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Subnet resource qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
—	ENI Resources qcs::vpc:$region:$account:eni/*	vpc:vpc vpc:subnet vpc:region	vpc: vpc indicates the developer's VPC. vpc: subnet indicates the developer's subnet. vpc: Region indicates the region where the VPC is located.
CreateRoute	Routing table resources qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateRouteTable	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Routing table resources qcs::vpc:$region:$account:rtb/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateSubnet	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Subnet gateway resources qcs::vpc:$region:$account:subnet/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
CreateSubnetAclRule	Network ACL resources qcs::vpc:$region: $account:acl/* qcs::vpc:$region: $account:acl/ $networkAclId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
—	Subnet gateway resources qcs::vpc:$region: $account:subnet/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
CreateVpcPeeringConnection	VPC resource (requester) qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region: $account:pcx/*	vpc:accepter_vpc vpc:requester_vpc vpc:region	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: Region indicates the region where the VPC is located.
CreateVpcPeeringConnectionEx	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resource qcs::vpc:$region: $account:pcx/*	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: accepter_vpc_region indicates the accepter region. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: requester_vpc_region indicates the requester region.
DeleteDirectConnectGateway	Direct connect gateway resources qcs::vpc:$region: $account:dcg/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is

API Operation	Resources	Condition	Remarks
	qcs::vpc$region: $account:dcg/ $directConnectGatewayId		located.
DeleteLocalDestinationIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteLocalIPTranslationAclRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteLocalIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteLocalSourceIPPortTranslationAclRule<	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeletePeerIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteLocalSourceIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteNatGatewaynat	Gateway resources qcs::vpc:$region: $account:nat/* qcs::vpc:$region: $account:nat/$natId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteNetworkAcl	Network ACL resources qcs::vpc:$region: $account:acl/*	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is

API Operation	Resources	Condition	Remarks
	qcs::vpc:$region: $account:acl/ $networkAclId		located.
DeleteNetworkInterface	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
DeleteRoute	Routing table resources qcs::vpc:$region: $account:rtb/* qcs::vpc:$region: $account:rtb/ $routeTableId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteRouteTable	Routing table resources qcs::vpc:$region: $account:rtb/* qcs::vpc:$region: $account:rtb/ $routeTableId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteSubnet	Subnet resource qcs::vpc:$region: $account:subnet/* qcs::vpc:$region: $account:subnet/ $subnetId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
DeleteUserGw	Customer gateway resources qcs::vpc:$region: $account:cgw/* qcs::vpc:$region: $account:cgw/$userGwId	vpc:region	vpc: Region indicates the region where the VPC is located.
DeleteVpc	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region vpc:vpc	vpc: Region indicates the region where the VPC is located.
DeleteVpcPeeringConnection	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc:$region: $account:pcx/ $peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
DeleteVpcPeeringConnectionEx	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc:$region: $account:pcx/ $peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region	vpc:requester_vpc vpc:requester_vpc_region
DeleteVpnConn	VPN channel resources qcs::vpc:$region: $account:vpnx/* qcs::vpc:$region: $account:vpnx/ $vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc: vpc represents the developer's VPC. vpc:vpngw indicates the gateway under the developer. vpc:usergw indicates the customer gateway under the developer. vpc: Region indicates the region where the VPC is located.
DetachClassicLinkVpc	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region vpc:vpc	vpc: Region indicates the region where the VPC is located.
—	CVM resources qcs::cvm:$region: $account:instance/* qcs::cvm:$region: $account:instance/ $instanceId	cvm:region	cvm: region indicates the area where the CVM is located
DetachNetworkInterface	CVM resources qcs::cvm:$region: $account:instance/* qcs::cvm:$region: $account:instance/ $instanceId	cvm:region	cvm: region indicates the area where the CVM is located
—	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
DeteleSubnetAclRule	Subnet resource qcs::vpc:$region: $account:subnet/* qcs::vpc:$region: $account:subnet/ $subnetId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
—	Network ACL resources qcs::vpc:$region: $account:acl/* qcs::vpc:$region: $account:acl/	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
	$networkAclId		
EipBindNatGateway	NAT gateway resources qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
EipUnBindNatGateway	NAT gateway resources qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
EnableVpcPeeringConnection	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region	
vpc:requester_vpc	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: Region indicates the region where the VPC is located.		
EnableVpcPeeringConnectionEx	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc pc:requester_vpc_region	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: accepter_vpc_region indicates the accepter region. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC.

API Operation	Resources	Condition	Remarks
			vpc: requester_vpc_region indicates the requester region.
MigrateNetworkInterface	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
—	CVM resources qcs::cvm:$region: $account:instance/* qcs::cvm:$region: $account:instance/ $instanceId (authorization is required before and after migration)	cvm:region	cvm: region indicates the area where the CVM is located.
MigratePrivateIpAddress	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
ModifyDirectConnectGateway	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyLocalDestinationIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyLocalIPTranslationAclRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyLocalIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region:	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
	$account:dcg/$directConnectGatewayId		
ModifyLocalSourceIPPortTranslationAclRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyPeerIPTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyLocalSourceIPPortTranslationNatRule	Direct connect gateway resources qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyNatGateway	NAT gateway resources qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/nat-dc7cdf	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyNetworkAcl	Network ACL resources qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyNetworkAclEntry	Network ACL resources qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyNetworkInterface	ENI resources qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.

API Operation	Resources	Condition	Remarks
ModifyPrivateIpAddress	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.
ModifyRouteTableAttribute	Routing table resources qcs::vpc:$region: $account:rtb/* qcs::vpc:$region: $account:rtb/ $routeTableId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifySubnetAttribute	Subnet resource qcs::vpc:$region: $account:subnet/* qcs::vpc:$region: $account:subnet/ $subnetId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
ModifyUserGw	Customer gateway resources qcs::vpc:$region: $account:cgw/* qcs::vpc:$region: $account:cgw/$userGwId	vpc:region	vpc: Region indicates the region where the VPC is located.
ModifyVpcAttribute	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:Region	vpc: Region indicates the region where the VPC is located.
ModifyVpcPeeringConnection	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc:$region: $account:pcx/ $peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_vpc
ModifyVpcPeeringConnectionEx	VPC resources qcs::vpc:$region: $account:vpc/* qcs::vpc:$region: $account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region: $account:pcx/* qcs::vpc:$region:	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC.

API Operation	Resources	Condition	Remarks
	$account:pcx/$peeringConnectionId		vpc: accepter_vpc_region indicates the accepter region. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: requester_vpc_region indicates the requester region.
ModifyVpnConnEx	VPN channel resources qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc: vpc represents the developer's VPC. vpc:vpngw indicates the gateway under the developer. vpc:usergw indicates the customer gateway under the developer. vpc: Region indicates the region where the VPC is located.
ModifyVpnGw	VPN gateway resources qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
RejectVpcPeeringConnection	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc: accepter_vpc indicates the accepter VPC, and the value is taken as the accepter VPC. vpc: requester_vpc indicates the requester VPC, and the value is taken as the requester VPC. vpc: Region indicates the region where the VPC is located.
RejectVpcPeeringConnectionEx	VPC resources qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc: Region indicates the region where the VPC is located.
—	Peering connection resources qcs::vpc:$region:	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc	vpc:requester_vpc_region

API Operation	Resources	Condition	Remarks
	$account:pcx/* qcs::vpc:$region: $account:pcx/ $peeringConnectionId		
ResetVpnConnSA	VPN channel resources qcs::vpc:$region: $account:vpnx/* qcs::vpc:$region: $account:vpnx/ $vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc: vpc represents the developer's VPC. vpc:vpngw indicates the gateway under the developer. vpc:usergw indicates the customer gateway under the developer. vpc: Region indicates the region where the VPC is located.
SetLocalIPTranslationAclRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	\vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
SetLocalSourceIPPortTranslationAclRule	Direct connect gateway resources qcs::vpc:$region: $account:dcg/* qcs::vpc:$region: $account:dcg/ $directConnectGatewayId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
SetSSLVpnDomain	VPN gateway resources qcs::vpc:$region: $account:vpngw/* qcs::vpc:$region: $account:vpngw/ $vpnGwId	vpc:vpc vpc:region	vpc: vpc indicates the developer's VPC. vpc: Region indicates the region where the VPC is located.
UnassignPrivateIpAddresses	ENI resources qcs::vpc:$region: $account:eni/* qcs::vpc:$region: $account:eni/ $networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc: vpc represents the developer's VPC. vpc: subnet indicates the subnet under the developer. vpc: Region indicates the region where the VPC is located.

Network Probing

Network probing is a service for monitoring the quality of VPC network connection, which can monitor key metrics such as the latency and packet loss rate of the network connection for you.

In a hybrid cloud network architecture, you will use VPN/dedicated line to connect the cloud VPC and your own IDC. In order to monitor the network quality of the connection in real time, you can create a network probing object in the subnet that needs to communicate with the IDC. After the probing object is created, the packet loss rate and latency of the probed link will be returned, helping you achieve the following features:

- Real-time monitoring of connection quality.
- Real-time alerts for connection failures.

Usage Instructions

- Network probing is Ping probing with a frequency of 20 times per minute.
- Up to 50 network probing instances can be created within each VPC.
- Network probing can be created for up to 20 subnets under the same VPC.

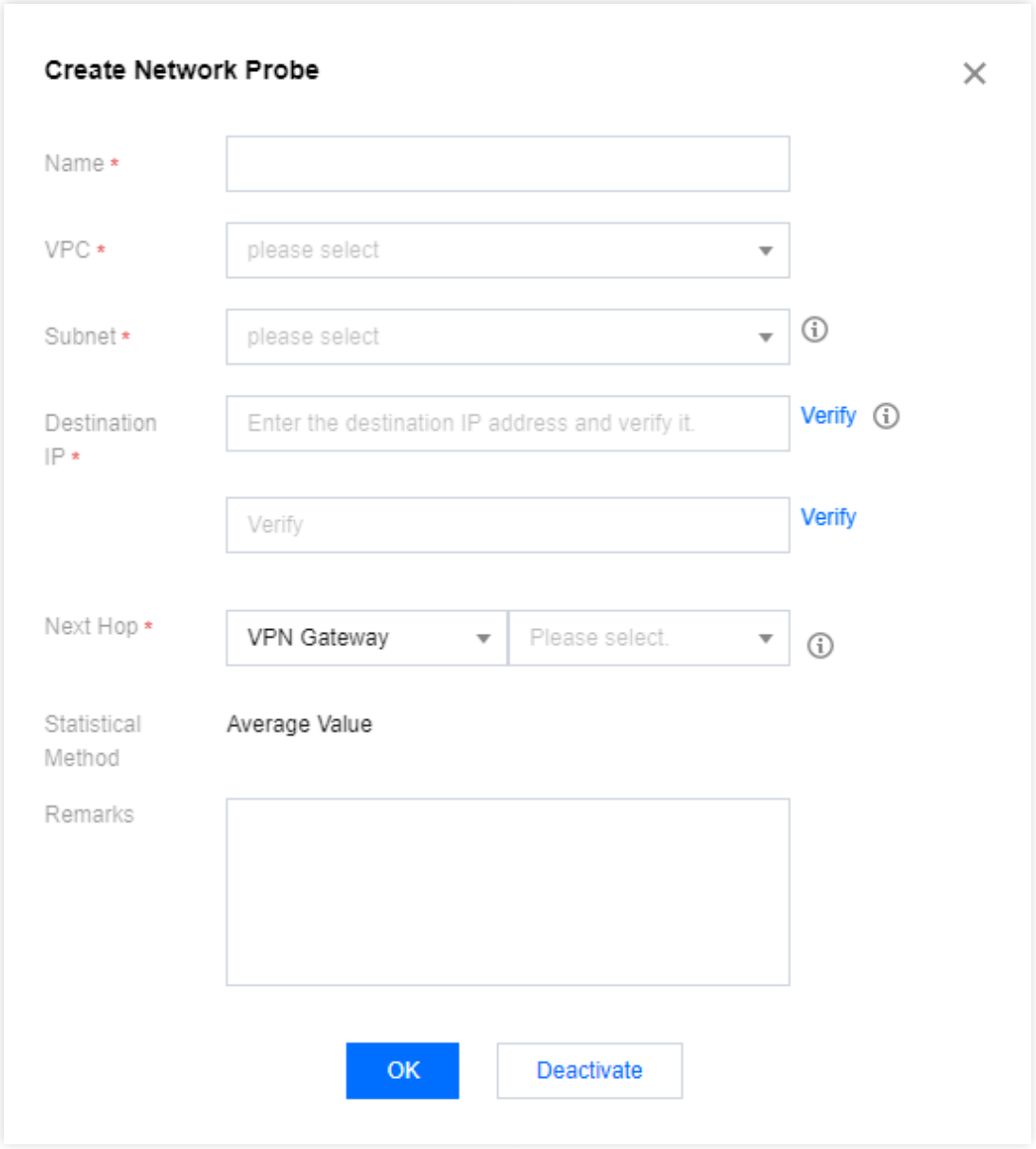
Create Network Probing

1. Log in to the VPC console.

2. In the left menu, click Network Probing.

3. At the top of the management console, click Create.

4. In the Create Network Probing pop-up window, fill in the relevant fields.



Field Description:

Field	Meaning
Name	The name of network probing.
Virtual Private Cloud,VPC	The VPC where the probing source IP is located.
Subnet	The subnet where the probing source IP is located.
Probing Destination IP	Network probing supports up to two destination IP addresses. Please enable ICMP firewall policy for the destination host of network probing.

Field	Meaning
Next Hop	For source next hop routes, please select the source next hop type and specific instances. Currently supported source next hop gateway types include: NAT gateway, peering connection, VPN gateway, direct connect gateway and CVM. Note: - After the next hop object is configured, the system will automatically add the corresponding 32-bit route to the route table associated with the subnet. - The network probing route is a system route and cannot be modified. - When switching a subnet's route, this system route will be deleted from the original subnet's associated route table and added to the subnet's newly created route table.

5. After filling in the fields, click Verify after Probing Destination IP.

- If the connection succeeded, click OK.
- If the connection failed, please check whether the subnet route is correctly configured or whether the destination probing target has allowed traffic through network ACLs, security groups, or other firewall rules. For details, see Manage Network ACL and Modify Security Group Rules.

Check Network Probing Latency and Packet Loss Rate

1. Log in to the VPC console.
2. In the left menu, click Network Probing.
3. In the Monitoring column of the target network probing instance, click the monitoring icon to view the network probing latency and packet loss rate.

Modify Network Probing

1. Log in to the VPC console.
2. In the left menu, click Network Probing.
3. In the list of network probing instances, find the network probing instance to be modified, and click Edit in the Operation column on the right.
4. In the Edit Network Probing dialog box, enter the information to be modified and click OK.

> Note:
>
> Name modification, probing destination IP, source next hop routing and annotation are supported.

Delete Network Probing

1. Log in to the VPC console.
2. In the left menu, click Network Probing.
3. In the list of network probing instances, find the network probing instance to be modified, and click Delete in the Operation column on the right.
4. In the pop-up confirmation box, click Delete.

> Note:
>
> Deleting a network probing instance will also delete associated alarm policies and route configurations of the network probing. Please assess the business impact and proceed with caution.

Configure Alarms

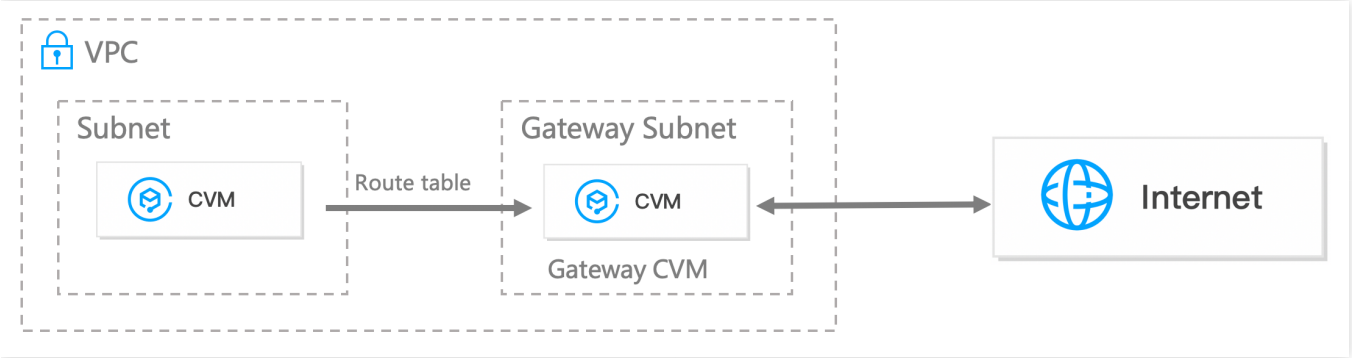
You can configure monitoring alarms for network probing. When a routing exception is detected, users can be alarmed in time to quickly switch the route and ensure service availability.

1. Log in to the Alarm Policy console.
2. Click Create.
3. In the pop-up Create Alarm Policy dialog box, fill in the policy name, set Policy Type to Virtual Private Cloud/Network Probing, select specific instances, configure alarm triggering conditions, alarm notifications and other information, and then click Complete.

Best Practice
Configure the cloud server as a public gateway

Overview

When some of the cloud servers in the Converge Cloud VPC do not have a regular public IP but need to access the Internet, you can use a cloud server with a public IP (either a regular public IP or an elastic public IP) to access the Internet. The public gateway cloud server will perform source address translation for outbound traffic. After the traffic from all other cloud servers passes through the public gateway cloud server to access the Internet, the source IP is converted to the public IP address of the public gateway cloud server, as shown in the diagram below:



Prerequisites

- Logged in to the Cloud Server Console.
- The public gateway cloud server can only forward routing requests for subnets other than its own. Therefore, the public gateway cloud server cannot be in the same subnet as the cloud servers that need to use the public gateway to access the Internet.
- The public gateway cloud server must be a Linux cloud server; Windows cloud servers cannot be used as a public gateway.

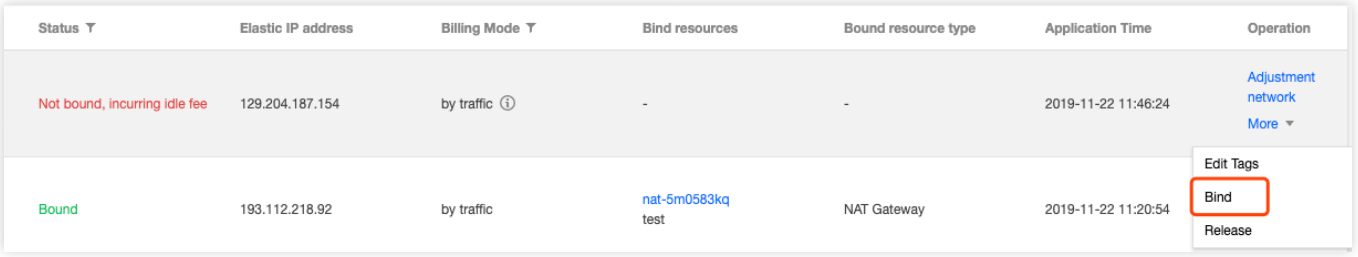
Directions

Step 1: bind an EIP (optional)

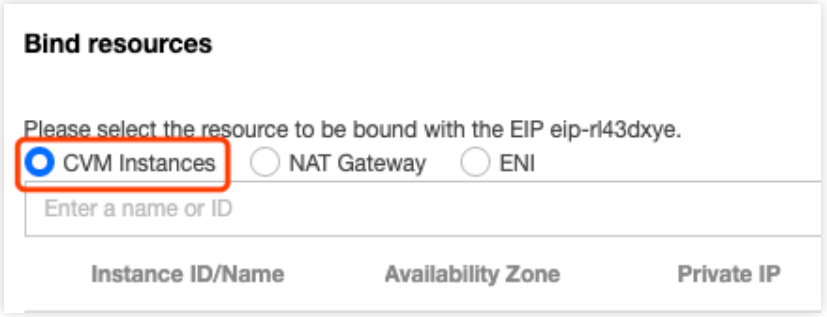
> Note:

> If the cloud server used as a public gateway already has a public IP address, skip this step and proceed with the subsequent steps.

1. In the left sidebar, click EIP to enter the elastic public IP management page.
2. In the operation column of the EIP that needs to be bind to an instance, select More > Bind.



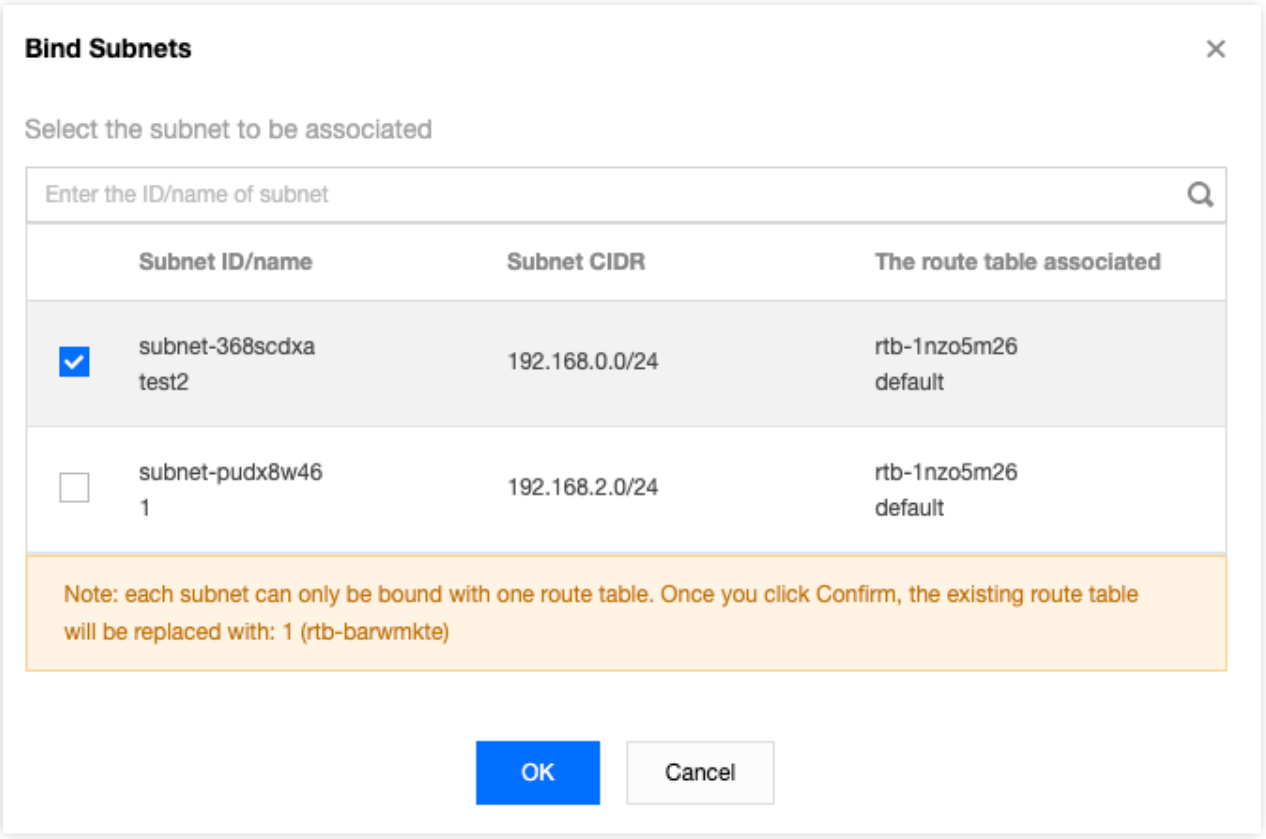
3. In the "Bind Resource" pop-up box, select a CVM instance chosen as the public gateway to bind.



Step 2: configure the subnet route table where the gateway resides

The gateway subnet and the regular subnet cannot share the same route table. You need to create a new, separate gateway route table and associate the gateway subnet with this route table.

1. Create a custom route table.
2. After creation, you will be prompted to associate the subnet. Directly associate the subnet where the public gateway server is located.

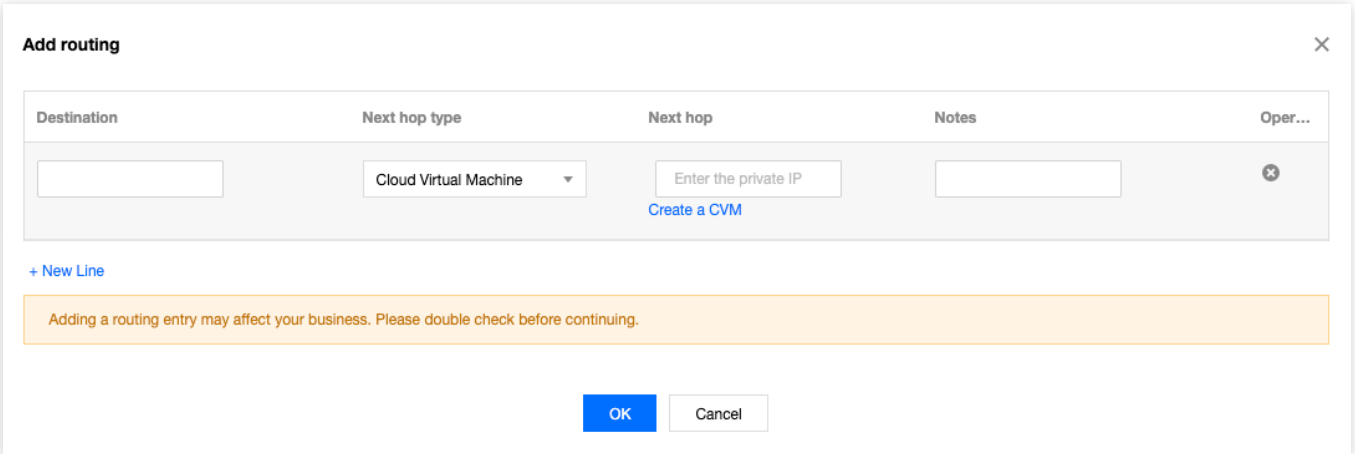


Step 3: configure the route table for the regular subnet

Configure the route table for the regular subnet to route default traffic through the public gateway cloud server, allowing cloud servers in the regular subnet to access the Internet via the routing and forwarding capability of the public gateway.

In the route table of the subnet where the regular cloud server is located, add the following routing policy:

- Destination: the public address you want to access.
- Next hop type: CVM.
- Next hop: the private network IP of the cloud server instance with the EIP bind in step 1.
  For detailed operations, please refer to Configure Route Policy.



Step 4: configure the public gateway

1. Log in to the public gateway cloud server, enable network forwarding, NAT proxy functionality, and related parameter optimizations.
2. Execute the following command to create a script named vpcGateway.sh in the /usr/local/sbin directory.

```
vim /usr/local/sbin/vpcGateway.sh
```

3. Press "i" to switch to edit mode and write the following code into the script.

```
# !/bin/bash
echo "------------------------------------------------"
echo " `date`"
echo "(1)ip_forward config....."
file="/etc/sysctl.conf"
grep -i "^net\.ipv4\.ip_forward.*" $file &>/dev/null && sed -i \
's/net\.ipv4\.ip_forward.*/net\.ipv4\.ip_forward = 1/' $file || \
echo "net.ipv4.ip_forward = 1" >> $file
echo 1 >/proc/sys/net/ipv4/ip_forward
[ `cat /proc/sys/net/ipv4/ip_forward` -eq 1 ] && echo "-->ip_forward:Success" || \
echo "-->ip_forward:Fail"
echo "(2)Iptables set....."
iptables -t nat -A POSTROUTING -j MASQUERADE && echo "-->nat:Success" || echo "-->nat:Fail"
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options timestamp && \
echo "-->mangle:Success" || echo "-->mangle:Fail"
echo "(3)nf_conntrack config....."
echo 262144 > /sys/module/nf_conntrack/parameters/hashsize
[ `cat /sys/module/nf_conntrack/parameters/hashsize` -eq 262144 ] && \
echo "-->hashsize:Success" || echo "-->hashsize:Fail"
echo 1048576 > /proc/sys/net/netfilter/nf_conntrack_max
[ `cat /proc/sys/net/netfilter/nf_conntrack_max` -eq 1048576 ] && \
echo "-->nf_conntrack_max:Success" || echo "-->nf_conntrack_max:Fail"
echo 10800 >/proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established \
[ `cat /proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established` -eq 10800 ] \
&& echo "-->nf_conntrack_tcp_timeout_established:Success" || \
echo "-->nf_conntrack_tcp_timeout_established:Fail"
```

4. Press "Esc", enter ":wq" to save the file and return.
5. Execute the following command to set the script file permissions.

```
chmod +x /usr/local/sbin/vpcGateway.sh
echo "/usr/local/sbin/vpcGateway.sh >/tmp/vpcGateway.log 2>&1" >> /etc/rc.local
```

6. Set the rps for the public gateway:

7. Execute the following command to create a script named set_rps.sh in the /usr/local/sbin directory.

vim /usr/local/sbin/set_rps.sh

8. Press "i" to switch to edit mode and write the following code into the script.

```
# !/bin/bash
echo "--------------------------------------------"
date
mask=0
i=0
total_nic_queues=0
get_all_mask() {
local cpu_nums=$1
if [ $cpu_nums -gt 32 ]; then
mask_tail=""
mask_low32="ffffffff"
idx=$((cpu_nums / 32))
cpu_reset=$((cpu_nums - idx * 32))
if [ $cpu_reset -eq 0 ]; then
mask=$mask_low32
for ((i = 2; i <= idx; i++)); do
mask="$mask,$mask_low32"
done
else
for ((i = 1; i <= idx; i++)); do
mask_tail="$mask_tail,$mask_low32"
done
mask_head_num=$((2 ** cpu_reset - 1))
mask=$(printf "%x%s" $mask_head_num $mask_tail)
fi
else
mask_num=$((2 ** cpu_nums - 1))
mask=$(printf "%x" $mask_num)
fi
echo $mask
}
set_rps() {
if ! command -v ethtool &>/dev/null; then
source /etc/profile
fi
ethtool=$(which ethtool)
cpu_nums=$(cat /proc/cpuinfo | grep processor | wc -l)
if [ $cpu_nums -eq 0 ]; then
exit 0
```

```
fi
mask=$(get_all_mask $cpu_nums)
echo "cpu number:$cpu_nums mask:0x$mask"
ethSet=$(ls -d /sys/class/net/eth*)
for entry in $ethSet; do
eth=$(basename $entry)
nic_queues=$(ls -l /sys/class/net/$eth/queues/ | grep rx- | wc -l)
if (($nic_queues == 0)); then
continue
fi
cat /proc/interrupts | grep "LiquidIO.*rxtx" &>/dev/null
if [ $? -ne 0 ]; then # not smartnic
#multi queue don't set rps
max_combined=$(
$ethtool -l $eth 2>/dev/null | grep -i "combined" | head -n 1 | awk '{print $2}'
)
#if ethtool -l $eth goes wrong.
[[ ! "$max_combined" =~ ^[0-9]+$ ]] && max_combined=1
if [ ${max_combined} -ge ${cpu_nums} ]; then
echo "$eth has equally nic queue as cpu, don't set rps for it..."
continue
fi
else
echo "$eth is smartnic, set rps for it..."
fi
echo "eth:$eth queues:$nic_queues"
total_nic_queues=$(($total_nic_queues + $nic_queues))
i=0
while (($i < $nic_queues)); do
echo $mask >/sys/class/net/$eth/queues/rx-$i/rps_cpus
echo 4096 >/sys/class/net/$eth/queues/rx-$i/rps_flow_cnt
i=$(($i + 1))
done
done
flow_entries=$((total_nic_queues * 4096))
echo "total_nic_queues:$total_nic_queues flow_entries:$flow_entries"
echo $flow_entries >/proc/sys/net/core/rps_sock_flow_entries
}
set_rps
```

9. Press "Esc", enter ":wq" to save the file and return.

10. Execute the following command to set the script file permissions.

```
chmod +x /usr/local/sbin/set_rps.sh
echo "/usr/local/sbin/set_rps.sh >/tmp/setRps.log 2>&1" >> /etc/rc.local
chmod +x /etc/rc.d/rc.local
```

11. After completing the above configuration, restart the public gateway cloud server to make the configuration effective. Then, test whether the cloud servers without public IPs can successfully access the Internet.

Adjust the Priority of NAT Gateway and EIP

When a subnet is associated with a NAT gateway, and the CVM in the subnet has a public network IP address (or an EIP), the CVM accesses the Internet through the NAT gateway by default because the priority of the exact match route is higher than that of the public network IP. However, you can set a routing policy to allow the CVM to access the Internet through its public network IP.

Directions

1. Ensure that a routing policy that points to the NAT gateway exists so that CVMs in the subnet that have no public network IP can still access the Internet through the NAT gateway. Cloud servers within the subnets associated with this route table that do not have public IP addresses can still access the Internet via the NAT Gateway and will not be affected.
2. Add a new routing policy with the Next Hop Type as Public Network IP of Cloud Virtual Machine and enter the Destination.
    - Destination: Enter the specific public network IP range or default route to be accessed by the service (0.0.0.0/1306182224162611120, where default route indicates that if the destination is not in the routing table, all data packets will use this default route).
    - Next hop type: public IP of the cloud server.

    > Note:
    >
    > - This routing policy, when configured with routing rules that have the same destination as the original ones pointing to the NAT Gateway or CVM, will always match this route preferentially.
    > - This routing policy will affect all subnets associated with this route table (please confirm the impact of this operation). Specifically, cloud servers within these subnets that have public IP addresses (or elastic IPs) will access the Internet via their public IPs instead of through the NAT Gateway.
    > - Cloud servers within the subnets associated with this route table that do not have public IP addresses can still access the Internet via the NAT Gateway and will not be affected.

Building High Availability Primary/ Secondary Cluster with HAVIP+Keepalived

This document will introduce how to build a high availability primary/secondary cluster with keepalived software + high availability virtual IP (HAVIP) in VPC.

Basic Principles

Typically, a high availability primary/secondary cluster consists of 2 servers: an active primary server and a standby secondary server. The two servers share the same VIP (Virtual IP). The VIP can only work on one primary server at the same time. When the primary device fails, the secondary server will take over the VIP to continue providing services. The high-availability primary/secondary model is widely applied, such as MySQL primary/replica switch and Nginx Web connect.

In VPC, high availability primary/secondary clusters can be implemented by deploying Keepalived on Cloud Virtual Machines. Keepalived is a VRRP protocol high availability software. To use Keepalived, first complete its configuration in the Keepalived.conf file.

- In traditional physical networks, Keepalived's VRRP protocol can be used to negotiate the primary/ secondary status. The principle is that the primary device periodically sends free ARP packets to refresh the MAC table of the up-link switch or terminal ARP table, triggering the migration of the VIP to the primary device.
- In VPC, keepalived can be deployed to build primary/secondary high availability clusters. Compared to physical networks, the main difference is:
    - The VIP used must be a High Availability Virtual IP (HAVIP) applied from the cloud platform.
    - The VIP has a subnet attribute and can only be bound between machines in the same subnet.

Notes

- It is recommended to use unicast method for VRRP communication.
- It is recommended to use Keepalived (1.2.24 version and above).
- Ensure the following garp-related parameters are configured. Because Keepalived relies on ARP packets to update IP information, missing these parameters may lead to scenarios where the primary device does not send ARP, causing communication anomalies.

```
garp_master_delay 1
garp_master_refresh 5
```

- Ensure each primary/secondary cluster within the same VPC needs to be configured with different vrrp router id.
- Ensure the "vrrp_strict" configuration is removed, that is, not using the strict mode.
- Control the number of VIPs configured on a single network interface. It is suggested that the number of Highly Available Virtual IPs bound to a single network interface not exceed five. If multiple virtual IPs are needed, it is recommended to add or modify the configuration vrrp_garp_master_repeat 1 in the global_defs section of the Keepalived configuration file.
- By adjusting the size of the adver_int parameter, balance the resistance to network jitter and disaster recovery speed. If the advert_int parameter is too small, it may be prone to frequent failovers and temporary dual-master (split brain) until the network recovers. If the advert_int parameter is too large, it could lead to slow failover (i.e., longer service downtime) when the host fails. Assess the impact of dual-master (split brain) on your business thoroughly.
- The interval parameter in the specific execution items (such as checkhaproxy) of the track_script script shall be appropriately increased to avoid script execution timeout causing a FAULT state.
- Optional: Be aware of the increase in disk usage caused by log printing, which can be resolved by tools such as logrotate.

Directions

> Note:
>
> The directions in this document are based on the following environmental conditions. When performing the operations, be sure to replace them with actual environmental parameters.
>
> - Primary Node Cloud Virtual Machine: HAVIP-01, 172.16.16.5
> - Replica Node Cloud Virtual Machine: HAVIP-02, 172.16.16.6
> - High Availability HAVIP: 172.16.16.12
> - EIP: 81.71.14.118
> - Image Version: CentOS 7.6 64-bit

Step 1: Applying for a VIP

1. Log in to the Virtual Private Cloud console.
2. In the left sidebar, select IP & Network Interface > High Availability Virtual IP.
3. On the HAVIP Management page, click Apply.
4. In the Apply for High Availability Virtual IP pop-up dialog box, enter the name, and select the Virtual Private Cloud and subnet where the HAVIP resides, and click OK.

> Note:
>
> The IP address of the HAVIP can be assigned automatically or can be filled in manually. If you choose to fill in manually, make sure that the private IP you fill in is within the subnet IP range and is not a system reserved IP. For example, if the subnet IP range is: 10.0.0.0/24, then the available private network IP range is: 10.0.0.2 - 10.0.0.254.

Step 2: Install keepalived software on the primary and secondary servers (version 1.2.24 and above is recommended)

This document provides the method for installing keepalived based on CentOS 7.6 image-type servers.

1. Check whether the keepalived software package version number meets requirements.

   ```
   yum list keepalived
   ```

- Yes = Execute 2
- No = Execute 3

2. Use yum to install the software package.

   ```
   yum install -y keepalived
   ```

3. Install the software package from the source code.

   ```
   tar zxvf keepalived-1.2.24.tar.gz
   cd keepalived-1.2.24
   ./configure --prefix=/
   make; make install
   chmod +x /etc/init.d/keepalived   // To prevent the error: env: /etc/init.d/keepalived: Permission denied
   ```

Step 3: Configure keepalived and bind the high-availability VIP to the primary/secondary Cloud Virtual Machine

1. Log in to the primary node Cloud Virtual Machine HAVIP-01, execute vim /etc/keepalived/

keepalived.conf , and modify the relevant configurations.

Note: In this example, HAVIP-01 and HAVIP-02 will be configured as "equal weight nodes", that is, both are set to BACKUP, with a priority of 100. The advantage is that it can reduce the number of failovers caused by jitter.

```
! Configuration File for keepalived
global_defs {
   notification_email {
     acassen@firewall.loc
     failover@firewall.loc
     sysadmin@firewall.loc
   }
   notification_email_from Alexandre.Cassen@firewall.loc
   smtp_server 192.168.200.1
   smtp_connect_timeout 30
   router_id LVS_DEVEL
   vrrp_skip_check_adv_addr
   vrrp_garp_interval 0
   vrrp_gna_interval 0
}
vrrp_script checkhaproxy
{
    script "/etc/keepalived/do_sth.sh" # Check if the business process is running properly. The "do_sth.
sh" file is a user-defined service process detection script, execute according to business needs, and rep
lace "do_sth.sh" with the actual script name when executing.
    interval 5
}
vrrp_instance VI_1 {
# Be aware of the primary-secondary parameter selection
state BACKUP             # Set the initial state to "Backup"
    interface eth0         # Set the network interface card bound to the VIP, for example, eth0.
    virtual_router_id 51    # Configure the virtual_router_id value for the cluster.
    nopreempt              # Enable non-preemptive mode.
    # preempt_delay 10      # valid when it is state MASTER
    priority 100           # Two devices are equal weight nodes of the same value
    advert_int 5
    authentication {
       auth_type PASS
       auth_pass 1111
    }
    unicast_src_ip 172.16.16.5  # Set the local private IP address.
    unicast_peer {
       172.16.16.6            # IP address of the peer device.
    }
    virtual_ipaddress {
```

```
        172.16.16.12          # Set the high availability virtual IP address.
    }
    notify_master "/etc/keepalived/notify_action.sh MASTER"
    notify_backup "/etc/keepalived/notify_action.sh BACKUP"
    notify_fault "/etc/keepalived/notify_action.sh FAULT"
    notify_stop "/etc/keepalived/notify_action.sh STOP"
    garp_master_delay 1    # Set the delay for updating the ARP cache after switching to the primary st
ate.
    garp_master_refresh 5   # Set the interval for the primary node to send the ARP message.

    track_interface {
            eth0              # Use the network interface card bound to the VIP, for example, eth0.
      }
    track_script {
      checkhaproxy
    }
}
```

2. Press esc to exit the edit mode and enter :wq.< to save and exit.

3. Log in to the replica node Cloud Virtual Machine HAVIP-02, execute vim /etc/keepalived/keepalived.conf , and modify the relevant configurations.

```
    ! Configuration File for keepalived
    global_defs {
      notification_email {
        acassen@firewall.loc
        failover@firewall.loc
        sysadmin@firewall.loc
      }
      notification_email_from Alexandre.Cassen@firewall.loc
      smtp_server 192.168.200.1
      smtp_connect_timeout 30
      router_id LVS_DEVEL
      vrrp_skip_check_adv_addr
      vrrp_garp_interval 0
      vrrp_gna_interval 0
    }
    vrrp_script checkhaproxy
    {
        script "/etc/keepalived/do_sth.sh"
        interval 5
    }
    vrrp_instance VI_1 {
    # Be aware of the primary-secondary parameter selection
```

```
state BACKUP            # Set the initial states to "Standby"
    interface eth0          # Set the network interface card bound to the VIP, for example, eth0.
    virtual_router_id 51    # Configure the virtual_router_id value for the cluster.
    nopreempt               # Enable non-preemptive mode.
    # preempt_delay 10      # valid when it is state MASTER
    priority 100            # Two devices are equal weight nodes of the same value
    advert_int 5
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.16.16.6  # Set the local private IP address.
    unicast_peer {
        172.16.16.5             # IP address of the peer device.
    }
    virtual_ipaddress {
        172.16.16.12            # Set the high availability virtual IP address.
    }
    notify_master "/etc/keepalived/notify_action.sh MASTER"
    notify_backup "/etc/keepalived/notify_action.sh BACKUP"
    notify_fault "/etc/keepalived/notify_action.sh FAULT"
    notify_stop "/etc/keepalived/notify_action.sh STOP"
    garp_master_delay 1    # Set the delay for updating the ARP cache after switching to the prima
ry state.
    garp_master_refresh 5   # Set the interval for the primary node to send the ARP message.
    track_interface {
            eth0              # Use the network interface card bound to the VIP, for example, eth0.
        }
    track_script {
      checkhaproxy
    }
}
```

4. Press esc to exit the edit mode and enter :wq.< to save and exit.

5. Restart the keepalived process to apply the configurations.

```
systemctl start keepalived
```

6. Check the primary/secondary status of the two CVMs and confirm that the HAVIP is correctly bound to the primary and secondary servers.

> Note:

> In this example, HAVIP-01 initiates the keepalived service first, so under normal circumstances, HAVIP-01 will be selected as the primary node. You can log in to the Highly Available Virtual IP Console to view the Cloud Virtual Machine bound to HAVIP as the primary node cloud HAVIP-01.

Step 4: Bind the EIP (optional)

1. In the HAVIP console, click Bind for the HAVIP.
2. In the Bind EIP dialog box, select the EIP to be bound and click OK. If no EIP is available, apply for one in the EIP console first.

Step 5: use notify_action.sh for simple log recording (optional)

The main logs of keepalived are still recorded in "/var/log/message", and you can add a script for simple log recording via notify.

1. Log in to the Cloud Virtual Machine and execute `vim /etc/keepalived/notify_action.sh` command to add the "notify_action.sh" script, which is as follows:

```
#!/bin/bash
#/etc/keepalived/notify_action.sh
log_file=/var/log/keepalived.log
log_write()
{
   echo "[`date '+%Y-%m-%d %T'`] $1" >> $log_file
}
[ ! -d /var/keepalived/ ] && mkdir -p /var/keepalived/

case "$1" in
   "MASTER" )
      echo -n "$1" > /var/keepalived/state
      log_write " notify_master"
      echo -n "0" /var/keepalived/vip_check_failed_count
      ;;
   "BACKUP" )
      echo -n "$1" > /var/keepalived/state
      log_write " notify_backup"
      ;;
   "FAULT" )
      echo -n "$1" > /var/keepalived/state
      log_write " notify_fault"
      ;;
   "STOP" )
      echo -n "$1" > /var/keepalived/state
      log_write " notify_stop"
      ;;
```

```
    *)
        log_write "notify_action.sh: STATE ERROR!!!"
        ;;
esac
```

2. Execute chmod a+x /etc/keepalived/notify_action.sh to modify the script permissions.

Step 6: Verify whether the VIP and public network IP are switched normally during primary/secondary switchover

Simulate the host failure by restarting the keepalived process, rebooting sub-machines and other methods to check whether VIP can migrate normally.

- If the primary/replica switch is completed, you can see that the host bound in the console has been switched to the backup Cloud Virtual Machine.
- Additionally, you can ping the VIP from within the VPC to observe the time interval from network interruption to recovery; each switch causes approximately 4 seconds of ping interruption. Pinging the EIP bound to HAVIP from the public network side also shows about 4 seconds of ping interruption per switch.
- Use ip addr show to check whether havip appears on the primary device network interface card.

Building High Availability DB with HAVIP+Windows Server Failover Cluster

1. Creating a HAVIP
   log in to HAVIP Console , and create a HAVIP. For detailed methods, please refer to Creating Highly Available Virtual IP.
2. Binding and Configuration
   The configuration is the same as that in the traditional mode. The backend server declares and negotiates which device will be bound with the created HAVIP. You simply need to specify the virtual IP address in the configuration file as HAVIP.
   In the cluster manager, add the HAVIP that was just created.
3. Verification
   After the configuration is completed, directly switch nodes for testing.
   Under normal circumstances, the network will be restored after only a brief interruption (which may be imperceptible if the failover is fast), and business operations remain unaffected.

Cross-account VPC service sharing via Private Link

This document describes how to quickly create a Private Link service and share the cloud services deployed in your VPC with VPCs of other accounts.

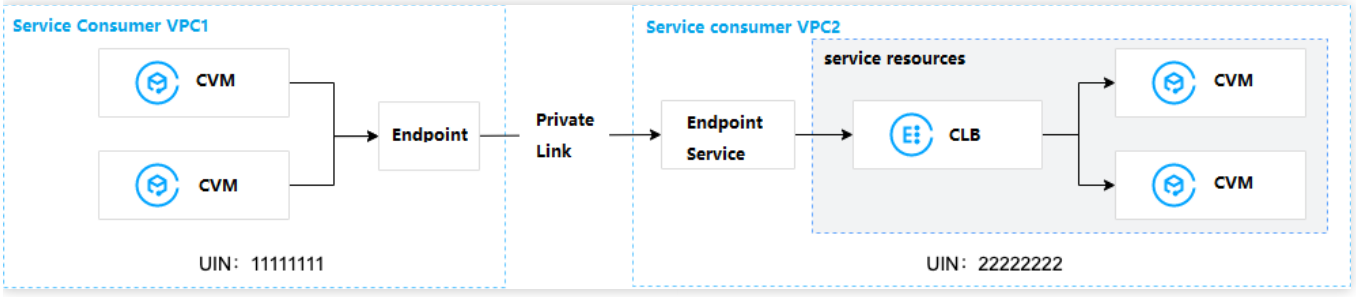
Background

You can use the Private Link service to establish a secure and stable access connection between VPCs, simplifying the network architecture and avoiding potential security risks associated with public internet access. With Private Link, you can establish secure and stable private connections between VPCs and cloud services, simplifying network architecture and avoiding potential security risks associated with accessing services via the public network.

To establish a connection using Private Link, you need to create both an endpoint service and an endpoint. Before creating the endpoint service, you need to create a private network Layer 4 CLB instance and create a listener associated with the Cloud Virtual Machine instance that has the deployed service. Then, when creating the endpoint service, associate it with the CLB instance. At this point, the endpoint service will serve as the business access entry for the service provider, available for the service user's created endpoint to request a connection. Once the connection is successfully established, the service user can access the service provider's deployed services.

Scenario Example

In this example business scenario, assume the business is deployed in VPC2. Now, the business needs to be shared for access by another account's VPC. To avoid potential security risks from public network access, use Private Link to achieve a secure intranet access solution from VPC1 to VPC2.



Prerequisites

- The service user shall inform the service provider of the UIN account. After the service user initiates a connection request, it can be connected only after the service provider accepts the request.
- In the service provider's VPC2, a private network Layer 4 CLB instance has already been created, and related service resources are deployed in the backend Cloud Virtual Machine instance. Ensure that the backend Cloud Virtual Machine instance can properly process requests forwarded by Cloud Load Balancer.
- The service provider shall inform the service user of VPORT for Cloud Load Balancer in advance.

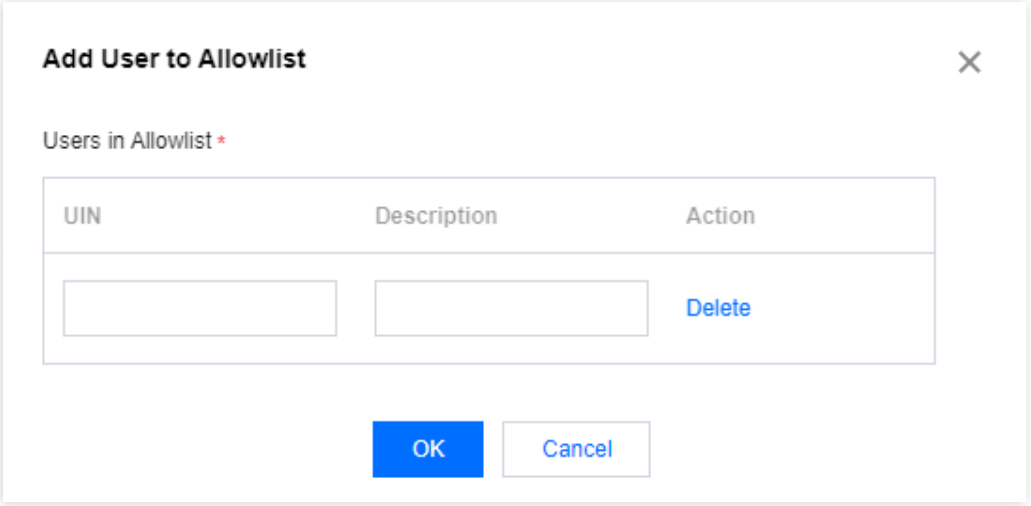
Directions

Step 1: The service provider creates an endpoint service

1. log in to the Endpoint Service Console.
2. Click Create.
3. In the pop-up Create Endpoint Service interface, configure the relevant parameters. Parameter description:
    - Service name: custom the name of endpoint service.
    - Region: The region of the endpoint service node.
    - Network: Select the associated VPC.
    - CLB: Select the CLB created under the VPC.
    - Auto Accept: Specifies whether the endpoint service automatically accepts connection requests initiated by the endpoint, with the default set to No. This document will maintain the default.
    - If it is the same account, then Auto Accept is available.
    - If it is a cross-account, when select Auto Accept and the endpoint is in the user allowlist, then the endpoint is available upon successful creation.
    - If it is cross-account and Auto Accept is not selected, the initial status of the successfully created endpoint is Pending Acceptance, and it needs to be accepted by the server-side to become available.
4. After completing the parameter settings, click OK to complete the creation of the endpoint service.

Step 2: add service consumer account allowlist

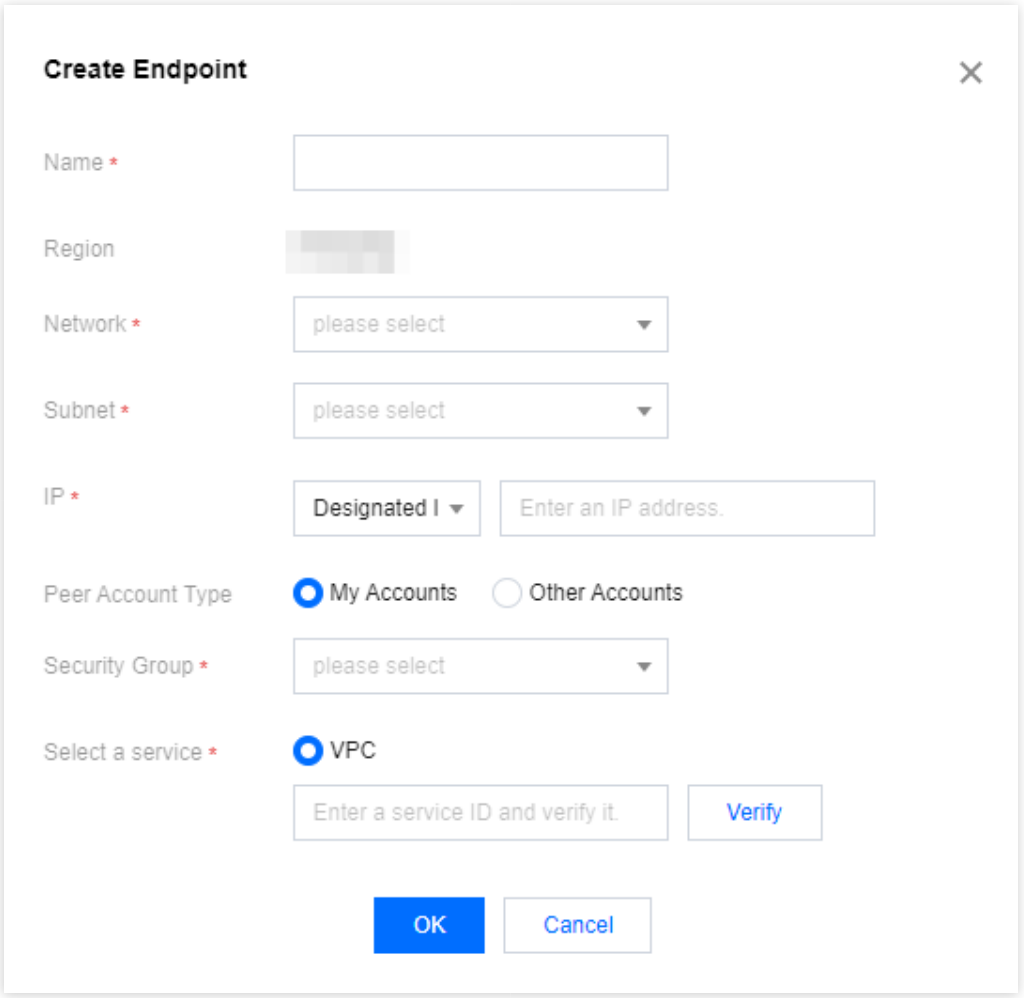
1. Click the ID of the created endpoint service to enter its details page.
2. click Allowlist tab to enter the User Allowlist Management interface.
3. Click [Add] to enter the [Add Allowlist Users] interface.



4. Enter the user UIN and user description. If multiple users need to be added, click Add.
5. After completing the user allowlist addition, click OK. The successfully added allowlist will be displayed in the list.

Step 3: The service user creates an endpoint

1. Log in to the Endpoint Console.
2. Click [Create] to enter the [Create Terminal Endpoint] interface.



Configure parameters of the endpoint.

- Name: custom the name of the endpoint.
- Region: The region where the endpoint is located.
- Network: Select the VPC where the endpoint is located.
- Subnet: Select the subnet where the endpoint is located.
- IP address: the IP address of the endpoint. You can specify an IP address, which should be a private IP address within the VPC, or opt for automatic IP assignment.
- Peer account type: Select the owning account of the VPC that needs access. My Account indicates access within the same account VPC, while Other Accounts signifies cross-account VPC access. For cross-account access, it is necessary to inform the peer account of your account number, and after initiating a connection request, server-side acceptance is required for connectivity.
- Select service: Enter the ID of the endpoint service and click Verify. Only services that have passed verification can be connected.

3. After the parameter settings are completed, click OK.

Step 4: (optional) bind security groups

Bind a security group to the endpoint to control the inbound traffic, and improve the security of business access.

1. Log in to the Security Group Console, create a security group and set its rules.
2. In the Security Group tab interface of the Endpoint Details page, you can bind a security group to the endpoint.

Step 5: manage endpoint connection requests

For cross-account, the service provider needs to accept the connection requests initiated by the user to establish a connection.

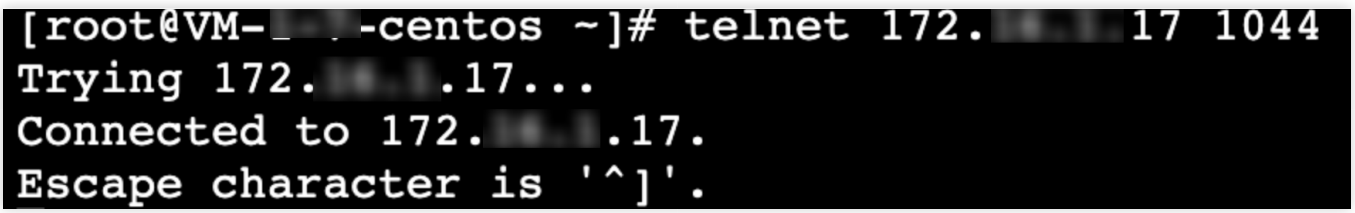
1. Click the ID of the created endpoint service to enter its details page.
2. Click the Endpoint Connection tab to enter the Endpoint Connection Management interface.
3. Handle the connection request status of the endpoint according to the actual situation. In this example, Acceptance is selected.
   Endpoint connections have three statuses: pending acceptance, available, and denied.

- For connections in the Denied state, you can perform the Acceptance operation. After execution, the status becomes Available.
- For connections in the Available state, you can perform the Deny operation. After execution, the status becomes Denied.
- For connection requests in the Pending Acceptance state, you can perform Acceptance or Deny, and after execution, the status becomes Available or Denied, respectively.

Note: The endpoint service can be connected by multiple endpoint. The status of the endpoint service refers to the status of each connection, not the status of the endpoint service alone.

Step 6: The service user initiates an access request for connection verification

1. Log in to a CVM under service user VPC1 and access the service provider's backend service through VIP+VPORT.
2. In this example, use telnet to verify connectivity by executing telnet VIP VPORT.
   Note: If the server does not have telnet installed, please install telnet first by executing yum install telnet.
   If the following information appears, it indicates a connection:



Multicast Communication Scenarios for Dedicated Tunnels

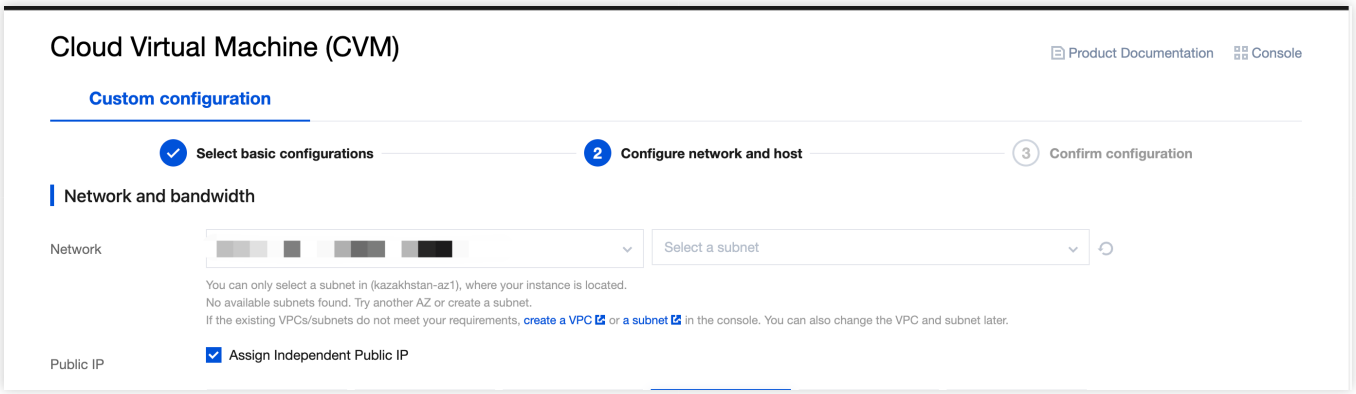
Scenarios

In a hybrid cloud networking scenario, you may need to establish connectivity between the multicast services in your on-premises IDC and the CVMs within a VPC of the cloud platform, enabling multicast mutual communication between the IDC and the cloud-based CVMs.
This section describes how to establish a multicast communication link between a VPC and an on-premises IDC using a standard DCGW and a dedicated tunnel, and provides an end-to-end connectivity verification method.

Operation Steps

Step 1: Creating a CVM Instance and Preparing Routes in the Target VPC

1. Log in to the CVM console.
2. Click Create to create a CVM instance, and select the target VPC and subnet in the Network and Bandwidth step.



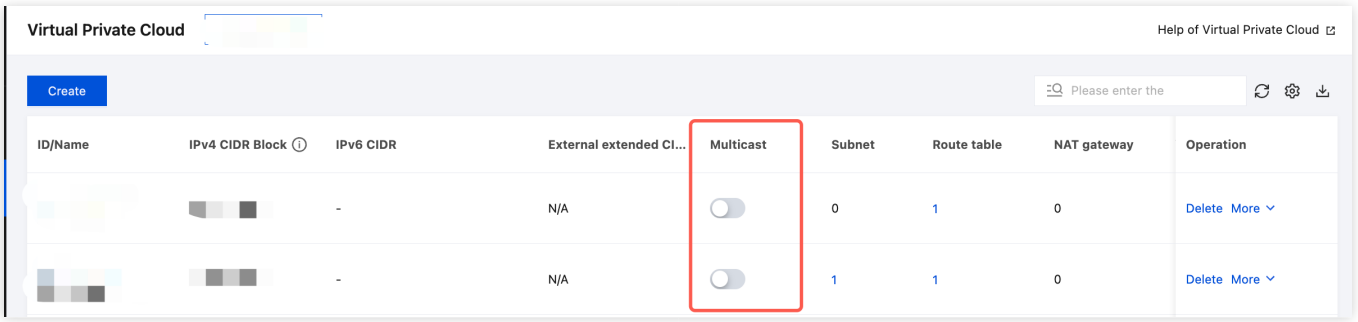
3. Log in to the VPC console.
4. Create a dedicated tunnel for a standard DCGW in the target VPC and fill in the User IDC IP Range parameter based on your actual situation.
5. After the dedicated tunnel is ready, modify the route table associated with the subnet where the CVM instance resides and add a route:

- Destination IP address: IP address of the IDC IP range for the dedicated tunnel.
- Next-hop type: standard DCGW.

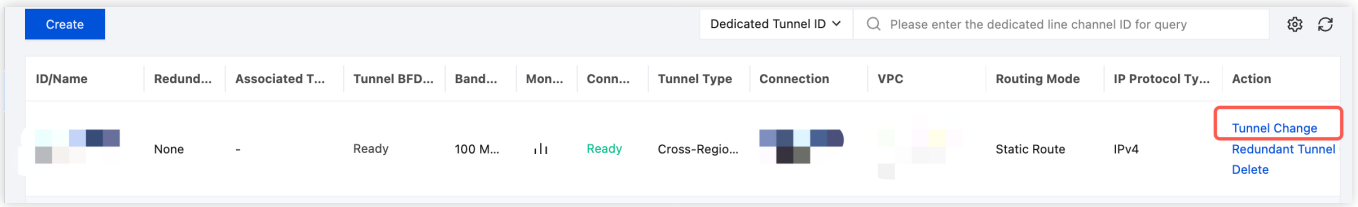
6. Verify that a route has been configured on the IDC switch, using an address in the VPC IP range as the destination IP address and the cloud boundary IP address as the next hop.

Step 2: Enabling Multicast for the Dedicated Tunnel

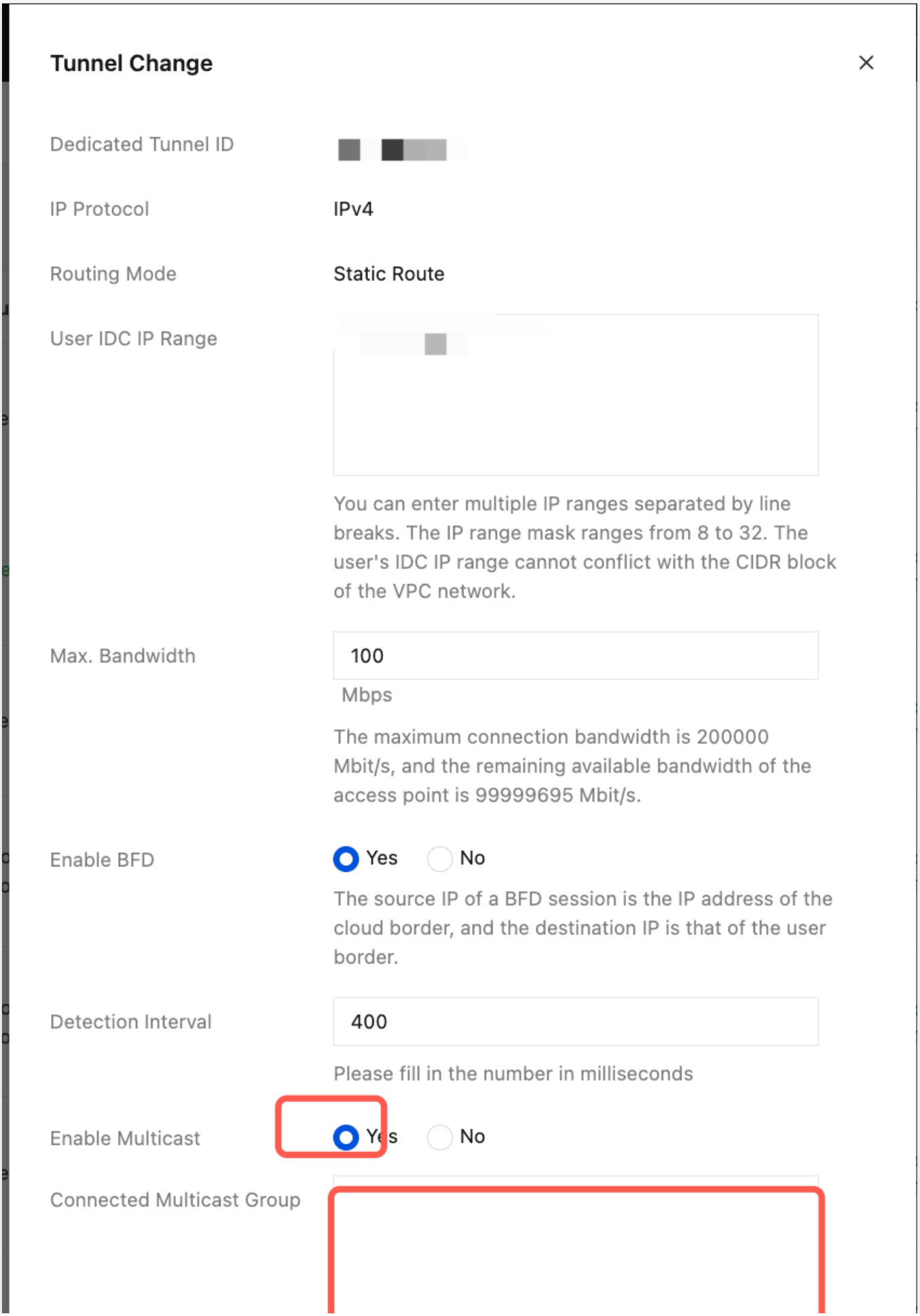
1. Log in to the VPC console and enable Multicast for the target VPC.

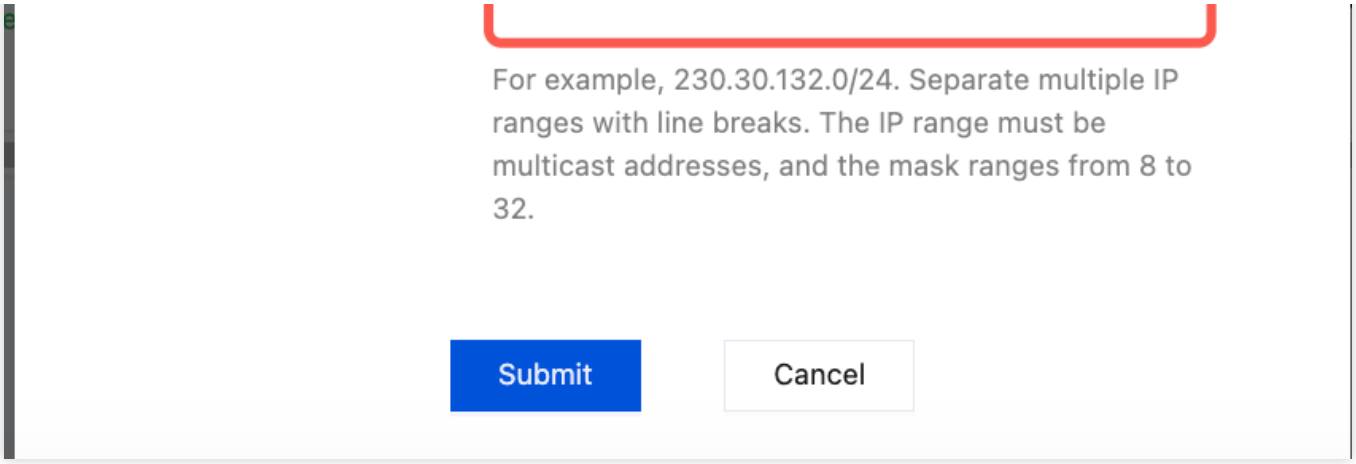


2. Log in to the Direct Connect console. On the dedicated tunnel page, click Tunnel Change in the Operation column on the right side of the tunnel whose parameters need to be changed.



3. On the Tunnel Change page, follow the on-screen prompt to Enable Multicast. Click Yes, specify the Connected Multicast Group parameter, and then click Submit to enable multicast for the dedicated tunnel.


Tunnel Change
Dedicated Tunnel ID
IP Protocol
IPv4
Routing Mode
Static Route
User IDC IP Range
You can enter multiple IP ranges separated by line breaks. The IP range mask ranges from 8 to 32. The user's IDC IP range cannot conflict with the CIDR block of the VPC network.
Max. Bandwidth
100
Mbps
The maximum connection bandwidth is 200000 Mbit/s, and the remaining available bandwidth of the access point is 99999695 Mbit/s.
Enable BFD
Yes
No
The source IP of a BFD session is the IP address of the cloud border, and the destination IP is that of the user border.
Detection Interval
400
Please fill in the number in milliseconds
Enable Multicast
Yes
No
Connected Multicast Group



Step 3: Configuring the PIM Protocol on the IDC Switch

Complete the corresponding multicast configuration on the IDC switch to ensure that the PIM neighbor relationship can be established properly.

> Note:
>
> The pimd tool can be installed on the IDC server to assist in multicast routing management.
>
> Download URL for binary pimd: https://drive.weixin.qq.com/s?k=AJEAIQdfAAoT4m0OKr.
>
> Compilation dependencies: GCC and Make. Install them using yum commands if they are not installed.
>
> Run the following compilation and installation commands after decompression:
>
> ./configure --enable-scoped-acls && make
>
> make install
>
> After compilation and installation, the /etc/pimd.conf file is automatically created. You can then start the pimd tool by executing ./pimd.

Step 4: Installing the iperf Testing Tool on the CVM Instance and IDC Server

1. Log in to the CVM instance and the IDC server separately and run the yum install -y iperf command to download and install the traffic testing tool iperf.

   > Note:
   >
   > For Ubuntu systems, run the apt install -y iperf command to install iperf.

Step 5: Verifying Multicast Connectivity

1. Run the following command to add the CVM instance to the multicast group: iperf -s -u -B 230.24.0.211 -i1.

   > Note:
   >
   > If multiple IP addresses are available on the CVM instance, use the -B parameter to bind communication IP addresses, for example: iperf -s -u -B 230.24.0.211 -i1 -B10.0.0.16.

2. Run the following command on the IDC server to send multicast messages to the multicast group: iperf -c 230.24.0.211 -t 500 -u -T64 -l 1000 -b 2000pps.

> Note:
>
> If multiple IP addresses are available on the IDC server, use the -B parameter to bind communication IP addresses (the IP addresses configured in User IDC IP Range for the tunnel), for example, iperf -c 230.24.0.211 -t 500 -u -T64 -l 1000 -b 2000pps -B 192.10.88.100.

3. The multicast communication is successful. The CVM instance can receive multicast messages, and no packet loss occurs after the traffic stabilizes.

FAQs
General
IP range and IP related

What are the restrictions on the IP range of VPC and subnet?

Converge Cloud VPC CIDR supports the use of any of the following private IP ranges:

- 10.0.0.0 - 10.255.255.255 (mask range between 16 - 28)
- 172.16.0.0 - 172.31.255.255 (mask range between 16 - 28)
- 192.168.0.0 - 192.168.255.255 (mask range between 16 - 28)
  The CIDR of a subnet must be within or the same as the CIDR of the VPC.

Can the IP ranges of VPC and subnet be modified?

- When creating a VPC and subnet, you need to specify their CIDR, which cannot be changed once created.
- If you cannot establish a peering connection due to overlapping private IP ranges, we recommend migrating instances within the VPC. For VPC migration, please refer to the Switching Private Network Services section in the Cloud Server documentation.

Can the private network of resources (CVMs, databases, etc.) within a VPC be modified?

- The main private network IP of the primary network card of a cloud server can be modified, but the main private network of auxiliary network cards cannot be modified.
- Private network load Balancer (CLB) / Cloud Databases do not support modifying private network IPs.

Can cloud servers or databases within a VPC be switched to other VPCs?

- Currently, server migration is supported, but database and other resource migration are not yet supported.
- Cloud servers can be migrated from the current VPC to another VPC under the same account. For directions and precautions, please refer to the "Switching Private Network Services" section in the Cloud Server documentation.

What is the purpose of EIP?

EIP is suitable for the following scenarios:

1. Disaster recovery
   We strongly recommend using EIPs for disaster recovery purposes. When one of your servers fails to

provide services, you can unbind the EIP from that machine and rebind it to a healthy machine, helping you to quickly restore services.

2. Reserved specific public IP
   When you need to reserve a specific public IP in your account, you can convert it to an EIP. After binding it to a device, you can use this IP for public network access. As long as you do not perform the release operation, the EIP will remain in your account.
3. Other special scenarios
   When you have other special situations that require IP replacement, you can convert a regular public IP to an EIP and achieve the replacement by binding/unbinding the EIP. However, EIP resources are valuable, and there are quota limits per region for each account. We recommend that you plan and use them reasonably.

How to keep the public IP unchanged?

When you need to reserve a specific public IP in your account, you can convert it to an EIP. After binding it to a device, you can use this IP for public network access. As long as you do not perform the release operation, the EIP will remain in your account.

Can EIP be converted back to a regular public IP?

EIP cannot be converted back to a regular public IP.

Product Quotas Related

Are there any quotas for VPCs? How many VPCs can be created per account?

Some resources in VPCs have usage quota limits. By default, each account can create 5 private networks per region.

EIP application failed? How many EIPs can be applied for per account?

- The number of EIPs that can be applied for per cloud platform account in each region is 20.
- Each cloud platform account can make purchases up to the quota number times 2 per day (defaulting to 40 times). When unbinding an EIP, each account can reassign public IPs for free up to 10 times per day.

Connection Categories
Connecting to the Public Network

How to apply for a public IP if a cloud server is not assigned a public IP when purchased?

If you did not allocate a public network when purchasing a cloud server, you cannot apply for a regular public IP for that cloud server. However, you can achieve the same functionality through an EIP.

- An EIP is a type of public IP address that remains fixed within a region. Unlike regular public IPs, it is bind to your account, meaning you can bind and unbind an EIP to different cloud servers as needed (one binding at a time).
- Due to the special nature of EIPs, if you have applied for an EIP but have not bind it to an instance, you will incur idle fees. For details, please refer to the billing of EIPs.

How do instances (cloud servers, databases) without a public IP address access the public Internet?

Instances without a public IP can apply for an EIP (refer to the previous question), or access the public Internet through a NAT Gateway.
NAT Gateway can provide both SNAT and DNAT functions for cloud servers within a private network. If you have multiple cloud servers that need to access the Internet through a single public IP, you can use NAT Gateway.

Can cloud servers change their public IP?

If your cloud server is bind to an EIP, you need to unbind that EIP, then apply for a new EIP or bind it with an existing one.

Can you apply to increase the quota after reaching the limit of EIPs?

Due to the limited resources of EIPs, each account can only apply for 20 per region and cannot apply for an increase in quota. For cloud servers without public IPs, you can use methods such as NAT Gateway to access the public Internet.

If a cloud server has a public IP or EIP, and the subnet it belongs to is associated with a NAT Gateway, how can public access be achieved?

If a cloud server has a public IP or EIP, and the subnet is associated with a NAT Gateway, meaning the route table sets the next hop of the subnet's public access traffic to the NAT Gateway, then by default, all traffic for accessing the public Internet from that cloud server will go through the NAT Gateway.

If you need to modify the priority so that the traffic of cloud servers accessing the public Internet goes

through a public IP, please refer to adjusting the priority of NAT Gateway and public IP.

Safety Categories
VPC Security Related

How to ensure the security of cloud servers in VPC?

VPC itself is a logically isolated network environment, and traffic control can be achieved by setting up security groups and network ACLs:

- Security groups: Provide network traffic control at the CVM instance level. Traffic not allowed in or out of instances will be automatically denied.
- Network ACLs: Provide network traffic control at the subnet level.

Port and security group related

Port related

Why should I open a port, and how?

You need to open the port in the security group before you can use the service corresponding to the port.
Example:
To access a webpage using port 8080, you need to open and allow this port in the security group settings.
The steps to open a port are as follows:

1. Log in to the security group console and click on the security group bind to the instance to enter the details page.
2. Select inbound/outbound rules and click Add Rule.
3. Enter your IP address (range) and the port information you need to open, then select Allow.
   For detailed directions, see Adding Security Group Rules.

Why can't the service be used after modifying the port?

After modifying the service port, you also need to open the corresponding port in the corresponding security group, otherwise the service will not be available.

Which ports are not supported by the cloud platform?

The following ports pose security risks. Due to security considerations, the operator blocks them, resulting in inaccessible access. It is recommended to change the port and avoid using the following ports for listening:

Protocol	Ports not supported
TCP	42,135,137,138,139,445,593,1025,1434,1068,3127,3128,3129,3130,4444,5554,9996
UDP	1026、1027、1434、1068、5554、9996、1028、1433、135-139

Security group related

Why is there a default deny rule in the security group?

Security group rules are applied sequentially from top to bottom. After the preceding allow rules are matched, other rules are defaultly denied. If all ports are allowed through the rules, then this final deny rule will not take effect. For security reasons, we provide this default setting.

What impact does selecting the incorrect security group have on instances bind to it? How can this be resolved?

- Issue risks
- Remote connections (SSH) to Linux instances, and remote desktop logs-in to Windows instances, may fail.
- Remote ping to the public IP and private network IP of CVM instances under this security group may fail.
- HTTP access to web services exposed by instances under this security group may fail.
- Instances under this security group may experience failures when accessing Internet services.
- Solution
- If the above issues occur, you can reconfigure the security group rules in the console's security group management, for example: only bind the default allow-all security group.
- For specific security group settings, please refer to Security Group - Security Group Rules.

What are the direction and policy of security groups?

- The direction of security group policies is divided into outbound and inbound. Outbound direction refers to filtering the outbound traffic of cloud servers, while inbound direction refers to filtering the inbound traffic of cloud servers.
- Security group policies are divided into Allow and Deny traffic.

What is the order of effectiveness for security group policies?

The order of effectiveness for security group policies is from top to bottom. The matching order of traffic through security group policies is from top to bottom. Once a match is successful, the policy takes effect.

Why can IPs that are not allowed by the security group still access cloud servers?

There may be the following reasons:

- The CVM may be bind to multiple security groups, and the specific IP is allowed in other security groups.
- The specific IP belongs to approved Converge Cloud public services.

Does using a security group mean that iptables cannot be used?

No. Security groups and iptables can be used simultaneously. Your traffic will be filtered twice, and the traffic flow is as follows:

- Outbound direction: processes on the instance > iptables > security group.
- Inbound direction: security group > iptables > processes on the instance.

Is there cloud API support for cloning security groups across projects and regions?

For the convenience of console users, we currently provide console support, and there is no direct cloud API support. You can indirectly achieve the cloning of security groups across projects and regions through the existing cloud API for batch import and export of security group rules.

Will cloning security groups across projects and regions also copy the cloud servers managed by the security group?

No, when cloning security groups across regions, only the original security group's inbound and outbound rules are cloned, and cloud servers need to be associated separately.

API Documentation
Virtual Private Cloud (VPC)(vpc)
version(2017-03-12)
API overview

API version

V3

CCN APIs

Interface name	Interface function
AcceptAttachCcnInstances	AcceptAttachCcnInstances
AttachCcnInstances	AttachCcnInstances
DescribeCcnAttachedInstances	DescribeCcnAttachedInstances
DescribeCcnRegionBandwidthLimits	DescribeCcnRegionBandwidthLimits
DescribeCcnRoutes	DescribeCcnRoutes
DetachCcnInstances	DetachCcnInstances
RejectAttachCcnInstances	RejectAttachCcnInstances
SetCcnRegionBandwidthLimits	SetCcnRegionBandwidthLimits

Direct Connect Gateway APIs

Interface name	Interface function
CreateDirectConnectGateway	CreateDirectConnectGateway
CreateLocalDestinationIpPortTranslationNatRule	CreateLocalDestinationIpPortTranslationNatRule
CreateLocalIpTranslationAclRule	CreateLocalIpTranslationAclRule
CreateLocalIpTranslationNatRule	CreateLocalIpTranslationNatRule
CreateLocalSourceIpPortTranslationAclRule	CreateLocalSourceIpPortTranslationAclRule
CreateLocalSourceIpPortTranslationNatRule	CreateLocalSourceIpPortTranslationNatRule
DeleteDirectConnectGateway	DeleteDirectConnectGateway

Interface name	Interface function
DeleteLocalDestinationIpPortTranslationNatRule	DeleteLocalDestinationIpPortTranslationNatRule
DeleteLocalIpTranslationAclRule	DeleteLocalIpTranslationAclRule
DeleteLocalIpTranslationNatRule	DeleteLocalIpTranslationNatRule
DeleteLocalSourceIpPortTranslationAclRule	DeleteLocalSourceIpPortTranslationAclRule
DeleteLocalSourceIpPortTranslationNatRule	DeleteLocalSourceIpPortTranslationNatRule
DescribeDirectConnectGateways	DescribeDirectConnectGateways
DescribeLocalDestinationIpPortTranslationNatRules	DescribeLocalDestinationIpPortTranslationNatRules
DescribeLocalIpTranslationAclRules	DescribeLocalIpTranslationAclRules
DescribeLocalIpTranslationNatRules	DescribeLocalIpTranslationNatRules
DescribeLocalSourceIpPortTranslationAclRules	DescribeLocalSourceIpPortTranslationAclRules
DescribeLocalSourceIpPortTranslationNatRules	DescribeLocalSourceIpPortTranslationNatRules
DescribePeerIpTranslationNatRules	DescribePeerIpTranslationNatRules
ModifyDirectConnectGatewayAttribute	ModifyDirectConnectGatewayAttribute
ModifyLocalDestinationIpPortTranslationNatRule	ModifyLocalDestinationIpPortTranslationNatRule
ModifyLocalIpTranslationAclRule	ModifyLocalIpTranslationAclRule
ModifyLocalIpTranslationNatRule	ModifyLocalIpTranslationNatRule
ModifyLocalSourceIpPortTranslationAclRule	ModifyLocalSourceIpPortTranslationAclRule
ModifyLocalSourceIpPortTranslationNatRule	ModifyLocalSourceIpPortTranslationNatRule
ModifyPeerIpTranslationNatRule	ModifyPeerIpTranslationNatRule

ENI APIs

Interface name	Interface function
AssignIpv6Addresses	AssignIpv6Addresses
AssignPrivateIpAddresses	AssignPrivateIpAddresses
AssociateNetworkInterfaceSecurityGroups	AssociateNetworkInterfaceSecurityGroups
AttachNetworkInterface	AttachNetworkInterface
CreateAndAttachNetworkInterface	CreateAndAttachNetworkInterface
CreateNetworkInterface	CreateNetworkInterface
DeleteNetworkInterface	DeleteNetworkInterface

Interface name	Interface function
DescribeNetworkInterfaceLimit	DescribeNetworkInterfaceLimit
DescribeNetworkInterfaces	DescribeNetworkInterfaces
DescribeNetworkInterfacesEx	DescribeNetworkInterfacesEx
DetachNetworkInterface	DetachNetworkInterface
DisassociateNetworkInterfaceSecurityGroups	DisassociateNetworkInterfaceSecurityGroups
MigrateNetworkInterface	MigrateNetworkInterface
MigratePrivateIpAddress	MigratePrivateIpAddress
ModifyIpv6AddressesAttribute	ModifyIpv6AddressesAttribute
ModifyNetworkInterfaceAttribute	ModifyNetworkInterfaceAttribute
ModifyPrivateIpAddressesAttribute	ModifyPrivateIpAddressesAttribute
UnassignIpv6Addresses	UnassignIpv6Addresses
UnassignPrivateIpAddresses	UnassignPrivateIpAddresses

Elastic IP APIs

Interface name	Interface function
AllocateAddresses	AllocateAddresses
AssociateAddress	AssociateAddress
DescribeAddressQuota	DescribeAddressQuota
DescribeAddresses	DescribeAddresses
DescribeNetworkInterfaceExtendIps	DescribeNetworkInterfaceExtendIps
DescribeTaskResult	DescribeTaskResult
DisassociateAddress	DisassociateAddress
ModifyAddressAttribute	ModifyAddressAttribute
ModifyAddressesBandwidth	ModifyAddressesBandwidth
ModifyNetworkInterfaceExtendIp	ModifyNetworkInterfaceExtendIp
ReleaseAddresses	ReleaseAddresses
TransformAddress	TransformAddress

Elastic IPv6 APIs

Interface name	Interface function
AllocateIp6AddressesBandwidth	AllocateIp6AddressesBandwidth
DescribeIp6Addresses	DescribeIp6Addresses
ModifyIp6AddressesBandwidth	ModifyIp6AddressesBandwidth
ReleaseIp6AddressesBandwidth	ReleaseIp6AddressesBandwidth

Gateway Traffic Monitoring APIs

Interface name	Interface function
DescribeGatewayFlowQos	DescribeGatewayFlowQos
DisableGatewayFlowMonitor	DisableGatewayFlowMonitor
EnableGatewayFlowMonitor	EnableGatewayFlowMonitor
ModifyGatewayFlowQos	ModifyGatewayFlowQos

High Availability Virtual IP APIs

Interface name	Interface function
CreateHaVip	CreateHaVip
DeleteHaVip	DeleteHaVip
DescribeHaVips	DescribeHaVips
HaVipAssociateAddressIp	HaVipAssociateAddressIp
HaVipDisassociateAddressIp	HaVipDisassociateAddressIp
ModifyHaVipAttribute	ModifyHaVipAttribute

IPv6 Translation Service APIs

Interface name	Interface function
AddIp6Rules	AddIp6Rules
CreateIp6Translators	CreateIp6Translators
DeleteIp6Translators	DeleteIp6Translators
DescribeIp6TranslatorQuota	DescribeIp6TranslatorQuota
DescribeIp6Translators	DescribeIp6Translators

Interface name	Interface function
ModifyIp6Rule	ModifyIp6Rule
ModifyIp6Translator	ModifyIp6Translator
RemoveIp6Rules	RemoveIp6Rules

NAT Gateway APIs

Interface name	Interface function
AssociateNatGatewayAddress	AssociateNatGatewayAddress
CreateNatGateway	CreateNatGateway
CreateNatGatewayDestinationIpPortTranslationNatRule	CreateNatGatewayDestinationIpPortTranslationNatRule
CreateNatGatewaySourceIpTranslationNatRule	CreateNatGatewaySourceIpTranslationNatRule
DeleteNatGateway	DeleteNatGateway
DeleteNatGatewayDestinationIpPortTranslationNatRule	DeleteNatGatewayDestinationIpPortTranslationNatRule
DeleteNatGatewaySourceIpTranslationNatRule	DeleteNatGatewaySourceIpTranslationNatRule
DescribeNatGatewayDestinationIpPortTranslationNatRules	DescribeNatGatewayDestinationIpPortTranslationNatRules
DescribeNatGatewaySourceIpTranslationNatRules	DescribeNatGatewaySourceIpTranslationNatRules
DescribeNatGateways	DescribeNatGateways
DisassociateNatGatewayAddress	DisassociateNatGatewayAddress
ModifyNatGatewayAddressStatus	ModifyNatGatewayAddressStatus
ModifyNatGatewayAttribute	ModifyNatGatewayAttribute
ModifyNatGatewayDestinationIpPortTranslationNatRule	ModifyNatGatewayDestinationIpPortTranslationNatRule
ModifyNatGatewaySourceIpTranslationNatRule	ModifyNatGatewaySourceIpTranslationNatRule
ResetNatGatewayConnection	ResetNatGatewayConnection

Network ACL APIs

Interface name	Interface function
AssociateNetworkAclSubnets	AssociateNetworkAclSubnets
CreateNetworkAcl	CreateNetworkAcl
DeleteNetworkAcl	DeleteNetworkAcl

Interface name	Interface function
DescribeNetworkAcls	DescribeNetworkAcls
DisassociateNetworkAclSubnets	DisassociateNetworkAclSubnets
ModifyNetworkAclAttribute	ModifyNetworkAclAttribute
ModifyNetworkAclEntries	ModifyNetworkAclEntries

Network Parameter Template APIs

Interface name	Interface function
CreateAddressTemplate	CreateAddressTemplate
CreateAddressTemplateGroup	CreateAddressTemplateGroup
CreateServiceTemplate	CreateServiceTemplate
CreateServiceTemplateGroup	CreateServiceTemplateGroup
DeleteAddressTemplate	DeleteAddressTemplate
DeleteAddressTemplateGroup	DeleteAddressTemplateGroup
DeleteServiceTemplate	DeleteServiceTemplate
DeleteServiceTemplateGroup	DeleteServiceTemplateGroup
DescribeAddressTemplateGroups	DescribeAddressTemplateGroups
DescribeAddressTemplates	DescribeAddressTemplates
DescribeServiceTemplateGroups	DescribeServiceTemplateGroups
DescribeServiceTemplates	DescribeServiceTemplates
DescribeTemplateLimits	DescribeTemplateLimits
ModifyAddressTemplateAttribute	ModifyAddressTemplateAttribute
ModifyAddressTemplateGroupAttribute	ModifyAddressTemplateGroupAttribute
ModifyServiceTemplateAttribute	ModifyServiceTemplateAttribute
ModifyServiceTemplateGroupAttribute	ModifyServiceTemplateGroupAttribute

Network Probe APIs

Interface name	Interface function
CheckNetDetectState	CheckNetDetectState

Interface name	Interface function
CreateNetDetect	CreateNetDetect
DeleteNetDetect	DeleteNetDetect
DescribeNetDetectStates	DescribeNetDetectStates
DescribeNetDetects	DescribeNetDetects
ModifyNetDetect	ModifyNetDetect

Other APIs

Interface name	Interface function
CreateVpcEndPoint	CreateVpcEndPoint
DescribeGatewayFlowMonitorDetail	DescribeGatewayFlowMonitorDetail

Peering Connection APIs

Interface name	Interface function
AcceptVpcPeeringConnection	AcceptVpcPeeringConnection
AcceptVpcPeeringConnectionEx	AcceptVpcPeeringConnectionEx
CreateVpcPeeringConnection	CreateVpcPeeringConnection
CreateVpcPeeringConnectionEx	CreateVpcPeeringConnectionEx
DeleteVpcPeeringConnection	DeleteVpcPeeringConnection
DeleteVpcPeeringConnectionEx	DeleteVpcPeeringConnectionEx
EnableVpcPeeringConnection	EnableVpcPeeringConnection
EnableVpcPeeringConnectionEx	EnableVpcPeeringConnectionEx
ModifyVpcPeeringConnection	ModifyVpcPeeringConnection
ModifyVpcPeeringConnectionEx	ModifyVpcPeeringConnectionEx
RejectVpcPeeringConnection	RejectVpcPeeringConnection
RejectVpcPeeringConnectionEx	RejectVpcPeeringConnectionEx

Private Link APIs

Interface name	Interface function

Interface name	Interface function
CreateVpcEndPointService	CreateVpcEndPointService
CreateVpcEndPointServiceWhiteList	CreateVpcEndPointServiceWhiteList
DeleteVpcEndPoint	DeleteVpcEndPoint
DeleteVpcEndPointService	DeleteVpcEndPointService
DeleteVpcEndPointServiceWhiteList	DeleteVpcEndPointServiceWhiteList
DescribeVpcEndPoint	DescribeVpcEndPoint
DescribeVpcEndPointService	DescribeVpcEndPointService
DescribeVpcEndPointServiceWhiteList	DescribeVpcEndPointServiceWhiteList
DisassociateVpcEndPointSecurityGroups	DisassociateVpcEndPointSecurityGroups
EnableVpcEndPointConnect	EnableVpcEndPointConnect
EnableVpcEndPointConnection	EnableVpcEndPointConnection
ModifyVpcEndPointAttribute	ModifyVpcEndPointAttribute
ModifyVpcEndPointServiceAttribute	ModifyVpcEndPointServiceAttribute
ModifyVpcEndPointServiceWhiteList	ModifyVpcEndPointServiceWhiteList

Routing Table APIs

Interface name	Interface function
CreateIpv6Routes	CreateIpv6Routes
CreateRouteTable	CreateRouteTable
CreateRoutes	CreateRoutes
DeleteIpv6Routes	DeleteIpv6Routes
DeleteRouteTable	DeleteRouteTable
DeleteRoutes	DeleteRoutes
DescribeRouteConflicts	DescribeRouteConflicts
DescribeRouteTables	DescribeRouteTables
DisableRoutes	DisableRoutes
EnableRoutes	EnableRoutes
ModifyIpv6Routes	ModifyIpv6Routes
ModifyRouteTableAttribute	ModifyRouteTableAttribute

Interface name	Interface function
ReplaceRouteTableAssociation	ReplaceRouteTableAssociation
ReplaceRoutes	ReplaceRoutes
ResetRoutes	ResetRoutes

Security Group APIs

Interface name	Interface function
CreateDefaultSecurityGroup	CreateDefaultSecurityGroup
CreateSecurityGroup	CreateSecurityGroup
CreateSecurityGroupPolicies	CreateSecurityGroupPolicies
CreateSecurityGroupWithPolicies	CreateSecurityGroupWithPolicies
DeleteSecurityGroup	DeleteSecurityGroup
DeleteSecurityGroupPolicies	DeleteSecurityGroupPolicies
DescribeDBInstancesWithSecurityGroup	DescribeDBInstancesWithSecurityGroup
DescribeSecurityGroupAssociationStatistics	DescribeSecurityGroupAssociationStatistics
DescribeSecurityGroupLimits	DescribeSecurityGroupLimits
DescribeSecurityGroupPolicies	DescribeSecurityGroupPolicies
DescribeSecurityGroupReferences	DescribeSecurityGroupReferences
DescribeSecurityGroups	DescribeSecurityGroups
ModifySecurityGroupAttribute	ModifySecurityGroupAttribute
ModifySecurityGroupPolicies	ModifySecurityGroupPolicies
ReplaceSecurityGroupPolicy	ReplaceSecurityGroupPolicy

Subnet APIs

Interface name	Interface function
AssignIpv6SubnetCidrBlock	AssignIpv6SubnetCidrBlock
CheckDefaultSubnet	CheckDefaultSubnet
CheckIpInSubnet	CheckIpInSubnet
CreateSubnet	CreateSubnet

Interface name	Interface function
CreateSubnets	CreateSubnets
DeleteSubnet	DeleteSubnet
DescribeSubnets	DescribeSubnets
ModifySubnetAttribute	ModifySubnetAttribute
UnassignIpv6SubnetCidrBlock	UnassignIpv6SubnetCidrBlock

VPC APIs

Interface name	Interface function
AssignIpv6CidrBlock	AssignIpv6CidrBlock
AttachClassicLinkVpc	AttachClassicLinkVpc
CheckAssistantCidr	CheckAssistantCidr
CreateAssistantCidr	CreateAssistantCidr
CreateDefaultVpc	CreateDefaultVpc
CreateLocalGateway	CreateLocalGateway
CreateVpc	CreateVpc
DeleteAssistantCidr	DeleteAssistantCidr
DeleteLocalGateway	DeleteLocalGateway
DeleteVpc	DeleteVpc
DescribeAccountAttributes	DescribeAccountAttributes
DescribeAssistantCidr	DescribeAssistantCidr
DescribeClassicLinkInstances	DescribeClassicLinkInstances
DescribeIpv6Section	DescribeIpv6Section
DescribeIpv6Vpc	DescribeIpv6Vpc
DescribeLocalGateway	DescribeLocalGateway
DescribeNmsCidrs	DescribeNmsCidrs
DescribeUsedIpAddress	DescribeUsedIpAddress
DescribeVpcInstances	DescribeVpcInstances
DescribeVpcIpv6Addresses	DescribeVpcIpv6Addresses
DescribeVpcLimits	DescribeVpcLimits

Interface name	Interface function
DescribeVpcPrivateIpAddresses	DescribeVpcPrivateIpAddresses
DescribeVpcs	DescribeVpcs
DetachClassicLinkVpc	DetachClassicLinkVpc
ModifyAssistantCidr	ModifyAssistantCidr
ModifyLocalGateway	ModifyLocalGateway
ModifyVpcAttribute	ModifyVpcAttribute
ResetHaVip	ResetHaVip
UnassignIpv6CidrBlock	UnassignIpv6CidrBlock

VPN Gateway APIs

Interface name	Interface function
CreateCustomerGateway	CreateCustomerGateway
CreateGatewayVpnSSLClient	CreateGatewayVpnSSLClient
CreateVpnConnection	CreateVpnConnection
CreateVpnGateway	CreateVpnGateway
CreateVpnGatewaySSLServer	CreateVpnGatewaySSLServer
DeleteCustomerGateway	DeleteCustomerGateway
DeleteVpnConnection	DeleteVpnConnection
DeleteVpnGateway	DeleteVpnGateway
DeleteVpnGatewaySSLClient	DeleteVpnGatewaySSLClient
DeleteVpnGatewaySSLServer	DeleteVpnGatewaySSLServer
DescribeCustomerGatewayVendors	DescribeCustomerGatewayVendors
DescribeCustomerGateways	DescribeCustomerGateways
DescribeVpcResourceDashboard	DescribeVpcResourceDashboard
DescribeVpnConnections	DescribeVpnConnections
DescribeVpnGatewayCcnRoutes	DescribeVpnGatewayCcnRoutes
DescribeVpnGatewaySSLClients	DescribeVpnGatewaySSLClients
DescribeVpnGatewaySSLServers	DescribeVpnGatewaySSLServers
DescribeVpnGateways	DescribeVpnGateways

Interface name	Interface function
DisableVpnGatewaySSLClientCert	DisableVpnGatewaySSLClientCert
DownloadCustomerGatewayConfiguration	DownloadCustomerGatewayConfiguration
DownloadVpnGatewaySSLClientCert	DownloadVpnGatewaySSLClientCert
EnableVpnGatewaySSLClientCert	EnableVpnGatewaySSLClientCert
InquiryPriceCreateVpnGateway	InquiryPriceCreateVpnGateway
InquiryPriceResetVpnGatewayInternetMaxBandwidth	InquiryPriceResetVpnGatewayInternetMaxBandwidth
ModifyCustomerGatewayAttribute	ModifyCustomerGatewayAttribute
ModifyVpnConnectionAttribute	ModifyVpnConnectionAttribute
ModifyVpnGatewayAttribute	ModifyVpnGatewayAttribute
ModifyVpnGatewayCcnRoutes	ModifyVpnGatewayCcnRoutes
ModifyVpnGatewaySSLClient	ModifyVpnGatewaySSLClient
ResetVpnConnection	ResetVpnConnection
ResetVpnGatewayInternetMaxBandwidth	ResetVpnGatewayInternetMaxBandwidth

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:


```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```


- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:


```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```


- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

CCN APIs
AcceptAttachCcnInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AcceptAttachCcnInstances) is used for the CCN owner to accept and agree to the association operation when instances are associated across accounts.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-12-07 22:43:49.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AcceptAttachCcnInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-gree226l
Instances	Yes	No	Array of CcnInstance	Accept associated instance list. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
UnsupportedOperation.CcnNotAttached	The instance is not associated with a CCN.
UnsupportedOperation.UnableCrossFinance	The current CCN cannot be associated with Finance Cloud instances.

AttachCcnInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AttachCcnInstances) is used to load network instances into CCN instances, which include VPCs and Direct Connect gateways.

The number of network instances that can be associated with each CCN is limited. For details, refer to the product documentation. If expansion is needed, contact the online customer service.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-05-30 20:12:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AttachCcnInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-gree226l
CcnUin	No	No	String	UIN of CCN (root account). The default is the UIN of the current account. Example: 100000072292
Instances	Yes	No	Array of CcnInstance	Associated Network Instance List Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
ResourceNotFound	The resource does not exist
UnsupportedOperation.CcnAttached	The instance is already associated with a CCN.
UnsupportedOperation.UnableCrossBorder	Cross-border is not supported.
UnsupportedOperation.UinNotFound	The account ID does not exist.
InvalidParameterValue.CcnAttachBmvpcLimitExceeded	The number of BM VPCs associated with the specified CCN has reached the upper limit.
UnsupportedOperation.UnableCrossFinance	The current CCN cannot be associated with Finance Cloud instances.

DescribeCcnAttachedInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeCcnAttachedInstances) is used to query the network instances associated with a CCN instance.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-01-23 01:17:29.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCcnAttachedInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	No	Uint64	Offset Example: 0
Limit	No	No	Uint64	Returned quantity Example: 20
Filters	No	No	Array of Filter	Filters: • ccn-id - String - (Filters) CCN instance ID. • instance-type - String - (Filters) Type of associated instance. • instance-region - String - (Filters) Region of the associated instance. • instance-id - String - (Filters) Associated instance ID. Example:View
CcnId	No	No	String	CCN instance ID Example: ccn-245ecr35
OrderField	No	No	String	Sorting fields. Supports CcnId, InstanceType, InstanceId, InstanceName, InstanceRegion, AttachedTime, and State. Example: CcnId
OrderDirection	No	No	String	Sorting method. ASC : Ascending order, DESC : Descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example:
InstanceSet	Array of CcnAttachedInstance	Associated instance list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeCcnRegionBandwidthLimits

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeCcnRegionBandwidthLimits) is used to query the outbound bandwidth limits for each region of CCN. This API only returns regions included in the associated network instances.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-09-30 19:56:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCcnRegionBandwidthLimits
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-f49l6u0z

3. Output Parameters

Parameter name	Type	Description
CcnRegionBandwidthLimitSet	Array of CcnRegionBandwidthLimit	The regional outbound bandwidth cap of the CCN Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeCcnRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeCcnRoutes) is used to query routes that have been added to the CCN.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-12-20 05:37:04.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCcnRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-gree226l. Example: ccn-gree226l
RouteIds	No	No	Array of String	Unique ID of CCN routing policy, e.g., ccnr-f49l6u0z. Example: ccnr-f49l6u0z
Filters	No	No	Array of Filter	Filters. Parameters RouteIds and Filters must not be specified simultaneously. • route-id - String - (Filters) Routing policy ID. • cidr-block - String - (Filters) Destination endpoint. • instance-type - String - (Filters) Type of the next hop. • instance-region - String - (Filters) Region of the next hop. • instance-id - String - (Filters) Next hop instance ID. Example:View
Offset	No	No	Uint64	Offset Example: 0
Limit	No	No	Uint64	Returned quantity Example: 10

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example:
RouteSet	Array of CcnRoute	CCN routing policy object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DetachCcnInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DetachCcnInstances) is used to disassociate specified network instances from a CCN instance.

After network instances are disassociated, the corresponding routing policies will be deleted altogether.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-11-15 17:40:59.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DetachCcnInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-gree226l
Instances	Yes	No	Array of CcnInstance	List of network instances to dissociate Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

RejectAttachCcnInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (RejectAttachCcnInstances) is used for the CCN owner to reject the association operation when instances are associated across accounts.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-12-07 22:50:42.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RejectAttachCcnInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-gree226l
Instances	Yes	No	Array of CcnInstance	List of instances rejecting association. Example:View

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
UnsupportedOperation.CcnNotAttached	The instance is not associated with a CCN.

SetCcnRegionBandwidthLimits

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (SetCcnRegionBandwidthLimits) is used to set the outbound bandwidth limit for each region of a CCN, and can only be used to set the outbound bandwidth limits for regions included in the associated network instances.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-07-04 20:13:00.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SetCcnRegionBandwidthLimits
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CcnId	Yes	No	String	CCN instance ID, e.g., ccn-f49l6u0z. Example: ccn-f49l6u0z
CcnRegionBandwidthLimits	Yes	No	Array of CcnRegionBandwidthLimit	The regional outbound bandwidth cap of the CCN. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

Direct Connect Gateway APIs
CreateDirectConnectGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateDirectConnectGateway) is used to create a Direct Connect gateway.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 03:57:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDirectConnectGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayName	Yes	No	String	Direct Connect Gateway Name Example: demo
NetworkType	Yes	No	String	Associated network type. Valid values: • VPC - VPC . Example: VPC
NetworkInstanceId	Yes	No	String	• When NetworkType is VPC, the value here is specified as the VPC instance ID . Example: vpc-m7sr81gh
GatewayType	Yes	No	String	Gateway type. Valid values: • NORMAL - (default) standard type . • NAT - NAT type . NAT type supports network address translation configuration and cannot be changed after being set. You can create a NAT type DC gateway and a non-NAT type DC gateway in a VPC. Example: NAT
Bandwidth	No	No	Int64	Bandwidth rate limit value of Direct Connect gateway. Example: 0

3. Output Parameters

Parameter name	Type	Description
DirectConnectGateway	DirectConnectGateway	Direct Connect gateway object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

CreateLocalDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create local destination IP port translation for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-15 00:37:55.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalDestinationIpPortTranslationNatRuleSet	Yes	No	Array of LocalDestinationIpPortTranslationNatRule	Local destination IP port translation Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed

Error Code	Description
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter
ResourceNotFound	The resource does not exist

CreateLocalIpTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create a local IP translation ACL rule for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-06 10:12:55.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalIpTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OriginalIp	Yes	No	String	Original IP Example: 10.0.0.5
TranslationIp	Yes	No	String	Mapping IP Example: 2.2.2.2
LocalIpTranslationAclRuleSet	Yes	No	Array of LocalIpTranslationAclRule	Local IP translation list ACL list Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter
ResourceNotFound	The resource does not exist

CreateLocalIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create local IP translation for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-01 20:52:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalIpTranslationNatRuleSet	Yes	No	Array of LocalIpTranslationNatRule	Local IP translation list Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API.

Parameter name	Type	Description
		Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

CreateLocalSourceIpPortTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create the local source IP port translation ACL rule for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-13 04:35:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalSourceIpPortTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
TranslationIpPool	Yes	No	String	IP pool Example: 2.2.2.2/16
LocalSourceIpPortTranslationAclRuleSet	Yes	No	Array of LocalSourceIpPortTranslationAclRule	Local source IP port translation ACL list Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

Error Code	Description
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter
ResourceNotFound	The resource does not exist

CreateLocalSourceIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create local source IP port translation for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 19:00:01.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalSourceIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalSourceIpPortTranslationNatRuleSet	Yes	No	Array of LocalSourceIpPortTranslationNatRule	Local source IP port translation list Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API. Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.

Error Code	Description
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

DeleteDirectConnectGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteDirectConnectGateway) is used to delete Direct Connect gateways.

If it is a NAT gateway, deleting the Direct Connect gateway will also clear the NAT rules and ACL policies.
After the Direct Connect gateway is deleted, the system will delete the routing policies related to the Direct Connect gateway from the routing table.
This API is completed asynchronously. To query the result of the asynchronous task, use the `TaskId` returned by this API to poll the `DescribeVpcTaskResult` API.
Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 04:07:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteDirectConnectGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Unique ID of Direct Connect gateway, e.g., dcg-9o233uri. Example: dcg-e6mxyyvj

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Task ID of this asynchronous task. Example: 65535

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DeleteLocalDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete the local destination IP port translation of a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-15 00:45:03.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalDestinationIpPortTranslationNatRuleSet	Yes	No	Array of LocalDestinationIpPortTranslationNatRule	Customer IP Translation List Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed

Error Code	Description
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

DeleteLocalIpTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete Direct Connect gateway local IP translation ACL rules

Default interface request rate limit: 20 times per second.

Interface update time: 2025-06-17 15:15:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalIpTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OriginalIp	Yes	No	String	Original IP Example: 10.0.0.5
TranslationIp	Yes	No	String	Mapping IP Example: 2.2.2.2

Parameter name	Required	Allow NULL	Type	Description
LocalIpTranslationAclRuleSet	Yes	No	Array of AclRuleId	Local IP translation list ACL list Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.

Error Code	Description
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.

DeleteLocalIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete the local IP translation of a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-06 10:16:10.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalIpTranslationNatRuleSet	Yes	No	Array of LocalIpTranslationNatRule	Local IP translation list Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API.

Parameter name	Type	Description
		Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

DeleteLocalSourceIpPortTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete the local source IP port translation ACL rule for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-13 04:36:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalSourceIpPortTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
TranslationIpPool	Yes	No	String	IP pool Example: 2.2.2.2/16
LocalSourceIpPortTranslationAclRuleSet	Yes	No	Array of AclRuleIdType	Local source IP port translation ACL list Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

DeleteLocalSourceIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete the local source IP port translation of a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 19:03:50.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalSourceIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
LocalSourceIpPortTranslationNatRuleSet	Yes	No	Array of LocalSourceIpPortTranslationNatRule	Local source IP port translation list Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API. Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidProjectId.NotFound	The project ID is invalid.
InvalidParameter	Invalid input parameters.

Error Code	Description
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

DescribeDirectConnectGateways

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeDirectConnectGateways) is used to query Direct Connect gateways.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 04:01:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDirectConnectGateways
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayIds	No	No	Array of String	Unique ID of Direct Connect gateway, e.g., dcg-9o233uri. Example: ["dcg-dimeg9zd\r\n","dcg-6eeis68f\r\n","dcg-94cdyvfr\r\n"]
Filters	No	No	Array of Filter	Filters. Parameters DirectConnectGatewayIds and Filters must not be specified simultaneously. • direct-connect-gateway-id - String - Unique ID of the Direct Connect gateway, e.g., dcg-9o233uri . • direct-connect-gateway-name - String - Name of the Direct Connect gateway, fuzzy search by default. • direct-connect-gateway-ip - String - IP of the Direct Connect gateway. • gateway-type - String - Gateway type, options: NORMAL (Standard), NAT (NAT type). • network-type - String - Network type, options: VPC (VPC type), CCN (CCN type). • ccn-id - String - CCN ID where the Direct Connect gateway is located. • vpc-id - String - VPC ID where the Direct Connect gateway is located. Example:View
Offset	No	No	Uint64	Offset. Example: 0
Limit	No	No	Uint64	Returned quantity. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example: 1
DirectConnectGatewaySet	Array of DirectConnectGateway	Direct Connect gateway object array. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

DescribeLocalDestinationIpPortTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query Direct Connect gateway local destination IP port translation

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-24 05:43:25.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalDestinationIpPortTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects. The default value is 20. Example: 1
Filters	No	No	Array of Filter	Filter criteria, which support filtering by description. Example:View

3. Output Parameters

Parameter name	Type	Description
LocalDestinationIpPortTranslationNatRuleSet	Array of LocalDestinationIpPortTranslationNatRule	Local destination IP port translation list Example:View
TotalCount	Int64	Number of local destination IP port translation list that meet the criteria Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.

DescribeLocalIpTranslationAclRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the local IP translation ACL rule for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-01 21:14:04.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalIpTranslationAclRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects, 100 by default. Example: 1
Filters	No	No	Array of Filter	Filter criteria, supporting filtering by original-ip and translation-ip. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
LocalIpTranslationAclRuleSet	Array of LocalIpTranslationAclRule	Local IP translation ACL rule list Example:View
TotalCount	Int64	Count of local IP translation ACL rule lists that meet the criteria Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.

DescribeLocalIpTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the local IP translation of a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-24 05:32:59.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalIpTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects. The default value is 20. Example: 1
Filters	No	No	Array of Filter	Filter criteria, which support filtering by description. Example:View

3. Output Parameters

Parameter name	Type	Description
LocalIpTranslationNatRuleSet	Array of LocalIpTranslationNatRule	Local IP translation list Example:View
TotalCount	Int64	Number of eligible local IP translation lists Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.

DescribeLocalSourceIpPortTranslationAclRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query Direct Connect gateway local source IP port translation ACL rules

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-02 14:50:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalSourceIpPortTranslationAclRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects, 100 by default. Example: 1
Filters	No	No	Array of Filter	Filter criteria, which supports filtering by translation-ip-pool. Example:View

3. Output Parameters

Parameter name	Type	Description
LocalSourceIpPortTranslationAclRuleSet	Array of LocalSourceIpPortTranslationAclRule	Local source IP port translation ACL rule list Example:View
TotalCount	Int64	Number of eligible local source IP port translation ACL rules Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

DescribeLocalSourceIpPortTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query Direct Connect gateway local source IP port translation

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-24 05:46:52.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalSourceIpPortTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects. The default value is 20. Example: 1
Filters	No	No	Array of Filter	Filter criteria, which support filtering by description. Example:View

3. Output Parameters

Parameter name	Type	Description
LocalSourceIpPortTranslationNatRuleSet	Array of LocalSourceIpPortTranslationNatRule	Local source IP port translation list Example:View
TotalCount	Int64	Number of eligible local source IP port translation lists Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InternalServerError	Internal operation error.
InvalidInstance.NotSupported	The instance is not supported.

DescribePeerIpTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the Direct Connect customer gateway IP translation

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-27 03:21:37.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribePeerIpTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Number of request objects. The default value is 20. Example: 20
Filters	No	No	Array of Filter	Filter criteria, which support filtering by description. Example:View

3. Output Parameters

Parameter name	Type	Description
PeerIpTranslationNatRuleSet	Array of LocalIpTranslationNatRule	Customer IP translation list Example:View
TotalCount	Int64	Count of eligible customer IP translation lists Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.

ModifyDirectConnectGatewayAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyDirectConnectGatewayAttribute) is used to modify the attributes of a Direct Connect gateway.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-28 11:26:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyDirectConnectGatewayAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Unique ID of Direct Connect gateway, e.g., dcg-9o233uri. Example: dcg-k6cswwhx
DirectConnectGatewayName	No	No	String	Direct Connect gateway name, which can be named arbitrarily, but must not exceed 60 characters. Example: new+name
CcnRouteType	No	No	String	CCN route learning type, options: BGP (Automatic learning), STATIC (Static, i.e., user configuration). Modification of CcnRouteType is only supported for CCN type Direct Connect gateways that have enabled the BGP feature. Example: BGP
EnableBGPCommunity	No	No	Bool	The BGP community attribute is enabled for Direct Connect gateway. Example: True
Bandwidth	No	No	Int64	Bandwidth rate limit value of Direct Connect gateway. Example: 100

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation.DirectConnectGatewayIsUpdatingCommunity	The Direct Connect gateway is updating the BGP Community attribute.
InvalidParameter	Invalid input parameters.
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

ModifyLocalDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the local destination IP port translation for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-02 20:08:25.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OldProtocol	Yes	No	String	Old Protocol Example: tcp
OldOriginalPort	Yes	No	Int64	Legacy source port Example: 80
OldOriginalIp	Yes	No	String	Legacy source IP Example: 10.0.0.5

Parameter name	Required	Allow NULL	Type	Description
OldTranslationPort	Yes	No	Int64	Legacy destination port Example: 80
OldTranslationIp	Yes	No	String	Legacy destination IP Example: 2.2.2.2
Protocol	No	No	String	Modified Protocol Example: tcp
OriginalPort	No	No	Int64	Modified Source Port Example: 80
OriginalIp	No	No	String	Modified Source IP Example: 10.0.0.5
TranslationPort	No	No	Int64	Modified Destination Port Example: 80
TranslationIp	No	No	String	Modified destination IP Example: 2.2.2.2
Description	No	No	String	Description after modification Example: for_demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit

Error Code	Description
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ModifyLocalIpTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the local IP translation ACL rule for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-02 20:01:55.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalIpTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OriginalIp	Yes	No	String	Original IP Example: 10.0.0.5
TranslationIp	Yes	No	String	Mapping IP Example: 2.2.2.2
LocalIpTranslationAclRuleSet	Yes	No	Array of LocalIpTranslationAclRuleNeedId	Local IP translation list ACL list Example:View

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ModifyLocalIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the local IP translation of a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-02 20:02:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OldOriginalIp	Yes	No	String	Old original IP Example: 10.0.0.5
OldTranslationIp	Yes	No	String	Deprecated mapping IP Example: 2.2.2.2
OriginalIp	Yes	No	String	Modified Original IP Example: 10.0.0.5
TranslationIp	Yes	No	String	Modified mapping IP Example: 2.2.2.2

Parameter name	Required	Allow NULL	Type	Description
Description	Yes	No	String	Description after modification Example: for_demo

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.

Error Code	Description
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ModifyLocalSourceIpPortTranslationAclRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the local source IP port translation ACL rule for a Direct Connect gateway.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-02 20:02:49.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalSourceIpPortTranslationAclRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
TranslationIpPool	Yes	No	String	IP pool Example: 2.2.2.2/16
LocalSourceIpPortTranslationAclRuleSet	Yes	No	Array of LocalSourceIpPortTranslationAclRuleNeedId	Local source IP port translation ACL list Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.

Error Code	Description
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ModifyLocalSourceIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the local source IP port translation for a Direct Connect gateway

Default interface request rate limit: 20 times per second.

Interface update time: 2025-06-17 15:23:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalSourceIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OldLocalSourceIpPortTranslationNatRule	Yes	No	LocalSourceIpPortTranslationNatRule	Original local source IP port translation Example:View
NewLocalSourceIpPortTranslationNatRule	Yes	No	LocalSourceIpPortTranslationNatRule	New Local Source IP Port Translation Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Asynchronous task TaskId. Task status can be queried using the DescribeTaskResult API. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.

Error Code	Description
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ModifyPeerIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the Direct Connect customer gateway IP translation

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-02 20:03:38.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyPeerIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectGatewayId	Yes	No	String	Direct connect gateway ID Example: dcg-e6mxyyvj
VpcId	Yes	No	String	Character-type VPCID Example: vpc-67wlqf6v
OldOriginalIp	Yes	No	String	Old original IP Example: 10.0.0.5
OldTranslationIp	Yes	No	String	Deprecated mapping IP Example: 2.2.2.2

Parameter name	Required	Allow NULL	Type	Description
OriginalIp	Yes	No	String	Modified Original IP Example: 10.0.0.5
TranslationIp	Yes	No	String	Modified mapping IP Example: 2.2.2.2
Description	Yes	No	String	Description after modification Example: for_demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
InvalidParameterValue.IpExists	It already exists in the rules.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
InvalidParameterValue.NatRuleExists	Existed

Error Code	Description
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
InvalidParameter.InvalidPortType	Port Type Error
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.Empty	Missing parameter

ENI APIs
AssignIpv6Addresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssignIpv6Addresses) is used for ENI to apply for IPv6 addresses.

This API is completed asynchronously. To query the execution results of asynchronous tasks, use the RequestId returned by this API to poll the QueryTask API.

- The number of IP addresses that a single ENI can bind is limited. For more information on resource limitations, see ENI Usage Limits.
- You can specify the IPv6 addresses to apply for. The address type cannot be the primary IP. IPv6 address can temporarily only serve as an auxiliary IP.
- The address must be within the subnet of the ENI and cannot be occupied.* When one or more auxiliary IPv6 addresses are applied for on an ENI, the API will return a specified number of auxiliary IPv6 addresses within the subnet IP range of the ENI.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-01 04:51:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssignIpv6Addresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID , e.g., eni-m6dyj72l . Example: eni-5u5biujl
Ipv6Addresses	No	No	Array of Ipv6Address	Specified IPv6 address list. Up to 10 at a time. It is calculated together with the input parameter Ipv6AddressCount to determine the quota. Either Ipv6AddressCount or IPv6 addresses must be specified. Example:View
Ipv6AddressCount	No	No	Uint64	The number of automatically assigned IPv6 addresses. The total number of private IP addresses cannot exceed the quota. The quota is calculated in combination with the input parameter Ipv6Addresses . Either Ipv6Addresses or this field is required. Example: 1

3. Output Parameters

Parameter name	Type	Description
Ipv6AddressSet	Array of Ipv6Address	List of IPv6 addresses allocated to the ENI. Example:View
taskId	Int64	Des task taskId Example: 213415
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation.InvalidState	The resource status is invalid.
MissingParameter	Missing parameters. The request did not carry the required parameter.
LimitExceeded.Address	The number of IP addresses allocated has reached the upper limit.
UnsupportedOperation.UnassignCidrBlock	The IPv6 IP range is not allocated.
ResourceInUse.Address	The specified IP address is already in use.
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.

AssignPrivateIpAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssignPrivateIpAddresses) is used for ENI to apply for a private IP.

- There is a limit to the number of IP addresses an ENI can be bound to. For more information on resource restrictions, see ENI Usage Limits.
- It is acceptable to specify a private IP address to apply for. The private IP address type cannot be the primary IP. The primary IP already exists and cannot be modified, and the private IP must be within the ENI's subnet and must not be occupied.
- When one or more auxiliary private IPs are applied for on an ENI, the API will return a specified number of auxiliary private IPs within the subnet IP range of the ENI.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-01 04:53:40.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssignPrivateIpAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-afo43z61
PrivateIpAddresses	No	No	Array of PrivateIpAddressSpecification	Specified VPC IP information, up to 10 can be specified at once. At least one of this and SecondaryPrivateIpAddressCount should be provided. Example:View
SecondaryPrivateIpAddressCount	No	No	Uint64	Number of newly applied private IP addresses. At least one of PrivateIpAddresses and it must be provided. The total number of private IP addresses must not exceed the quota. For details, see <a href="/document/product/576/18527">ENI Usage Limits. Example: 2

3. Output Parameters

Parameter name	Type	Description
PrivateIpAddressSet	Array of PrivateIpAddressSpecification	Private IP details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInsufficient	Insufficient resources

AssociateNetworkInterfaceSecurityGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssociateNetworkInterfaceSecurityGroups) is used to bind security groups (SecurityGroup) with ENI.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-05 00:34:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssociateNetworkInterfaceSecurityGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceIds	Yes	No	Array of String	ENI instance ID, e.g., eni-pxir56ns. The upper limit of instances per request is 100. Example: ["eni-1a2b3c4d"]
SecurityGroupIds	Yes	No	Array of String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. The upper limit of instances per request is 100. Example: ["sg-1a2b3c4d"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

AttachNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to bind an ENI to a CVM instance.

- One CVM instance can bind multiple ENIs but can have only one primary network interface. For details on limits, see Usage Limits.
- One ENI can only be bound to one CVM instance at a time.
- Only CVM instances that are running or have been shut down can bind ENIs. See InstanceStatus for specific CVM instance statuses.
- The CVM instance bound to an ENI should be on a VPC, and the availability zone of the CVM instance should be the same as that of the ENI's subnet.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-14 01:11:56.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AttachNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-m6dyj72l

Parameter name	Required	Allow NULL	Type	Description
InstanceId	Yes	No	String	CVM instance ID, e.g., ins-r8hr2upy. Example: ins-r8hr2upy

3. Output Parameters

Parameter name	Type	Description
taskId	Int64	Des task taskId Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.

CreateAndAttachNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateAndAttachNetworkInterface) is used to create ENIs and bind CVMs.

- When creating an ENI, you can specify a private IP and can designate a primary IP. The specified private IP must be within the subnet of the ENI and not already in use.
- When creating an ENI, you can specify the number of private IPs to apply for, and the system will generate private IP addresses randomly.
- There is a limit to the number of IP addresses to which an ENI can be bound. For more information on resource restrictions, see ENI Usage Limits.
- When an ENI is created, it can be bound to existing security groups.
- When an ENI is created, it can be bound to tags. The list of tags in the response represents the successfully added tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-30 17:12:07.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateAndAttachNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-m0c2kcun
NetworkInterfaceName	Yes	No	String	ENI name, up to 60 bytes in length. Example: eni-ed3452de
SubnetId	Yes	No	String	Subnet instance ID of the ENI, e.g., subnet-0ap8nwca. Example: subnet-76r802pg
PrivateIpAddresses	No	No	Array of PrivateIpAddressSpecification	Specified VPC IP information, up to 10 can be specified at once. Example:View
SecondaryPrivateIpAddressCount	No	No	Uint64	Number of newly applied private IP addresses. The total number of private IP addresses must not exceed the quota. Example: 1
SecurityGroupIds	No	No	Array of String	Specifies the bound security group, e.g., ['sg-1dd51d']. Example: ['sg-75ww503r']
InstanceId	Yes	No	String	CVM instance ID. Example: ins-demoag78
NetworkInterfaceDescription	No	No	String	ENI description. The name can be given freely but must not exceed 60 characters. Example: uiui
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
NetworkInterface	NetworkInterface	ENI instances. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

CreateNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateNetworkInterface) is used to create ENIs.

- When creating an ENI, you can specify a private IP and can designate a primary IP. The specified private IP must be within the subnet of the ENI and not already in use.
- When creating an ENI, you can specify the number of private IPs to apply for, and the system will generate private IP addresses randomly.
- There is a limit to the number of IP addresses to which an ENI can be bound. For more information on resource restrictions, see ENI Usage Limits.
- When an ENI is created, it can be bound to existing security groups.
- When an ENI is created, it can be bound to tags. The list of tags in the response represents the successfully added tags.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-10-26 02:54:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-0akboI5v
NetworkInterfaceName	Yes	No	String	ENI name, up to 60 bytes in length. Example: demoNIC
NetworkInterfaceDescription	No	No	String	ENI description. The name can be given freely but must not exceed 60 characters. Example: demoDesc
SubnetId	Yes	No	String	Subnet instance ID of the ENI, e.g., subnet-0ap8nwca. Example: subnet-76r802pg
SecondaryPrivateIpAddressCount	No	No	Uint64	Number of newly applied private IP addresses. The total number of private IP addresses must not exceed the quota. Example: 1
SecurityGroupIds	No	No	Array of String	Specifies the bound security group, e.g., ['sg-1dd51d']. Example: ['sg-75ww503r']
PrivateIpAddresses	No	No	Array of PrivateIpAddressSpecification	Specified VPC IP information, up to 10 can be specified at once. Example:View
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
NetworkInterface	NetworkInterface	ENI instances. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Reserved	The parameter value is a reserved object of the system.
InvalidParameterValue.Range	The parameter value is not within the specified range.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DeleteNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNetworkInterface) is used to delete ENIs.

- An ENI cannot be deleted if it has been bound to a CVM.
- To delete a specified ENI, it must be unbound from the child machine first. After deletion, all private IPs on the ENI will be returned.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-04 23:35:51.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-m6dyj72l

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	Des task taskId Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

DescribeNetworkInterfaceLimit

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNetworkInterfaceLimit) is used to query the ENI quota for a CVM instance ID or an ENI ID, returning the ENI quota that the CVM instance or ENI can bind, as well as the IP quota that can be allocated to the ENI.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 20:26:37.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetworkInterfaceLimit
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	CVM instance ID or ENI ID to be queried Example: ins-4lsnc7dz

3. Output Parameters

Parameter name	Type	Description
EniQuantity	Int64	ENI quota Example:

Parameter name	Type	Description
EniPrivateIpAddressQuantity	Int64	IP quota assignable to each ENI Example:
SubEniPrivateIpAddressQuantity	Int64	Quota of IP addresses that can be assigned to each sub-ENI. Example:
ExtendEniQuantity	Uint64	Extended network interface card quantity Example:
ExtendEniPrivateIpAddressQuantity	Uint64	Number of extended network interface card addresses Example:
SubEniQuantity	Uint64	Relay ENI quota. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist

DescribeNetworkInterfaces

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNetworkInterfaces) is used to query the ENI list.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:28:11.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetworkInterfaces
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceIds	No	No	Array of String	ENI instance ID query, e.g., eni-pxir56ns. The upper limit of instances per request is 100. Parameters NetworkInterfaceIds and Filters must not be specified simultaneously. Example: ["eni-kiaim12s"]
Filters	No	No	Array of Filter	Filter criteria. Parameters NetworkInterfaceIds and Filters must not be specified simultaneously. • vpc-id - String - (Filter criteria) VPC instance ID, e.g., vpc-f49l6u0z. • subnet-id - String - (Filter criteria) Subnet instance ID, e.g., subnet-f49l6u0z. • network-interface-id - String - (Filter criteria) ENI instance ID, e.g., eni-5k56k7k7. • attachment.instance-id - String - (Filter criteria) Bound CVM instance ID, e.g., ins-3nqpdn3i. • groups.security-group-id - String - (Filter criteria) Bound security group instance ID, e.g., sg-f9ekbxeq. • network-interface-name - String - (Filter criteria) Network interface card instance name. • network-interface-description - String - (Filter criteria) Network interface card instance description. • address-ip - String - (Filter criteria) Private IPv4 address. • tag-key - String - Required or Not: No - (Filter criteria) Filter by tag key. Refer to example 2 for usage. • tag:tag-key - String - Required or Not: No - (Filter criteria) Filter by tag key-value pair. Replace tag-key with the specific tag key. Refer to example 3 for usage. • is-primary - Boolean - Required or Not: No - (Filter criteria) Filter by whether it is the primary network interface card. When the value is true, filter only the primary network interface card; when the value is false, filter only the auxiliary network interface card; when the filter parameter is not provided, filter both the primary and auxiliary network interface cards. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
NetworkInterfaceSet	Array of NetworkInterface	Instance detail list. Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
UnauthorizedOperation	Unauthorized operation

DescribeNetworkInterfacesEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to query the cross-tenant elastic network interface (ENI) list.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-12-29 00:20:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetworkInterfacesEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceIds	No	No	Array of String	ENI instance ID query, e.g., eni-pxir56ns. The upper limit of instances per request is 100. Parameters NetworkInterfaceIds and Filters must not be specified simultaneously. Example: ["eni-nswq8wkq"]
Filters	No	No	Array of Filter	Filters Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10
VpcAppId	No	No	Int64	The APPID of the VPC user. Example: 1300224712
VpcUin	No	No	String	The UIN of the VPC user. Example: 700000483554
VpcSubAccountUin	No	No	String	The SubAccountUin of the VPC user. Example: 700000483554
Business	No	No	String	The cross-tenant business name, such as TKE or SCF. Example: TKE
BusinessOwner	No	No	String	A business identifier that can uniquely identify a specific business resource. Example: dockerMaster

3. Output Parameters

Parameter name	Type	Description
NetworkInterfaceSet	Array of NetworkInterface	Instance detail list. Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
UnsupportedOperation.UinNotFound	The account ID does not exist.
InvalidParameter.FilterInvalidKey	

Error Code	Description
InternalError.ModuleError	
LimitExceeded.ActionLimited	

DetachNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DetachNetworkInterface) is used to unbind an ENI from a CVM.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-12 19:12:46.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DetachNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-afo43z61
InstanceId	Yes	No	String	CVM instance ID, e.g., ins-r8hr2upy. Example: ins-r8hr2upy

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
taskId	Int64	Des task taskId Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DisassociateNetworkInterfaceSecurityGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisassociateNetworkInterfaceSecurityGroups) is used for an ENI to unbind from a security group. It supports complete unbinding of the ENI from the security group.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-05 00:35:09.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateNetworkInterfaceSecurityGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceIds	Yes	No	Array of String	ENI instance ID, e.g., eni-pxir56ns. The upper limit of instances per request is 100. Example: ["eni-demoag78"]
SecurityGroupIds	Yes	No	Array of String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. The upper limit of instances per request is 100. Example: ["sg-demoag78"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

MigrateNetworkInterface

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (MigrateNetworkInterface) is used for ENI migration.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-12 19:15:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: MigrateNetworkInterface
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-m6dyj72l
SourceInstanceId	Yes	No	String	ID of CVM instance currently bound to the ENI, e.g., ins-r8hr2upy. Example: ins-r8hr2upy
DestinationInstanceId	Yes	No	String	The destination CVM instance ID to migrate. Example: ins-7qs3ou6z

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be

Parameter name	Type	Description
		provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

MigratePrivateIpAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (MigratePrivateIpAddress) is used to migrate a private IP within an ENI.

- This API is to migrate a private IP from one ENI to another. The primary IP address cannot be migrated.
- The ENIs before and after migration must be in the same subnet.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:38:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: MigratePrivateIpAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceNetworkInterfaceId	Yes	No	String	ENI instance ID bound to the private IP, e.g., eni-m6dyj72l. Example: eni-m6dyj722
DestinationNetworkInterfaceId	Yes	No	String	Target ENI instance ID awaiting migration. Example: eni-m6dyj72l
PrivateIpAddress	Yes	No	String	Migrated private IP address, e.g., 10.0.0.6. Example: 10.0.0.6

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnauthorizedOperation.PrimaryIp	The primary IP does not support the specified operation.
UnauthorizedOperation.AttachmentNotFound	The binding relationship does not exist.
ResourceNotFound	The resource does not exist

ModifyIpv6AddressesAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyIpv6AddressesAttribute) is used to modify the private IPv6 address attributes of an ENI.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-04-26 18:34:32.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyIpv6AddressesAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID , e.g., eni-m6dyj72l . Example: eni-m6dyj72l
Ipv6Addresses	Yes	No	Array of Ipv6Address	Designated private IPv6 address information. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs

Parameter name	Type	Description
		to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
UnsupportedOperation.InvalidState	The resource status is invalid.
UnsupportedOperation.AttachmentNotFound	The binding relationship does not exist.

ModifyNetworkInterfaceAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNetworkInterfaceAttribute) is used to modify ENI attributes.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-20 03:54:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetworkInterfaceAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-pxir56ns. Example: eni-afo43z61
NetworkInterfaceName	No	No	String	ENI name, up to 60 bytes in length. Example: NewName
NetworkInterfaceDescription	No	No	String	ENI description. The name can be given freely but must not exceed 60 characters. Example: demo
SecurityGroupIds	No	No	Array of String	Specifies the bound security group, e.g., ['sg-1dd51d']. Example: ['sg-75ww503r']

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyPrivateIpAddressesAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyPrivateIpAddressesAttribute) is used to modify the private IP attributes of an ENI.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-18 04:11:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyPrivateIpAddressesAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-afo43z61
PrivateIpAddresses	Yes	No	Array of PrivateIpAddressSpecification	Specified private IP information. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

UnassignIpv6Addresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (UnassignIpv6Addresses) is used to release ENI IPv6 addresses.

This API is completed asynchronously. To query the result of the asynchronous task, use the RequestId returned by this API to poll the QueryTask API.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-04-26 18:33:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UnassignIpv6Addresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID , e.g., eni-m6dyj72l . Example: eni-9c8zkfev
Ipv6Addresses	Yes	No	Array of Ipv6Address	Specified IPv6 address list. Up to 10 can be specified at once. Example:View

3. Output Parameters

Parameter name	Type	Description
taskId	Int64	Des task taskId Example: 213415
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnauthorizedOperation.PrimaryIp	The primary IP does not support the specified operation.
UnauthorizedOperation.AttachmentNotFound	The binding relationship does not exist.
UnsupportedOperation.InvalidState	The resource status is invalid.
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.

UnassignPrivateIpAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (UnassignPrivateIpAddresses) is used for ENIs to return private IPs.

- After returning the auxiliary private IPs on the ENI, the API will automatically disassociates the EIP. The ENI's primary private IP must not be returned.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-11-16 23:24:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UnassignPrivateIpAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceId	Yes	No	String	ENI instance ID, e.g., eni-m6dyj72l. Example: eni-afo43z61
PrivateIpAddresses	Yes	No	Array of PrivateIpAddressSpecification	Specified VPC IP information, up to 10 can be specified at once. Example:View

3. Output Parameters

Parameter name	Type	Description
taskId	Int64	Des task taskId Example: 213415
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
ResourceNotFound	The resource does not exist

Elastic IP APIs
AllocateAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AllocateAddresses) is used to apply for one or more Elastic IPs (referred to as EIP).

- An EIP is a static IP address designed for dynamic cloud computing. With an EIP, you can quickly remap the EIP to another instance, thereby shielding against instance failures.
- Your EIP is associated with your cloud platform account, not with any particular instance. It remains associated with your cloud platform account until you choose to explicitly release the address or if the account is overdue for more than 24 hours.
- There is a limit on the maximum quota of EIPs that a cloud platform account can apply for in each region, as detailed in the EIP Product Introduction. The aforementioned quota can be obtained through the DescribeAddressQuota API.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-06-24 18:32:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AllocateAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressCount	No	No	Int64	EIP quantity. Default value: 1. Example: 1
InternetServiceProvider	No	No	String	EIP line type. • User with static single-line IP address allowlist enabled. Valid values: • CMCC • CTCC • CUCC Note: Only some regions support static single-line IP addresses. Example: BGP
DedicatedClusterId	No	No	Array of String	Unique CDC ID. Example: cluster-gbo27yc4
InternetChargeType	No	No	String	EIP billing method. Example: TRAFFIC_POSTPAID_BY_HOUR
InternetMaxBandwidthOut	No	No	Int64	EIP bandwidth limit, unit: Mbps. • For users on the bandwidth uplift allowlist, the value range depends on the EIP billing method: • BANDWIDTH_PACKAGE: from 1 Mbps to 1000 Mbps • BANDWIDTH_POSTPAID_BY_HOUR: from 1 Mbps to 100 Mbps • TRAFFIC_POSTPAID_BY_HOUR: from 1 Mbps to 100 Mbps Default value: 1 Mbps. • For users not on the bandwidth uplift allowlist, the EIP bandwidth limit depends on the public network bandwidth limit of the instance it's bound to. This parameter is not required. Example: 10
AddressChargePrepaid	No	No	AddressChargePrepaid	Billing cycle, required in case of prepaid mode. Example:View
DealId	No	No	String	Order ID, internal parameters. Example: 20200609000000528579909840049393
AddressType	No	No	String	EIP type. Default value: EIP. Example: AnycastEIP
Zone	No	No	String	EIP availability zone, used to specify the availability zone to apply for EIP. Example: ap-region-1
ZoneName	No	No	String	EIP availability zone, used to specify the availability zone to apply for EIP. Example:
VipCluster	No	No	Array of String	Specifies IP address to apply for EIP. Each account has a quota of three times per month. Example: ['10.0.0.5']
Tags	No	No	Array of Tag	List of tags to associate. Example:View
BandwidthPackageId	No	No	String	Unique ID parameter for the BGP bandwidth package. Setting this parameter and having InternetChargeType as BANDWIDTH_PACKAGE indicate that the created EIP will join this BGP bandwidth package and adopt the bandwidth package billing mode. Example: bwp-6jnvlsv4

3. Output Parameters

Parameter name	Type	Description
AddressSet	Array of String	List of unique IDs for requested EIPs. Example: ["eip-m44ku5d2"]
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: 61531428
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
AddressQuotaLimitExceeded	Insufficient account quota. Each account can create up to 20 EIPs in each region.
AddressQuotaLimitExceeded.DailyAllocate	Insufficient purchase attempts. The number of daily subscriptions for each account in each region is twice the quota.

AssociateAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssociateAddress) is used to bind EIPs to a specified private IP on an instance or ENI.

- Binding an EIP to an instance (CVM) essentially indicates binding the EIP to the primary private IP of the primary network interface card on the instance.
- Binding an EIP to the primary private IP of the primary network interface card will automatically unbind and release a normal public IP that was previously bound.
- Binding an EIP to a specified network interface card's private IP (not the primary network interface card's primary private IP) requires unbinding the EIP first before binding it anew.
- To bind an EIP to a NAT gateway, use the API [AssociateNatGatewayAddress](../NAT Gateway APIs/AssociateNatGatewayAddress).
- An EIP that is overdue or blocked cannot be bound.
- Only EIPs in the UNBIND state can be bound.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-06-24 00:16:26.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssociateAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressId	Yes	No	String	The unique ID identifying the EIP, such as `eip-jrkzpvgt`. Example: eip-ek0cdz1g
InstanceId	No	No	String	The ID of the instance to be bound. The instance ID is in the format `ins-jrkzpvgt`. You can retrieve it by logging in to the Console or through the `InstanceId` returned by the DescribeInstances API. Example: ins-1bmpb9tu
NetworkInterfaceId	No	No	String	The ID of the ENI to be bound. The ENI ID is in the format `eni-jrkzpvgt`. The parameters `NetworkInterfaceId` and `InstanceId` cannot be specified simultaneously. You can query the ENI ID by logging in to the console or from the `networkInterfaceId` field in the response of the DescribeNetworkInterfaces API. Example: eni-jyhoac61
PrivateIpAddress	No	No	String	Private IP to be bound. If `NetworkInterfaceId` is specified, `PrivateIpAddress` must also be specified, indicating that the EIP will be bound to the specified private IP of the ENI. Also, ensure that the specified `PrivateIpAddress` is a private IP on the given `NetworkInterfaceId`. The specified ENI's private IP can be queried by logging into the console, or obtained from the `privateIpAddress` returned by the DescribeNetworkInterfaces API. Example: 10.0.0.120

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: 501251411
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InvalidAddressId.Blocked	The designated EIP is in a blocked state. Binding operation cannot be performed while the EIP is blocked. Unbinding is required first.
InvalidAddressIdState.InArrears	The specified EIP is in arrears state.
InvalidAddressId.Blocked	The designated EIP is in a blocked state. Binding operation cannot be performed while the EIP is blocked. Unbinding is required first.
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidAddressIdStatus.NotPermit	The current status of the designated EIP does not allow for binding operation. Binding operation can only be performed when the EIP's status is UNBIND.
InvalidInstance.NotSupported	The instance is not supported.
InvalidInstanceId.AlreadyBindEip	The specified instance has already been bound with an EIP. The current EIP must be unbound before another binding operation can be performed.
InvalidNetworkInterfaceId.NotFound	The specified NetworkInterfaceId does not exist or the specified PrivateIpAddress is not on the NetworkInterfaceId.
InvalidParameterConflict	The specified two parameters conflict with each other and can not coexist. An EIP can only be bound to an instance or a specified private network IP of a designated network interface.
InvalidPrivateIpAddress.AlreadyBindEip	The specified private IP of the specified ENI has already been bound to an EIP. It cannot be bound again.
MissingParameter	Missing parameters. The request did not carry the required parameter.
MissingResourceId	Missing bound entity. Either InstanceId, NetworkInterfaceId, or PrivateIpAddress must be specified.

DescribeAddressQuota

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAddressQuota) is used to inquire about the quota information of your account's [EIP] (/tcloud/Compute/CVM/292128/661327/nasinfo_flexpnip) in the current region. For details on quota, see EIP Product Introduction.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-12-28 23:52:43.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAddressQuota
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
QuotaSet	Array of Quota	Account EIP quota information. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

DescribeAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAddresses) is used to query the details of one or more EIPs.

- If the parameter is null, it returns a certain number (as specified by Limit, 20 by default) of EIPs for the current user.

Default interface request rate limit: 10 times per second.

Interface update time: 2023-01-07 03:39:59.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressIds	No	No	Array of String	A list of unique IDs identifying the EIPs. Each EIP unique ID is in the format eip-jrkzpvgt . The parameters AddressIds and Filters cannot be specified simultaneously. Example: eip-jrkzpvgt
Filters	No	No	Array of Filter	Each request can include up to 10 Filters , with a maximum of 5 values for each Filter.Values . The parameters AddressIds and Filters cannot be specified simultaneously. Detailed filtering conditions are as follows: • address-id - String - required or not: no - (filtering condition) filters by the unique ID of the EIP. The EIP unique ID is in the format eip-jrkzpvgt. • dedicated-cluster-id - String - required or not: no - (filtering condition) filters by the unique ID of the CDC. The CDC unique ID is in the format cluster-jrkzpvgt. • address-name - String - required or not: no - (filtering condition) filters by the name of the EIP. Fuzzy filtering is not supported. • address-ip - String - required or not: no - (filtering condition) filters by the IP address of the EIP. • address-status - String - required or not: no - (filtering condition) filters by the status of the EIP. Possible statuses include 'CREATING', 'BINDING', 'BIND', 'UNBINDING', 'UNBIND', 'OFFLINING', and 'BIND_ENI'. • instance-id - String - required or not: no - (filtering condition) filters by the instance ID bound to the EIP. The instance ID is in the format ins-jrkzpvgt. • private-ip-address - String - required or not: no - (filtering condition) filters by the private IP address bound to the EIP. • network-interface-id - String - required or not: no - (filtering condition) filters by the ENI ID bound to the EIP. The ENI ID is in the format eni-jrkzpvgt. • is-arrears - String - required or not: no - (filtering condition) filters by whether the EIP is in arrears. (TRUE: The EIP is in arrears
Offset	No	No	Int64	The offset, with a default value of 0. For more details about Offset , see the relevant section in the API introduction. Example: 0
Limit	No	No	Int64	The number of returned results, with a default value of 20 and a maximum value of 100. For more details about Limit , see the relevant section in the API Overview. Example: 20
ContainsCdc	No	No	Array of String	Whether the query results should include EIP information within the CDC. ALL : Include all EIPs. NO_CDC : Exclude EIPs within the CDC. ONLY_CDC : Include only EIPs within the CDC. Example: ALL

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible EIPs. Example:
AddressSet	Array of Address	EIP detail list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DescribeNetworkInterfaceExtendIps

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Obtain the expanded IP of an ENI

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 20:24:33.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetworkInterfaceExtendIps
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkInterfaceIds	Yes	No	Array of String	List of Unique IDs of ENIs Example: ['eni-hhabo1ev']
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of rows per page, 100 by default. Example: 20

3. Output Parameters

Parameter name	Type	Description
NetworkInterfaceExtendIpSet	Array of NetworkInterfaceExtendIp	Return the extended IP range Example:View
TotalCount	Uint64	Returned total entries Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist

DescribeTaskResult

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the execution result of an EIP async task

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-31 19:22:34.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTaskResult
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
TaskId	No	No	Uint64	Asynchronous task ID. Either TaskId or DealName must be provided. Example: jkt456
DealName	No	No	String	Billing order number. Either TaskId or DealName is required. Example: 20241017224547

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Task ID Example: jkt456
Result	String	Execution result, including SUCCESS, FAILED and RUNNING Example: 234566
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DisassociateAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisassociateAddress) is used to unbind EIPs.

- Supports unbinding of EIPs on CVM instances and ENI.
- Unbinding of EIPs on NAT is not supported. For unbinding EIPs on NAT, refer to [DisassociateNatGatewayAddress] (../NAT Gateway APIs/DisassociateNatGatewayAddress).
- Only EIPs in the BIND and BIND_ENI states can be unbound.
- If an EIP is blocked, it cannot be unbound.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-06-24 01:44:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressId	Yes	No	String	The unique ID identifying the EIP, such as eip-jrkzpvgt . Example: eip-ek0cdz1g

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: 61531411

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InvalidParameter	Invalid input parameters.
InvalidAddressId.Blocked	The designated EIP is in a blocked state. Binding operation cannot be performed while the EIP is blocked. Unbinding is required first.
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidAddressIdStatus.NotPermit	The current status of the designated EIP does not allow for binding operation. Binding operation can only be performed when the EIP's status is UNBIND.
InvalidInstance.NotSupported	The instance is not supported.

ModifyAddressAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyAddressAttribute) is used to modify the names of EIPs.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-06-18 23:01:43.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAddressAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressId	Yes	No	String	The unique ID identifying the EIP, such as eip-jrkzpvgt . Example: eip-p2x6wxc0
AddressName	No	No	String	EIP name after modification, up to 20 characters in length. Example: demo_eip

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

ModifyAddressesBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyAddressesBandwidth) is used to adjust the bandwidth of EIPs, including postpaid EIPs, prepaid EIPs, and bandwidth package EIPs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-18 01:40:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAddressesBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressIds	Yes	No	Array of String	Unique EIP ID, e.g., eip-xxxx. Example: ["eip-alfxy9c8"]
InternetMaxBandwidthOut	Yes	No	Int64	Adjust bandwidth target value Example: 2
StartTime	No	No	Datetime	Start Time of Monthly Subscription Example: 2021-07-20 00:00:00
EndTime	No	No	Datetime	Monthly subscribed bandwidth end time Example: 2021-07-20 00:00:00

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: 11531422
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

ModifyNetworkInterfaceExtendIp

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the extended IP of ENI

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-13 04:53:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetworkInterfaceExtendIp
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Unique ID of VPC Example: vpc-67wlqf6v
NetworkInterfaceId	Yes	No	String	Unique ID of ENI Example: eni-67wlqf6v
Ips	No	No	Array of String	Extended IP list Example: 10.0.0.7

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameter	Invalid input parameters.
UnauthorizedOperation	Unauthorized operation

ReleaseAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ReleaseAddresses) is used to release one or more EIPs.

- This operation is irreversible, and the IP address associated with the EIP will no longer belong to you after release.
- Only EIPs in the UNBIND state can be released.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-06-18 01:36:21.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ReleaseAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressIds	Yes	No	Array of String	A list of unique IDs identifying the EIPs. Each EIP unique ID is in the format eip-jrkzpvgt . Example: ["eip-gzc5rgr2"]

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: jkt31420
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidAddressState	The current status of the specified EIP does not allow this operation.

TransformAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (TransformAddress) is used to translate an instance's regular public IP into an EIP.

- The platform limits the number of times to unbind EIP and re-allocate regular public IPs per day per user per region (see EIP Product Introduction). The above quota can be obtained through the API [DescribeAddressQuota](../Elastic IP APIs/DescribeAddressQuota).

Default interface request rate limit: 10 times per second.

Interface update time: 2025-09-17 12:06:11.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: TransformAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	The instance ID with the public IP address to be operated on. The instance ID is in the format ins-jrkzpvgt . You can retrieve it by logging in to the Console or through the InstanceId returned by the DescribeInstances API. Example: ins-3ea0qeu6

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	Task ID Example: 21
AddressId	String	Resource ID Example: eip-s6c9f6r7
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
AddressQuotaLimitExceeded	Insufficient account quota. Each account can create up to 20 EIPs in each region.
AddressQuotaLimitExceeded.DailyAllocate	Insufficient purchase attempts. The number of daily subscriptions for each account in each region is twice the quota.
InvalidInstance.NotSupported	The instance is not supported.

Elastic IPv6 APIs
AllocateIp6AddressesBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used for the initial allocation of public network bandwidth to an IPv6 address.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-02 18:06:31.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AllocateIp6AddressesBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6Addresses	Yes	No	Array of String	IPv6 address for which public network access is required. Example: 2402:4e00:1011:9b02:0:98e8:f0fd:3a85
InternetMaxBandwidthOut	No	No	Int64	Bandwidth, in Mbps. The default value is 1 Mbps. Example: 50
InternetChargeType	No	No	String	Network billing mode. IPV6 currently supports TRAFFIC_POSTPAID_BY_HOUR. The default is TRAFFIC_POSTPAID_BY_HOUR. Example: TRAFFIC_POSTPAID_BY_HOUR
BindResourceType	No	No	String	Binding resource type. Valid values: BIND_BMS: indicates BMS IPv6; BIND_INSTANCE_OR_EIP indicates instance IPv6. Example: BIND_BMS

3. Output Parameters

Parameter name	Type	Description
AddressSet	Array of String	Unique ID list of EIP IPv6. Example: eip-68dqs5ri
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: 194395704
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InternalServerError	Internal operation error.

DescribeIp6Addresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to query the IPv6 address information.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-03 07:43:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIp6Addresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6AddressIds	No	No	Array of String	A list of unique IDs identifying IPv6. Each IPv6 unique ID is in the format eip-jrkzpvgt . The parameters Ip6AddressIds and Filters cannot be specified simultaneously. Example: eip-37xao8t
Filters	No	No	Array of Filter	For each request, the upper limit is 10 for Filters and 5 for Filter.Values . Parameters AddressIds and Filters cannot be specified at the same time. Detailed filtering conditions are as follows: • address-ip - String - Required: No - (Filtering condition) Filter by EIP. • network-interface-id - String - Required: No - (Filtering condition) Filter by unique ENI ID. • bind-resource-type - String - Required: No - (Filtering condition) Filter by bound resource type. BIND_BMS: bound to the IPv6 address of a BMS instance; BIND_INSTANCE_OR_EIP: bound to the IPv6 address of a CVM instance or an ENI. Example:View
Offset	No	No	Int64	The offset, with a default value of 0. For more details about Offset , see the relevant section in the API introduction. Example: 10
Limit	No	No	Int64	The number of returned results, with a default value of 20 and a maximum value of 100. For more details about Limit , see the relevant section in the API Overview. Example: 10

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible IPv6. Example:
AddressSet	Array of Address	IPv6 details list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InternalServerError	Internal operation error.
InvalidAddressId.NotFound	The specified EIP does not exist.

ModifyIp6AddressesBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify the bandwidth of IPv6 address access to the internet.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-02 17:38:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyIp6AddressesBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6Addresses	No	No	Array of String	IPv6 address. Either Ip6Addresses or Ip6AddressId must be provided, and only 1 parameter can be provided. Example: ["2402:4e00:1000:200:0:8d8a:60b7:87f8"]
Ip6AddressIds	No	No	Array of String	The unique ID corresponding to the IPv6 address, such as eip-37xao8t. Either Ip6Addresses or Ip6AddressId should be passed in, but not both. Example: ["eip-6kr6f42w"]
InternetMaxBandwidthOut	Yes	No	Int64	Modified target bandwidth, in Mbps. Example: 50

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 53734868
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidAddressIdState.InArrears	The specified EIP is in arrears state.
InternalServerError	Internal operation error.
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidAccount.NotSupported	This account is not supported.

ReleaseIp6AddressesBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to release bandwidth for elastic IPv6 addresses.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-02 18:05:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ReleaseIp6AddressesBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6Addresses	No	No	Array of String	IPv6 address. Only one of Ip6Addresses and Ip6AddressIds must and can be provided. Example: 2402:4e00:1205:8c00:0:9835:2940:98d3
Ip6AddressIds	No	No	Array of String	The unique ID corresponding to the IPv6 address, such as eip-37xao8t. Either Ip6Addresses or Ip6AddressIds should be passed in, but not both. Example: eip-demoag78

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous task TaskId. The task status can be queried using the DescribeTaskResult API. Example: jkt
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InternalServerError	Internal operation error.

Gateway Traffic Monitoring APIs DescribeGatewayFlowQos

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeGatewayFlowQos) is used to query the gateway access IP traffic control bandwidth.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:44:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeGatewayFlowQos
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
GatewayId	Yes	No	String	Gateway instance ID. Currently we support the following gateway instance types, Direct Connect gateway instance ID, e.g., dcg-ltjahce6; NAT gateway instance ID, e.g., nat-ltjahce6; VPN gateway instance ID, e.g., vpn-ltjahce6. Example: vpngw-4je9dgin
IpAddresses	No	No	Array of String	Rate limited CVM's private IP. Example: 10.0.0.12
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
GatewayQosSet	Array of GatewayQos	Instance detail list. Example:View

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

DisableGatewayFlowMonitor

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisableGatewayFlowMonitor) is used to disable gateway traffic monitoring.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:43:46.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisableGatewayFlowMonitor
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
GatewayId	Yes	No	String	Gateway instance ID. Currently we support the following gateway instance types, Direct Connect gateway instance ID, e.g., dcg-ltjahce6; NAT gateway instance ID, e.g., nat-ltjahce6; VPN gateway instance ID, e.g., vpn-ltjahce6. Example: vpngw-gree226l

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

Error Code	Description
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

EnableGatewayFlowMonitor

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (EnableGatewayFlowMonitor) is used to enable gateway traffic monitoring.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:43:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableGatewayFlowMonitor
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
GatewayId	Yes	No	String	Gateway instance ID. Currently we support the following gateway instance, Direct Connect gateway instance ID, e.g., dcg-ltjahce6; NAT gateway instance ID, e.g., nat-ltjahce6; VPN gateway instance ID, e.g., vpn-ltjahce6. Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

ModifyGatewayFlowQos

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyGatewayFlowQos) is used to adjust the gateway traffic control bandwidth.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:44:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyGatewayFlowQos
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
GatewayId	Yes	No	String	Gateway instance ID. Currently we support the following gateway instance types, Direct Connect gateway instance ID, e.g., dcg-ltjahce6; NAT gateway instance ID, e.g., nat-ltjahce6; VPN gateway instance ID, e.g., vpn-ltjahce6. Example: vpngw-gree226l
Bandwidth	Yes	No	Uint64	Traffic control bandwidth value. Example: 10
IpAddresses	Yes	No	Array of String	Rate limited CVM's private IP. Example: 10.0.0.2

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

High Availability Virtual IP APIs
CreateHaVip

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateHaVip) is used to create a HAVIP.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-26 04:15:21.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateHaVip
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC ID of HAVIP. Example: vpc-6v2ht8q5
SubnetId	Yes	No	String	Subnet ID of HAVIP. Example: subnet-qq51iwr4
HaVipName	Yes	No	String	HAVIP name. Example: demo+name
Vip	No	No	String	Specifies a virtual IP address, which must fall under the VPC IP range and must not be occupied. If not specified, it will be automatically allocated. Example: 10.4.6.15

3. Output Parameters

Parameter name	Type	Description
HaVip	HaVip	HAVIP object. Example:View
IsCdc	Uint64	Whether it is a CDC type HAVIP. Example:
CheckAssociate	Bool	Whether HAVIP drift range verification is enabled. Example:
FlushedTime	String	HAVIP refresh time. This parameter is used only as an output parameter. The refresh of FlushTime will be triggered by the following scenarios: (1) The instance sends a gratuitous ARP to trigger HAVIP drift. (2) Manually unbind the HAVIP from the ENI. The default value is 0000-00-00 00:00:00 when there is no update. Example:
Visible	Bool	Whether the HAVIP is visible to the tenant. Example:
CdcId	String	CDC instance ID. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

DeleteHaVip

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteHaVip) is used to delete HAVIP.

This API is completed asynchronously. To query the execution results of asynchronous tasks, use the RequestId returned by this API to poll the QueryTask API.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-10-20 18:02:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteHaVip
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HaVipId	Yes	No	String	Unique ID of HAVIP , e.g., havip-9o233uri . Example: havip-9o233uri

3. Output Parameters

Parameter	Type	Description

name		
taskId	Int64	Des task taskId Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeHaVips

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeHaVips) is used to query the list of high availability virtual IPs (HAVIPs).

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-15 19:35:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHaVips
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	Yes	Uint64	Offset. 0 by default. Example: 0
Limit	No	Yes	Uint64	Number of returns, 20 by default, up to 100. Example: 20
Business	No	Yes	String	Product workload name. For example, TKE, SCF, or NFV. Example: NFV
IpAddressType	No	Yes	String	Protocol type. Valid values: Ipv4 and Ipv6. Default value: Ipv4. Example: Ipv4
HaVipIds	No	Yes	Array of String	Unique ID of HAVIP , e.g., havip-9o233uri . Example: ["havip-bk4275i0","havip-2kce8v4q"]
Filters	No	Yes	Array of Filter	Filtering conditions. The parameters HaVipIds and Filters cannot be specified at the same time. • havip-id - String - Unique ID of HAVIP . For example, havip-9o233uri . • havip-name - String - Name of HAVIP . • vpc-id - String - VPC ID of HAVIP . • subnet-id - String - Subnet ID of HAVIP . • vip - String - VIP address of HAVIP . • address-ip - String - Elastic IP address (EIP) bound to HAVIP . • havip-association.instance-id - String - Instance or ENI bound to HAVIP . • havip-association.instance-type - String - Type of the object bound to HAVIP . Valid values: CVM and ENI. • check-associate - Bool - Whether to verify the bound instance or ENI when HAVIP switch is enabled. • cdc-id - String - CDC instance ID. Example:View

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example: 1
HaVipSet	Array of HaVip	HAVIP object array. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InvalidParameter.FilterInvalidKey	
InternalError.ModuleError	

HaVipAssociateAddressIp

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (HaVipAssociateAddressIp) is used for HAVIP to bind EIP

This API is completed asynchronously. To query the execution results of asynchronous tasks, use the RequestId returned by this API to poll the QueryTask API.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-10-20 18:04:24.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: HaVipAssociateAddressIp
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HaVipId	Yes	No	String	Unique ID of HAVIP, e.g., havip-9o233uri. It must be a HAVIP that has not been bound to an EIP. Example: havip-9o233uri
AddressIp	Yes	No	String	Public IP, which must be an EIP not bound to HAVIP Example: 119.29.93.218

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.BindEIP	An EIP is already bound.

HaVipDisassociateAddressIp

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (HaVipDisassociateAddressIp) is used to disassociate the EIPs that have been bound to a HAVIP.

This API is completed asynchronously. To query the result of the asynchronous task, use the RequestId returned by this API to poll the QueryTask API.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-10-20 18:04:48.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: HaVipDisassociateAddressIp
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HaVipId	Yes	No	String	Unique ID of HAVIP, e.g., havip-9o233uri. It must be a HAVIP that has been bound to an EIP. Example: havip-9o233uri

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.UnbindEIP	No EIP is bound.

ModifyHaVipAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyHaVipAttribute) is used to modify the attributes of HAVIP.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-10-12 03:49:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyHaVipAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HaVipId	Yes	No	String	Unique ID of HAVIP , e.g., havip-9o233uri . Example: havip-9o233uri
HaVipName	Yes	No	String	HAVIP name, which can be named arbitrarily, but must not exceed 60 characters. Example: demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

IPv6 Translation Service APIs
AddIp6Rules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

1. This API is used to add IPv6 translation rules to a translation instance.
2. It supports adding translation rules in batch under the same translation instance, with a maximum of 50 rules per account in a region.
3. A complete translation rule includes vip6:vport6:protocol:vip:vport, where vip6:vport6:protocol must be unique.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-04 03:29:14.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AddIp6Rules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorId	Yes	No	String	The unique ID of the IPv6 translation instance, such as ip6-37xao8t. Example: ip6-90pt7p9q
Ip6RuleName	No	No	String	Name of IPV6 Translation Rules Example: "IPv6 Rule1"
Ip6RuleInfos	Yes	No	Array of Ip6RuleInfo	IPv6 Translation Rule Information Example:View

3. Output Parameters

Parameter name	Type	Description
Ip6RuleSet	Array of String	Unique ID array of the IPv6 translation rule, such as rule6-7v3vwgec. Example: ["rule6-f3se1mki"]

Parameter name	Type	Description
TaskId	String	TaskId, used by O&M, without any actual business meaning Example: 481e9b6e-81d1-4859-b8cf-a673e010b388
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InternalServerError	Internal operation error.

CreateIp6Translators

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

1. This API is used to create IPv6 to IPv4 translation instances, supporting batch operations.
2. A single account is allowed to create up to 10 translation instances in one region.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-05-22 19:39:48.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateIp6Translators
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorName	No	No	String	Translation instance name Example: "www_lakalakk"
Ip6TranslatorCount	No	No	Int64	Number of translation instances to be created, 1 by default. Example: 1
Ip6InternetServiceProvider	No	No	String	Translation instance ISP attribute, which can be "CMCC", "CTCC", "CUCC", and "BGP". Example: "BGP"
IdcList	Yes	No	Array of String	IDC of Created Translation Instance Example: idc-shxdq123

3. Output Parameters

Parameter name	Type	Description
Ip6TranslatorSet	Array of String	An array of unique IDs for the translation instances, such as ip6-37xao8t. Example:
TaskId	String	TaskId, used by O&M, without any actual business meaning Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

DeleteIp6Translators

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

1. This API is used to release IPv6 translation instances and supports batch operations.
2. If an IPv6 translation instance has translation rules, they will be deleted as well.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-01-25 00:01:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteIp6Translators
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorIds	Yes	No	Array of String	The unique ID of the IPv6 translation instance to be released, such as ip6-37xao8t. Example: ip6-demoag78

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous Task ID Example: 93662
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

Error Code	Description
InternalServerError	Internal operation error.

DescribeIp6TranslatorQuota

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the quota of IPv6 translation instances and rules for the account in the specified region.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-12-05 20:13:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIp6TranslatorQuota
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorIds	No	No	Array of String	The list of unique IDs for the IPv6 translation instances to be queried, such as ip6-37xao8t. Example: ip6-demoag78

3. Output Parameters

Parameter name	Type	Description
QuotaSet	Array of Quota	The IPv6 translation instance and rule quota information for the account in the specified region. The QUOTAID attribute, identified as TOTAL_TRANSLATOR_QUOTA, represents the IPv6 translation instance quota information for the account in the specified region. The QUOTAID attribute, which is the unique ID of the IPv6 translation instance (such as ip6-37xao8t), indicates the quota for the translation rules that can be created under that specific instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

DescribeIp6Translators

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

1. This API is used to query the IPv6 translation instances under the account and their bound translation rule information.
2. Filter queries are supported.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-01-24 23:59:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIp6Translators
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorIds	No	No	Array of String	An array of unique IDs for IPv6 translation instances, such as ip6-37xao8t. Example: ip6-demoag78
Filters	No	No	Array of Filter	The upper limit per request is 10 for Filters, and 5 for Filter.Values. Parameters Ip6TranslatorIds and Filters must not be specified simultaneously. Detailed filter criteria are as follows: • ip6-translator-id - String - Required or Not: No - (Filter criteria) Filter by the unique ID of the IPv6 translation instance, e.g., ip6-xxxxxxx. • ip6-translator-vip6 - String - Required or Not: No - (Filter criteria) Filter by IPv6 address. Fuzzy filtering is not supported. • ip6-translator-name - String - Required or Not: No - (Filter criteria) Filter by the name of the IPv6 translation instance. Fuzzy filtering is not supported. • ip6-translator-status - String - Required or Not: No - (Filter criteria) Filter by the status of the IPv6 translation instance. The status values are CREATING, RUNNING, DELETING, and MODIFYING. Example:View
Offset	No	No	Int64	The offset, with a default value of 0. For more details about Offset , see the relevant section in the API introduction. Example: 0
Limit	No	No	Int64	The number of returned results, with a default value of 20 and a maximum value of 100. For more details about Limit , see the relevant section in the API Overview. Example: 1

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of IPv6 translation instances that meet the filtering criteria. Example:
Ip6TranslatorSet	Array of Ip6Translator	Eligible IPv6 translation instance details Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

ModifyIp6Rule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify IPv6 translation rules, currently only supporting modification of the translation rule name, IPv4 address, and IPv4 port number.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-01-25 01:40:59.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyIp6Rule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorId	Yes	No	String	The unique ID of the IPv6 translation instance, such as ip6-37xao8t. Example: ip6-90pt7p9q
Ip6RuleId	Yes	No	String	Unique ID of the IPv6 translation rule, such as rule6-7v3vwgec. Example: rule6-7v3vwgec
Ip6RuleName	No	No	String	Modified Name for IPv6 Translation Rules Example: "rule_name"
Vip	No	No	String	IPv4 address after modification of IPv6 translation rules Example: 100.192.3.9
Vport	No	No	Int64	IPv4 port number after modification of the IPv6 translation rules Example: 77

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

ModifyIp6Translator

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify IPv6 translation instance attributes, currently only supporting modification of instance name.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-01-25 01:26:31.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyIp6Translator
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorId	Yes	No	String	The unique ID of the IPv6 translation instance, such as ip6-37xao8tx. Example: ip6-demoag78
Ip6TranslatorName	No	No	String	Modified Name of IPv6 Translation Instance Example: demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

RemoveIp6Rules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

1. This API is to delete IPv6 translation rules.
2. It supports the batch deletion of multiple translation rules under the same translation instance.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-01-25 00:03:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RemoveIp6Rules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Ip6TranslatorId	Yes	No	String	The unique ID of the IPv6 translation instance to which the translation rule belongs, such as ip6-37xao8t. Example: ip6-ma6nzj9n
Ip6RuleIds	Yes	No	Array of String	The IPv6 translation rule to be deleted, such as rule6-7v3vwgec. Example: rule6-c1kjyfup

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Asynchronous Task ID Example: 93662
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

NAT Gateway APIs
AssociateNatGatewayAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssociateNatGatewayAddress) is used to bind an EIP to a NAT gateway.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 17:58:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssociateNatGatewayAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-mdbjfr0y
AddressCount	No	No	Uint64	Number of EIPs to apply for. The system will produce N EIPs according to your request. At least either AddressCount or PublicAddresses must be input. Example: 1
PublicIpAddresses	No	No	Array of String	Array of elastic IPs bound to NAT gateway, where either AddressCount or PublicAddresses must be provided. Example: ["139.199.232.212\n"]
Zone	No	No	String	EIP availability area, input when EIP is automatically allocated. Example: ap-region-2

3. Output Parameters

Parameter name	Type	Description
taskId	Int64	Des task taskId Example: 213415
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied
ResourceInUse.Address	The specified IP address is already in use.
UnsupportedOperation.InvalidState	The resource status is invalid.
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.
LimitExceeded.PublicIpAddressPerNatGatewayLimitExceeded	The number of elastic IPs bound to the NAT gateway has exceeded the upper limit.
UnsupportedOperation.PublicIpAddressIsNotExisted	The elastic IP bound to the NAT gateway does not exist.
UnsupportedOperation	Operation unsupported.

CreateNatGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateNatGateway) is used to create NAT gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-11-13 02:54:07.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNatGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayName	Yes	No	String	NAT gateway name Example: demo_name
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-rkzpefgh
InternetMaxBandwidthOut	No	No	Uint64	Maximum public bandwidth of a NAT gateway (unit: Mbps), which can be 20, 50, 100, 200, 500, 1000, 2000, and 5000. Default: 100 Mbps. Example: 10
MaxConcurrentConnection	No	No	Uint64	NAT gateway concurrent connection limit, supported values: 1000000, 3000000, and 10000000. The default value is 100000. Example: 1000000
AddressCount	No	No	Uint64	Number of EIPs to apply for. The system will produce N EIPs according to your request. At least either AddressCount or PublicAddresses must be input. Example: 1
PublicIpAddresses	No	No	Array of String	Array of elastic IPs bound to NAT gateway, where either AddressCount or PublicAddresses must be provided. Example: ["139.199.232.119"]
Zone	No	No	String	Availability zone. For example, ap-region-1 . Example: ap-region-1
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View
InternetServiceProvider	No	No	String	ISP type Example: BGP

3. Output Parameters

Parameter name	Type	Description
NatGatewaySet	Array of NatGateway	NAT gateway object array. Example:View
TotalCount	Uint64	Number of eligible NAT gateway objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidVpcId.Malformed	Invalid VPC. The VPC instance ID is invalid.
InvalidVpcId.NotFound	Invalid VPC. The VPC resource does not exist.
InvalidParameter	Invalid input parameters.
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
UnsupportedOperation.InvalidState	The resource status is invalid.
AddressQuotaLimitExceeded	Insufficient account quota. Each account can create up to 20 EIPs in each region.
InternalServerError	Internal operation error.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

Error Code	Description
InvalidAddressState	The current status of the specified EIP does not allow this operation.
UnsupportedOperation.InsufficientFunds	Insufficient account balance
ResourceInUse.Address	The specified IP address is already in use.
ResourceNotFound	The resource does not exist
InvalidAccount.NotSupported	This account is not supported.
LimitExceeded.NatGatewayPerVpcLimitExceeded	The number of NAT gateways created by VPC has exceeded the upper limit.
LimitExceeded.PublicIpAddressPerNatGatewayLimitExceeded	The number of elastic IPs bound to the NAT gateway has exceeded the upper limit.
UnsupportedOperation.PublicIpAddressIsNotExisted	The elastic IP bound to the NAT gateway does not exist.
UnsupportedOperation.PublicIpAddressIsNotBGPIp	The elastic IP address bound to NAT gateway is not an IP of BGP attribute.
UnsupportedOperation.PublicIpAddressNotBilledByTraffic	The elastic IP bound to the NAT gateway is not charged by traffic.

CreateNatGatewayDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateNatGatewayDestinationIpPortTranslationNatRule) is used to create NAT gateway port forwarding rules.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:02:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNatGatewayDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-3isn9hr0
DestinationIpPortTranslationNatRules	Yes	No	Array of DestinationIpPortTranslationNatRule	The NAT gateway's port translation rules. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

CreateNatGatewaySourceIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateNatGatewaySourceIpTranslationNatRule) is used to create NAT gateway SNAT rules.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-08-30 23:20:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNatGatewaySourceIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., "nat-df45454". Example: nat-3isn9hr0
SourceIpTranslationNatRules	Yes	No	Array of SourceIpTranslationNatRule	NAT gateway SNAT translation rules Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

Error Code	Description
LimitExceeded	Exceeded the limit
UnknownParameter	Unknown parameter error
UnsupportedOperation	Operation unsupported.
MissingParameter	Missing parameters. The request did not carry the required parameter.
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.
UnsupportedOperation.UnbindEIP	No EIP is bound.
UnsupportedOperation	Operation unsupported.

DeleteNatGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNatGateway) is used to delete NAT gateways.
After the NAT gateway is deleted, the system will automatically delete route entries in the routing table that contain the NAT gateway, and will also unbind the EIPs.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:00:04.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNatGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-ig8xpno8

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
taskId	Int64	Des task taskId Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

DeleteNatGatewayDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNatGatewayDestinationIpPortTranslationNatRule) is used to delete the NAT gateway port forwarding rules.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:03:08.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNatGatewayDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-3isn9hr0
DestinationIpPortTranslationNatRules	Yes	No	Array of DestinationIpPortTranslationNatRule	The NAT gateway's port translation rules. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DeleteNatGatewaySourceIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNat GatewaySourceIpTranslationNatRule) is used to delete the SNAT forwarding rules of NAT gateway port.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-08-30 23:24:11.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNatGatewaySourceIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-3isn9hr0
NatGatewaySnatIds	Yes	No	Array of String	SNAT ID list of NAT gateway, e.g., snat-df43254 . Example: ["snat-3ixd0hr0\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
UnknownParameter	Unknown parameter error
UnsupportedOperation	Operation unsupported.
MissingParameter	Missing parameters. The request did not carry the required parameter.
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.

DescribeNatGatewayDestinationIpPortTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNat GatewayDestinationIpPortTranslationNatRules) is used to query the NAT gateway port forwarding rule object array.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:03:25.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNatGatewayDestinationIpPortTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayIds	No	No	Array of String	NAT gateway ID. Example: ["nat-3isn9hr0\r\n"]
Filters	No	No	Array of Filter	Filter criteria: Parameters NatGatewayIds and Filters must not be specified simultaneously. • nat-gateway-id - NAT gateway ID, e.g., nat-0yi4hekt; • vpc-id - VPC ID, e.g., vpc-0yi4hekt; • public-ip-address - EIP, e.g., 139.199.232.238; • public-port - Public port. • private-ip-address - Private IP, e.g., 10.0.0.1; • private-port - Private port. • description - Rule description. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
NatGatewayDestinationIpPortTranslationNatRuleSet	Array of NatGatewayDestinationIpPortTranslationNatRule	NAT gateway port forwarding rule object array. Example:View
TotalCount	Uint64	Number of eligible NAT gateway port forwarding rules objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
UnauthorizedOperation	Unauthorized operation
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InternalServerError	Internal operation error.
InvalidAddressId.NotFound	The specified EIP does not exist.

DescribeNatGatewaySourceIpTranslationNatRules

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNat GatewaySourceIpTranslationNatRules) is used to query the SNAT forwarding rule object array for the NAT gateway.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-08-30 23:11:46.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNatGatewaySourceIpTranslationNatRules
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	The unified NAT gateway ID, such as nat-jktxx454 . Example: nat-3isn9hr0
Filters	No	No	Array of SourceIpTranslationNatRule	Filter criteria: • resource-id, ID of subnet or CVM, e.g., subnet-0yi4hekt • public-ip-address, elastic IP, e.g., 139.199.232.238 • description, rule description. Example:View
Offset	No	No	Int64	Offset. 0 by default. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
SourceIpTranslationNatRuleSet	Array of SourceIpTranslationNatRule	NAT gateway SNAT rule object array. Example:View
TotalCount	Int64	Number of eligible NAT gateway port forwarding rules objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
InternalServerError	Internal operation error.
InvalidAddressId.NotFound	The specified EIP does not exist.

DescribeNatGateways

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNatGateways) is used to query NAT gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-07-05 17:39:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNatGateways
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayIds	No	No	Array of String	The unified NAT gateway ID, such as nat-jktxx454 . Example: ["nat-3isn9hr0\r\n","nat-mxkohguo\r\n"]
Filters	No	No	Array of Filter	Filtering conditions. The parameters NatGatewayIds and Filters cannot be specified simultaneously. • nat-gateway-id - String - (filtering condition) protocol port template instance ID, such as nat-jktxx454 . • vpc-id - String - (filtering condition) unique ID of the VPC, such as vpc-jktxx454 . • nat-gateway-name - String - (filtering condition) protocol port template instance ID, such as demo_nat . Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
NatGatewaySet	Array of NatGateway	NAT gateway object array. Example:View
TotalCount	Uint64	Number of eligible NAT gateway objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DisassociateNatGatewayAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisassociateNatGatewayAddress) is used to unbind an EIP from a NAT gateway.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:00:21.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateNatGatewayAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-mdbjfr0y
PublicIpAddresses	Yes	No	Array of String	Array of elastic IPs bound to NAT gateway. Example: ["139.199.232.212"]

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation.PublicIpAddressDisassociate	A NAT gateway must have at least one elastic IP, which cannot be unbound.

ModifyNatGatewayAddressStatus

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify the primary/secondary status of the EIP bound to a NAT gateway.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-01-17 19:30:45.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNatGatewayAddressStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Unique ID of the VPC. Example: vpc-ake3opls
NatGatewayId	Yes	No	String	Unique ID of the NAT gateway. Example: nat-rci9avb4
AddressId	Yes	No	String	ID of the public IP address. Example: eip-3q1lafds
MasterBackupStatus	Yes	No	String	Primary/ Secondary status: MASTER and BACKUP. Example: BACKUP

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ModifyNatGatewayAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNatGatewayAttribute) is used to modify the attributes of a NAT gateway.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-01-17 19:23:12.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNatGatewayAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-ig8xpno8
NatGatewayName	No	No	String	The name of the NAT gateway, such as demo_nat . Example: demonat gateway
InternetMaxBandwidthOut	No	No	Uint64	Maximum public network outbound bandwidth of NAT gateway (unit: Mbps). Example: 500
StrictSnatMode	No	No	Bool	Whether to disable forwarding for requests that do not match SNAT rules. true: disable forwarding; false: randomly select an EIP of the NAT instance for forwarding. Example: false

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

ModifyNatGatewayDestinationIpPortTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNatGatewayDestinationIpPortTranslationNatRule) is used to modify NAT gateway port forwarding rules.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-02 18:01:34.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNatGatewayDestinationIpPortTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df45454 . Example: nat-3isn9hr0
SourceNatRule	Yes	No	DestinationIpPortTranslationNatRule	Port translation rules for the source NAT gateway. Example:View
DestinationNatRule	Yes	No	DestinationIpPortTranslationNatRule	Destination NAT gateway's port translation rules. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceInUse	Resources occupied

ModifyNatGatewaySourceIpTranslationNatRule

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNatGatewaySourceIpTranslationNatRule) is used to modify NAT gateway SNAT forwarding rules.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-11-08 19:19:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNatGatewaySourceIpTranslationNatRule
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID, e.g., nat-df453454. Example: nat-3isn9hr0
SourceIpTranslationNatRule	Yes	No	SourceIpTranslationNatRule	NAT gateway SNAT translation rules. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.

Error Code	Description
UnknownParameter	Unknown parameter error
UnsupportedOperation	Operation unsupported.
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist

ResetNatGatewayConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ResetNatGatewayConnection) is used to reset the NAT gateway concurrent connection upper limit.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-08-02 17:59:40.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetNatGatewayConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NatGatewayId	Yes	No	String	NAT gateway ID. Example: nat-ig8xpno8
MaxConcurrentConnection	Yes	No	Uint64	Maximum concurrent connections of NAT gateway, e.g., 1,000,000, 3,000,000, and 10,000,000. Example: 3000000

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceInUse	Resources occupied
ResourceNotFound	The resource does not exist

Network ACL APIs
AssociateNetworkAclSubnets

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssociateNetworkAclSubnets) is used for a network ACL to associate subnets under a VPC.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 22:53:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssociateNetworkAclSubnets
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclId	Yes	No	String	The network ACL instance ID, such as acl-demoag78. Example: acl-demoag78
SubnetIds	Yes	No	Array of String	An array of subnet instance IDs, such as [subnet-demoag78]. Example: ["subnet-demoag78\r\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.

CreateNetworkAcl

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a network ACL.

- The inbound and outbound rules of the created network ACL are set to deny all by default. After creation, you typically need to call ModifyNetworkAclEntries to configure the rules as needed.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-30 17:29:56.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNetworkAcl
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-demoag78
NetworkAclName	Yes	No	String	Network ACL name, up to 60 bytes in length. Example: demo

3. Output Parameters

Parameter name	Type	Description
NetworkAcl	NetworkAcl	Network ACL instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.

DeleteNetworkAcl

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNetworkAcl) is used to delete network ACLs.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 22:53:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNetworkAcl
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclId	Yes	No	String	The network ACL instance ID, such as acl-demoag78. Example: acl-demoag78

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeNetworkAcls

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNetworkAcls) is used to query the list of network ACLs.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-12 05:01:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetworkAcls
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclIds	No	No	Array of String	An array of network ACL instance IDs, such as [acl-demoag78]. Each request supports a maximum of 100 instances. The parameters NetworkAclIds and Filters cannot be specified simultaneously. Example: [acl-demoag78]
Filters	No	No	Array of Filter	Filtering conditions. The parameters NetworkAclIds and Filters cannot be specified simultaneously. • vpc-id - String - (filtering condition) VPC instance ID, such as vpc-demoag78. • network-acl-id - String - (filtering condition) network ACL instance ID, such as acl-demoag78. • network-acl-name - String - (filtering condition) name of the network ACL instance. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default. The minimum value is 1, and the maximum value is 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
NetworkAclSet	Array of NetworkAcl	Instance detail list. Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.Range	The parameter value is not within the specified range.

DisassociateNetworkAclSubnets

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisassociateNetworkAclSubnets) is used to disassociate subnets under a VPC from the network ACL.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 22:53:32.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateNetworkAclSubnets
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclId	Yes	No	String	The network ACL instance ID, such as acl-demoag78. Example: acl-demoag78
SubnetIds	Yes	No	Array of String	An array of subnet instance IDs, such as [subnet-demoag78]. Example: ["subnet-demoag78\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.

ModifyNetworkAclAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNetworkAclAttribute) is used to modify network ACL attributes.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-10 22:54:05.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetworkAclAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclId	Yes	No	String	The network ACL instance ID, such as acl-demoag78. Example: acl-demoag78
NetworkAclName	Yes	No	String	Network ACL name, up to 60 bytes in length. Example: demo modify

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

ModifyNetworkAclEntries

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNetworkAclEntries) is used to modify (including add and delete) the inbound and outbound rules of a network ACL.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-26 03:09:04.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetworkAclEntries
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetworkAclId	Yes	No	String	The network ACL instance ID, such as acl-demoag78. Example: acl-demoag78
NetworkAclEntrySet	Yes	No	NetworkAclEntrySet	Network ACL rule set. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to

Parameter name	Type	Description
		be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.

Network Parameter Template APIs
CreateAddressTemplate

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateAddressTemplate) is used to create IP address templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:03:33.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateAddressTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateName	Yes	No	String	IP Address Template Name Example: demoName
Addresses	Yes	No	Array of String	Address information, which can be IP, CIDR, and IP range. Example: ["192.168.1.0/24\r\n","192.168.2.0/24\r\n"]

3. Output Parameters

Parameter name	Type	Description
AddressTemplate	AddressTemplate	IP address template object. Example:View
AddressesExtra	Array of AddressInfo	Address information, which supports carrying remarks and supports IP address, CIDR, and IP range. Either Addresses or AddressesExtra is required. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

CreateAddressTemplateGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateAddressTemplateGroup) is used to create IP address template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:06:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateAddressTemplateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateGroupName	Yes	No	String	IP address template collection name. Example: demoName
AddressTemplateIds	Yes	No	Array of String	IP address template instance ID, e.g., ipm-mdunqeb6. Example: ["ipm-88t6207k\r\n","ipm-mdunqeb6\r\n"]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
AddressTemplateGroup	AddressTemplateGroup	IP address template collection object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

CreateServiceTemplate

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateServiceTemplate) is used to create protocol port templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-07-09 01:46:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateServiceTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateName	Yes	No	String	Protocol Port Template Name Example: demoName
Services	Yes	No	Array of String	Supports individual ports, multiple ports, continuous ports, and all ports, with protocols including TCP, UDP, ICMP, and GRE protocols. Example: ["TCP:8080","UDP:99"]

3. Output Parameters

Parameter name	Type	Description
ServiceTemplate	ServiceTemplate	Protocol port template object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

CreateServiceTemplateGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateServiceTemplateGroup) is used to create protocol port template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:10:50.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateServiceTemplateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateGroupName	Yes	No	String	Protocol Port Template Collection Name Example: demoName
ServiceTemplateIds	Yes	No	Array of String	Protocol port template instance ID, e.g., ppm-4dw6agho. Example: ppm-4dw6agho

3. Output Parameters

Parameter name	Type	Description
ServiceTemplateGroup	ServiceTemplateGroup	Protocol port template collection object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
ResourceNotFound	The resource does not exist

DeleteAddressTemplate

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteAddressTemplate) is used to delete IP address templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-03-29 19:48:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteAddressTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateId	Yes	No	String	IP address template instance ID, e.g., ipm-09o5m8kc. Example: ipm-09o5m8kc

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.

DeleteAddressTemplateGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteAddressTemplateGroup) is used to delete IP address template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-03-29 19:48:21.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteAddressTemplateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateGroupId	Yes	No	String	IP address template collection instance ID, e.g., ipmg-90cex8mq. Example: ipmg-90cex8mq

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DeleteServiceTemplate

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteServiceTemplate) is used to delete protocol port templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-03-29 19:50:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteServiceTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateId	Yes	No	String	Protocol port template instance ID, e.g., ppm-e6dy460g. Example: pm-e6dy460g

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DeleteServiceTemplateGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteServiceTemplateGroup) is used to delete protocol port template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-03-29 19:50:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteServiceTemplateGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateGroupId	Yes	No	String	Protocol port template collection instance ID, e.g., ppmg-n17uxvve. Example: ppmg-n17uxvve

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeAddressTemplateGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAddressTemplateGroups) is used to query the IP address template collection.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-19 20:23:09.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAddressTemplateGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • address-template-group-name - String - (Filter criteria) IP address template collection name. • address-template-group-id - String - (Filter criteria) IP address template collection ID, e.g., ipmg-mdunqeb6. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 1
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example:
AddressTemplateGroupSet	Array of AddressTemplateGroup	IP address template. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

DescribeAddressTemplates

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAddressTemplates) is used to query IP address templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-07-08 06:46:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAddressTemplates
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • address-template-name - String - (Filter criteria) IP address template name. • address-template-id - String - (Filter criteria) IP address template instance ID, e.g., ipm-mdunqeb6. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example:
AddressTemplateSet	Array of AddressTemplate	IP address template. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

DescribeServiceTemplateGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeServiceTemplateGroups) is used to query the protocol port template collection.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-10-26 03:39:17.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeServiceTemplateGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • service-template-group-name - String - (Filter criteria) Protocol port template group name. • service-template-group-id - String - (Filter criteria) Protocol port template group instance ID, e.g., ppmg-e6dy460g. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example: 1
ServiceTemplateGroupSet	Array of ServiceTemplateGroup	Protocol port template collection. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

DescribeServiceTemplates

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeServiceTemplates) is used to query protocol port templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-07-09 00:17:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeServiceTemplates
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • service-template-name - String - (Filter criteria) Protocol port template name. • service-template-id - String - (Filter criteria) Protocol port template instance ID, e.g., ppm-e6dy460g. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example: 8
ServiceTemplateSet	Array of ServiceTemplate	Protocol port template object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

DescribeTemplateLimits

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeTemplateLimits) is used to query the list of parameter template quotas.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-24 19:27:00.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTemplateLimits
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
TemplateLimit	TemplateLimit	Parameter template quota object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ModifyAddressTemplateAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyAddressTemplateAttribute) is used to modify IP address templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-28 18:59:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAddressTemplateAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateId	Yes	No	String	IP address template instance ID, e.g., ipm-mdunqeb6. Example: ipm-mdunqeb6
AddressTemplateName	No	No	String	IP address template name. Example: demoName
Addresses	No	No	Array of String	Address information, which can be IP, CIDR, and IP range. Example: 10.0.0.5

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyAddressTemplateGroupAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyAddressTemplateGroupAttribute) is used to modify IP address template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-28 18:59:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAddressTemplateGroupAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressTemplateGroupId	Yes	No	String	IP address template collection instance ID, e.g., ipmg-2uw6ujo6. Example: ipmg-2uw6ujo6
AddressTemplateGroupName	No	No	String	IP address template collection name. Example: demo
AddressTemplateIds	No	No	Array of String	IP address template instance ID, e.g.: ipm-mdunqeb6. Example: ipm-mdunqeb6

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Duplicate	Input Parameters are repetitive.

ModifyServiceTemplateAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyServiceTemplateAttribute) is used to modify protocol port templates.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-28 18:59:21.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyServiceTemplateAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateId	Yes	No	String	Protocol port template instance ID, e.g., ppm-529nwwj8. Example: ppm-529nwwj8
ServiceTemplateName	No	No	String	Protocol port template name. Example: demoName
Services	No	No	Array of String	Supports individual ports, multiple ports, continuous ports, and all ports, with protocols including TCP, UDP, ICMP, and GRE protocols. Example: ppm-529nwwj8

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyServiceTemplateGroupAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyServiceTemplateGroupAttribute) is used to modify protocol port template collections.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-28 18:58:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyServiceTemplateGroupAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ServiceTemplateGroupId	Yes	No	String	Protocol port template collection instance ID, e.g., ppmg-ei8hfd9a. Example: ppmg-p4oaqawq
ServiceTemplateGroupName	No	No	String	Protocol port template collection name. Example: demo
ServiceTemplateIds	No	No	Array of String	Protocol port template instance ID, e.g., ppm-4dw6agho. Example: ['ppm-529nwwj8']

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

Network Probe APIs
CheckNetDetectState

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CheckNetDetectState) is used for network probe verification.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-03 05:38:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckNetDetectState
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetDetectId	No	No	String	The network detection instance ID, such as netd-demoag78. This parameter requires at least one of the following: VpcId, SubnetId, or NetDetectName. If NetDetectId is provided, it takes precedence. Example: netd-demoag78
VpcId	No	No	String	VPC instance ID , such as vpc-demoag78 . This parameter is used in conjunction with SubnetId and NetDetectName, and at least one of these should be specified along with NetDetectId. If NetDetectId is provided, it takes precedence. Example: vpc-7zayowkt
SubnetId	No	No	String	The subnet instance ID, such as subnet-demoag78. This parameter is used in conjunction with VpcId and NetDetectName, and at least one of these should be specified along with NetDetectId. If NetDetectId is provided, it takes precedence. Example: subnet-siqkaiqm
NetDetectName	No	No	String	Network probe name, up to 60 bytes in length. This parameter is used in conjunction with (VpcId, SubnetId), and at least one of NetDetectId and this parameter must be provided. When NetDetectId exists, it will be used. Example: name
DetectDestinationIp	Yes	No	Array of String	Probe destination IPv4 address array. The maximum number is two. Example: ["10.0.0.2\r\n","10.0.0.3\r\n"]
NextHopType	Yes	No	String	Type of next hop. Types currently supported are VPN: VPN gateway; DIRECTCONNECT: Direct Connect gateway; PEERCONNECTION: Peering connection; NAT: NAT gateway; NORMAL_CVM: Ordinary CVM. Example: NORMAL_CVM
NextHopDestination	Yes	No	String	The next hop target gateway, with valid values depending on the next hop type: When the next hop type is VPN, the value should be the VPN gateway ID, such as vpngw-demoag78. When the next hop type is DIRECTCONNECT, the value should be the Direct Connect gateway ID, such as dcg-demoag78. When the next hop type is PEERCONNECTION, the value should be the peering connection ID, such as pcx-demoag78. When the next hop type is NAT, the value should be the NAT gateway, such as nat-demoag78. When the next hop type is NORMAL_CVM, the value should be the CVM IPv4 address, such as 10.0.0.12. Example: 10.0.0.4

3. Output Parameters

Parameter name	Type	Description
NetDetectIpStateSet	Array of NetDetectIpState	Network probe validation result object array. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.
InvalidParameter.NextHopMismatch	The next hop type does not match it's gateway.
InvalidParameterValue.NetDetectSameIp	The probe destination IP is the same as that of another network probe within the same VPC and subnet.

CreateNetDetect

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateNetDetect) is used to create network probe.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:27:48.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNetDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	The VPC instance ID , such as vpc-demoag78 . Example: vpc-demoag78
SubnetId	Yes	No	String	The subnet instance ID, such as subnet-demoag78. Example: subnet-demoag78
NetDetectName	Yes	No	String	Network probe name, up to 60 bytes in length. Example: demo
DetectDestinationIp	Yes	No	Array of String	Probe destination IPv4 address array. The maximum number is two. Example: ["10.0.0.2\r\n","10.0.0.3\r\n"]
NextHopType	Yes	No	String	Type of next hop. Types currently supported are VPN: VPN gateway; DIRECTCONNECT: Direct Connect gateway; PEERCONNECTION: Peering connection; NAT: NAT gateway; NORMAL_CVM: Ordinary CVM. Example: NORMAL_CVM
NextHopDestination	Yes	No	String	The next hop target gateway, with valid values depending on the next hop type: When the next hop type is VPN, the value should be the VPN gateway ID, such as vpngw-demoag78. When the next hop type is DIRECTCONNECT, the value should be the Direct Connect gateway ID, such as dcg-demoag78. When the next hop type is PEERCONNECTION, the value should be the peering connection ID, such as pcx-demoag78. When the next hop type is NAT, the value should be the NAT gateway, such as nat-demoag78. When the next hop type is NORMAL_CVM, the value should be the CVM IPv4 address, such as 10.0.0.12. Example: 10.0.0.4
NetDetectDescription	No	No	String	Network probe description. Example: demo

3. Output Parameters

Parameter name	Type	Description
NetDetect	NetDetect	NetDetect object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.
InvalidParameter.NextHopMismatch	The next hop type does not match it's gateway.
InvalidParameterValue.NetDetectSameIp	The probe destination IP is the same as that of another network probe within the same VPC and subnet.
UnsupportedOperation.EcmpWithUserRoute	An ECMP is formed with the user-defined route.

DeleteNetDetect

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteNetDetect) is used to delete network probe instances.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-11-14 04:49:46.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNetDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetDetectId	Yes	No	String	The network detection instance ID , such as netd-demoag78 . Example: netd-demoag78

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeNetDetectStates

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNetDetectStates) is used to query the list of network probe verification results.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-11-14 04:52:42.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetDetectStates
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetDetectIds	No	No	Array of String	An array of network detection instance IDs , such as [netd-demoag78]. Example: ["netd-demoag78"]
Filters	No	No	Array of Filter	Filtering conditions. The parameters NetDetectIds and Filters cannot be specified simultaneously. • net-detect-id - String - (filtering condition) network detection instance ID, such as netd-demoag78. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
NetDetectStateSet	Array of NetDetectState	Array of the network probe validation result objects that meet the criteria. Example:View
TotalCount	Uint64	Number of eligible network probe validation objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.Range	The parameter value is not within the specified range.

DescribeNetDetects

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeNetDetects) is used to query the network probe list.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-11-14 04:52:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetDetects
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetDetectIds	No	No	Array of String	An array of network detection instance IDs , such as [netd-demoag78]. Example: netd-demoag78
Filters	No	No	Array of Filter	Filtering conditions. The parameters NetDetectIds and Filters cannot be specified simultaneously. • vpc-id - String - (filtering condition) VPC instance ID, such as vpc-demoag78. • net-detect-id - String - (filtering condition) network detection instance ID, such as netd-demoag78. • subnet-id - String - (filtering condition) subnet instance ID, such as subnet-demoag78. • net-detect-name - String - (filtering condition) network detection name. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
NetDetectSet	Array of NetDetect	Eligible network probe object array. Example:View
TotalCount	Uint64	Number of eligible network probe objects. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.Range	The parameter value is not within the specified range.

ModifyNetDetect

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyNetDetect) is used to modify network probe parameters.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-04 23:47:51.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
NetDetectId	Yes	No	String	The network detection instance ID , such as netd-demoag78 . Example: netd-demoag78
NetDetectName	No	No	String	Network probe name, up to 60 bytes in length. Example: demo
DetectDestinationIp	No	No	Array of String	Probe destination IPv4 address array. The maximum number is two. Example: ["10.0.0.2\r\n","10.0.0.3\r\n"]
NextHopType	No	No	String	Type of next hop. Types currently supported are VPN: VPN gateway; DIRECTCONNECT: Direct Connect gateway; PEERCONNECTION: Peering connection; NAT: NAT gateway; NORMAL_CVM: Ordinary CVM. Example: NORMAL_CVM
NextHopDestination	No	No	String	The next hop target gateway, with valid values depending on the next hop type: When the next hop type is VPN, the value should be the VPN gateway ID, such as vpngw-demoag78. When the next hop type is DIRECTCONNECT, the value should be the Direct Connect gateway ID, such as dcg-demoag78. When the next hop type is PEERCONNECTION, the value should be the peering connection ID, such as pcx-demoag78. When the next hop type is NAT, the value should be the NAT gateway, such as nat-demoag78. When the next hop type is NORMAL_CVM, the value should be the CVM IPv4 address, such as 10.0.0.12. Example: 10.0.0.4
NetDetectDescription	No	No	String	Network probe description. Example: demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.
InvalidParameter.NextHopMismatch	The next hop type does not match it's gateway.
InvalidParameterValue.NetDetectSameIp	The probe destination IP is the same as that of another network probe within the same VPC and subnet.

Other APIs
CreateVpcEndPoint

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create endpoint

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 03:41:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpcEndPoint
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID. Example: vpc-q26u781x.
SubnetId	Yes	No	String	Subnet instance ID. Example: subnet-qmqye6ew.
EndPointName	Yes	No	String	Endpoint name. Example: Example name.

Parameter name	Required	Allow NULL	Type	Description
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcsvc-ettmyyrn.
EndPointVip	No	No	String	Endpoint VIP. IP can be specified for request. Example: 10.0.0.0/16.
SecurityGroupId	No	No	String	Security group ID. Example: sg-demoag.
IpAddressType	No	No	String	Address Type Example: IPv4/IPv6
AppId	Yes	No	String	User ID Example: jkt45678

3. Output Parameters

Parameter name	Type	Description
EndPoint	EndPoint	Endpoint object details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
InvalidParameterValue	The parameter value is invalid.
ResourceInUse	Resources occupied
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.
InvalidParameterValue.Range	The parameter value is not within the specified range.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Reserved	The parameter value is a reserved object of the system.
ResourceUnavailable	Resource unavailable

DescribeGatewayFlowMonitorDetail

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeGatewayFlowMonitorDetail) is used to query the gateway traffic monitoring details.

- It only supports querying a single gateway instance. That is, at most one of the input parameters VpnId , DirectConnectGatewayId , PeeringConnectionId , and NatId can be and must be input.
- If the gateway has traffic, but calling this API does not return any data, confirm whether gateway traffic monitoring is enabled on the corresponding gateway detail page in the console.

Default interface request rate limit: 30 times per second.

Interface update time: 2019-03-02 18:52:49.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeGatewayFlowMonitorDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
TimePoint	Yes	No	Datetime	Time point, indicating the details to query in a minute, e.g., 2019-02-28 18:15:20 indicates that the details within the minute of 18:15 will be queried. Example: 2019-02-28 18:15:20
VpnId	No	No	String	VPN gateway instance ID, e.g., vpn-ltjahce6. Example: vpn-ltjahce6
DirectConnectGatewayId	No	No	String	Direct Connect gateway instance ID, e.g., dcg-ltjahce6. Example: dcg-ltjahce6
PeeringConnectionId	No	No	String	Peering connection instance ID, e.g., pcx-ltjahce6 . Example: pcx-ltjahce6
NatId	No	No	String	NAT gateway instance ID, e.g., nat-ltjahce6. Example: nat-ltjahce6
Offset	No	No	Uint64	Offset. Example: 0
Limit	No	No	Uint64	Returned quantity. Example: 20
OrderField	No	No	String	Sorting fields. InPkg , OutPkg , InTraffic , and OutTraffic are supported. Example: InPkg
OrderDirection	No	No	String	Sorting method. ASC : Ascending order, DESC : Descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example:
GatewayFlowMonitorDetailSet	Array of GatewayFlowMonitorDetail	Gateway traffic monitoring details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

Peering Connection APIs AcceptVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Accept an intra-region peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:18:50.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AcceptVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
UnsupportedOperation.VpcPeerInvalidStateChange	The peering connection status is abnormal.

AcceptVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Accept a cross-region peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:20:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AcceptVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID of this asynchronous task. Example: 21321

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

CreateVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create intra-region VPC peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 07:04:53.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceVpcId	Yes	No	String	Unique ID of the local VPC. Example: vpc-0npfx81k
PeeringConnectionName	Yes	No	String	PC name. Example: demo
DestinationVpcId	Yes	No	String	Unique ID of the customer VPC. Example: vpc-demoag78
DestinationUin	Yes	No	String	Customer user UIN. Example: 568722665
DestinationRegion	Yes	No	String	Customer region, compatible with public cloud APIs. Example: ap-region

3. Output Parameters

Parameter name	Type	Description
PeeringConnectionId	String	Peering connection instance ID. Example: pcx-4q8g18en
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

CreateVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create cross-region VPC PC

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-03 10:01:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Unique ID of the local VPC. Example: vpc-67wlqf6v
PeeringConnectionName	Yes	No	String	PC name. Example: demo
PeerVpcId	Yes	No	String	Unique ID of the customer VPC. Example: vpc-67wlqf6v
PeerUin	Yes	No	String	Customer user UIN. Example: 100000072292
PeerRegion	Yes	No	String	Customer region name. Example: 500002
Bandwidth	No	No	Int64	PC bandwidth value, 10 Mbps by default when it is not input. Example: 100
Type	No	No	Int64	Interconnection type. Currently, only VPC interconnection is supported. The value only includes 1. Example: 1
ChargeType	No	No	String	Billing type. Currently only billing by daily peak is supported, i.e. POSTPAID_BY_DAY_MAX. Example: POSTPAID_BY_DAY_MAX"
Zone	No	No	String	Availability zone name. Example: 500001

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
UnsupportedOperation.VpcPeerAlreadyExist	The peering connection already exists.

DeleteVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete intra-region VPC peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2023-04-23 03:30:43.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-r2kt047o

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist

DeleteVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete cross-region VPC PCs

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:43:55.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: 4

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 65535

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Malformed	Invalid input format.

EnableVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Enable an expired intra-region PC

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:54:14.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: 4

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Malformed	Invalid input format.

EnableVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Enable expired cross-region PC

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:55:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: 4

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Malformed	Invalid input format.

ModifyVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify an intra-region peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-06-17 15:25:59.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k
PeeringConnectionName	Yes	No	String	Instance name. Example: demo

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the attributes of cross-region peering connections

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:51:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k
PeeringConnectionName	No	No	String	Instance name. Example: demo
Bandwidth	No	No	Int64	Bandwidth value. Example: 100

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist

RejectVpcPeeringConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Reject an intra-region peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-03 09:58:02.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RejectVpcPeeringConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Malformed	Invalid input format.
UnsupportedOperation.InvalidState	The resource status is invalid.

RejectVpcPeeringConnectionEx

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Reject a cross-region peering connection

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-29 06:47:40.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RejectVpcPeeringConnectionEx
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PeeringConnectionId	Yes	No	String	Unique PC ID. Example: pcx-0npfx81k

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 65535

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist
UnsupportedOperation.InvalidState	The resource status is invalid.

Private Link APIs
CreateVpcEndPointService

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create an endpoint service.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 05:18:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpcEndPointService
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID. Example: vpc-ihwh81fr.
EndPointServiceName	Yes	No	String	Endpoint service name. Example: Terminal service demo001.
AutoAcceptFlag	Yes	No	Bool	Whether it is auto-accepted. Example: True.

Parameter name	Required	Allow NULL	Type	Description
ServiceInstanceId	Yes	No	String	Backend service ID, e.g., lb-xxx. Example: lb-7xwasqqy.
IpAddressType	No	No	String	Address Type Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description
EndPointService	EndPointService	Endpoint service object details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded	Exceeded the limit
ResourceInUse	Resources occupied
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
ResourceNotFound	The resource does not exist
ResourceUnavailable	Resource unavailable
InvalidParameterValue.Empty	Missing parameter

CreateVpcEndPointServiceWhiteList

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create an endpoint service allowlist

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-24 00:06:21.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpcEndPointServiceWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
UserUin	Yes	No	String	UIN. Example: jkt
Description	No	No	String	Allowlist description. Example: demo
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcsvc-b2mrmmx7

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnsupportedOperation.UinNotFound	The account ID does not exist.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DeleteVpcEndPoint

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete an endpoint

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 05:16:10.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpcEndPoint
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointId	Yes	No	String	Endpoint ID. Example: vpce-7czfogk8
IpAddressType	No	No	String	IP Address Type Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceInUse	Resources occupied
InvalidParameterValue.Malformed	Invalid input format.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

DeleteVpcEndPointService

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete endpoint services

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 05:15:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpcEndPointService
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointServiceId	Yes	No	String	Endpoint ID. Example: vpcsvc-demoag78
IpAddressType	No	No	String	IP Address Type Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceInUse	Resources occupied
InvalidParameterValue.Malformed	Invalid input format.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

DeleteVpcEndPointServiceWhiteList

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete an endpoint service allowlist

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-24 03:11:59.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpcEndPointServiceWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
UserUin	Yes	No	Array of String	User UIN array. Example: ['jkt']
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcsvc-b2mrmmx7

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation.UinNotFound	The account ID does not exist.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

DescribeVpcEndPoint

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the endpoint details

Default interface request rate limit: 20 times per second.

Interface update time: 2021-02-04 01:34:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcEndPoint
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • end-point-service-id String - (Filter criteria) Endpoint service ID. • end-point-name - String - (Filter criteria) Endpoint instance name. • end-point-id - String - (Filter criteria) Endpoint instance ID. • vpc-id - String - (Filter criteria) VPC instance ID. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 1

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Number of returns per page, 20 by default, up to 100. Example: 1
EndPointId	No	No	Array of String	Endpoint ID list. Example: vpce-fwzzlq4w
IpAddressType	No	No	String	IP Address Type Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description
EndPointSet	Array of EndPoint	Endpoint object. Example:View
TotalCount	Uint64	Number of endpoints that meet the query criteria. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DescribeVpcEndPointService

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query endpoint service list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-26 02:30:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcEndPointService
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filter criteria. • service-id String - (Filter criteria) Unique ID of the endpoint service. • service-name - String - (Filter criteria) Endpoint instance name. • service-instance-id - String - (Filter criteria) Unique ID of the backend service, e.g., lb-xxx. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns per page, 20 by default, up to 100. Example: 100

Parameter name	Required	Allow NULL	Type	Description
EndPointServiceIds	No	No	Array of String	Endpoint service ID. Example: vpcsvc-pzk35prh
IpAddressType	No	No	String	IP Address Type Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description
EndPointServiceSet	Array of EndPointService	Endpoint service object array. Example:View
TotalCount	Uint64	Number of items that meet the query criteria. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
InvalidParameterValue.Range	The parameter value is not within the specified range.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DescribeVpcEndPointServiceWhiteList

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query the service allowlist of endpoint services.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-27 01:15:12.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcEndPointServiceWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns per page, 20 by default, up to 100. Example: 0
Filters	No	No	Array of Filter	Filter criteria. • user-uin String - (Filter criteria) User UIN. • end-point-service-id String - (Filter criteria) ID of the endpoint service. Example:View

3. Output Parameters

Parameter name	Type	Description
VpcEndpointServiceUserSet	Array of VpcEndPointServiceUser	Allowlist object array. Example:View
TotalCount	Uint64	Number of eligible allowlist entries. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation.UinNotFound	The account ID does not exist.

DisassociateVpcEndPointSecurityGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Unbind security group at the endpoint.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 04:44:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateVpcEndPointSecurityGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupIds	Yes	No	Array of String	Security group ID array. Example: ['sg-75ww503r']
EndPointId	Yes	No	String	Endpoint ID. Example: vpce-7czfogk8

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

EnableVpcEndPointConnect

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Whether to accept endpoint connection requests.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-24 02:48:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableVpcEndPointConnect
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcsvc-8gdaqxi0
EndPointId	Yes	No	Array of String	Endpoint ID array. Example: ["vpce-8gdaqxi0"]
AcceptFlag	Yes	No	Bool	Whether to accept endpoint connection requests. Example: True
IpAddressType	No	No	String	Address Type Example: IPv4

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

EnableVpcEndPointConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Whether to accept endpoint connection requests.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 05:04:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableVpcEndPointConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcs-fwzzlq4w
EndPointId	Yes	No	String	Endpoint ID. Example: vpce-fwzzlq4w
AcceptFlag	Yes	No	Bool	Whether to accept endpoint connection requests. Example: true/false

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist
UnsupportedOperation.ActionNotFound	The API does not exist.

ModifyVpcEndPointAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify the endpoint

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-21 04:49:14.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcEndPointAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointId	Yes	No	String	Endpoint ID. Example: vpce-8gdaqxi0.
EndPointName	No	No	String	Endpoint name. Example: Name example.
SecurityGroupIds	No	No	Array of String	Security group ID list. Example: ['sg-75ww503r']
IpAddressType	No	No	String	IP address type. IPv4: v4 type; IPv6: v6 type. Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyVpcEndPointServiceAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify endpoint service-related information.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-23 01:30:24.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcEndPointServiceAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpces-hhth8n9j
EndPointServiceName	No	No	String	Endpoint service name. Example: demo
AutoAcceptFlag	No	No	Bool	Whether it is auto-accepted. Example: False
ServiceInstanceId	No	No	String	Backend service ID, e.g., lb-xxx. Example: lb-75d88uw8

Parameter name	Required	Allow NULL	Type	Description
VpcId	Yes	No	String	VPCID. Example: vpc-a2oj00df
IpAddressType	No	No	String	IP address type. IPv4: v4 type; IPv6: v6 type. Example: IPv4/IPv6

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceInUse	Resources occupied
InvalidParameterValue.Malformed	Invalid input format.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist
ResourceUnavailable	Resource unavailable

ModifyVpcEndPointServiceWhiteList

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify endpoint service allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-01-24 00:02:44.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcEndPointServiceWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
UserUin	Yes	No	String	User UIN. Example: jkt
Description	No	No	String	Allowlist description information. Example: demo
EndPointServiceId	Yes	No	String	Endpoint service ID. Example: vpcsvc-b2mrmmx7

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnsupportedOperation.UinNotFound	The account ID does not exist.
MissingParameter	Missing parameters. The request did not carry the required parameter.
ResourceNotFound	The resource does not exist

Routing Table APIs
CreateIpv6Routes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

User-created IPv6 route.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 19:58:31.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateIpv6Routes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-q8o2z892
Routes	Yes	No	Array of Route	Routing policy object. Example:View

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of new instances. Example:
RouteTableSet	Array of RouteTable	Routing table object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.

CreateRouteTable

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateRouteTable) is used to create a routing table.

- After a VPC is created, the system will create a default routing table, and all newly created subnets will be associated with this default routing table. You can directly use the default routing table to manage your routing policies under normal circumstances. When you have numerous routing policies, you can call this API to create additional routing tables to manage your policies.* When creating a routing table, you can also bind tags. The list of tags in the response represents the successfully added tags.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-13 23:59:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateRouteTable
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	ID of VPC instance to be operated. It can be accessed through VpcId in the returned value of the DescribeVpcs API. Example: vpc-2at5y1pn
RouteTableName	Yes	No	String	Routing table name, up to 60 bytes in length. Example: demoRouteTable
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
RouteTable	RouteTable	Routing table object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.

CreateRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateRoutes) is used to create routing policies.

- Add routing policies in batch to a specified routing table.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:08:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID. Example: rtb-n0yejvje
Routes	Yes	No	Array of Route	Routing policy object. Example:View

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of new instances. Example:
RouteTableSet	Array of RouteTable	Routing table object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.VpcCidrConflict	The destination IP range conflicts with the current VPC's CIDR.
InvalidParameterValue.CidrNotInPeerVpc	The destination IP range is not within the CIDR range of the peer VPC.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
UnsupportedOperation.Ecmp	ECMP is not supported.
UnsupportedOperation.EcmpWithCcnRoute	An ECMP is formed with the route to CCN.
UnsupportedOperation.EcmpWithUserRoute	An ECMP is formed with the user-defined route.
UnsupportedOperation.ConflictWithDockerRoute	Overlaps with the IP range of a TKE container under this VPC.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.

DeleteIpv6Routes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete the IPv6 routing rules of a routing table.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 20:20:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteIpv6Routes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table ID. Example: rtb-q8o2z892
RouteItemIds	Yes	No	Array of String	Routing policy ID. Example: ['rti-i8bap903']

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RouteSet	Array of Route	Deleted routing policies. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.
ResourceNotFound	The resource does not exist

DeleteRouteTable

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Delete a routing table

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-10 06:02:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteRouteTable
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DeleteRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteRoutes) is used to delete routing policies in batch from a routing table.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:37:17.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID. Example: rtb-f49l6u0z
Routes	Yes	No	Array of DellRoute	Routing policy object. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RouteSet	Array of Route	Details of deleted routing policies. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.

DescribeRouteConflicts

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeRouteConflicts) is used to query the conflict list between user-defined routing policies and CCN routing policies.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:31:57.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeRouteConflicts
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
DestinationCidrBlocks	Yes	No	Array of String	List of conflicting destination ports to be checked Example: ['1.0.0.0/8', '0.0.0.0']

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RouteConflictSet	Array of RouteConflict	Routing policy conflict list Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

DescribeRouteTables

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeRouteTables) is used to query routing tables.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-08-21 05:54:55.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeRouteTables
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableIds	No	No	Array of String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: ['rtb-azd4dt1c']
Filters	No	No	Array of Filter	Filters. Parameters RouteTableIds and Filters must not be specified simultaneously. • route-table-id - String - (Filters) Route table instance ID. • route-table-name - String - (Filters) Route table name. • vpc-id - String - (Filters) VPC instance ID, e.g., vpc-f49l6u0z. • association.main - String - (Filters) Whether it is a primary route table. • tag-key - String - Required or Not: No - (Filters) Filter by tag key. • tag:tag-key - String - Required or Not: No - (Filters) Filter by tag-key value pair. The tag-key is replaced with a specific tag key. For usage, refer to Example 2. Example:View
Offset	No	No	String	Offset. Example: 0
Limit	No	No	String	Number of request objects. Example: 1

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example:
RouteTableSet	Array of RouteTable	Routing table object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DisableRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DisableRoutes) is used to disable enabled subnet routes.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-11-15 17:42:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisableRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Unique routing table ID. Example: rtb-9wzwlnhc
RouteIds	Yes	No	Array of Uint64	Unique ID of routing policy. Example: ["18292\n","18293\n"]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.

EnableRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (EnableRoutes) is used to enable the subnet routes that have been disabled.

This API will check for route conflicts after enabling. If there is a conflict, the enabling process will fail. In case of route conflicts, conflicting routes must be disabled before the desired route is enabled.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-11-15 17:41:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Unique routing table ID. Example: rtb-9wzwlnhc
RouteIds	Yes	No	Array of Uint64	Unique ID of routing policy. Example: ["18292\n","18293\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
InvalidParameterValue.Malformed	Invalid input format.
UnsupportedOperation.Ecmp	ECMP is not supported.

ModifyIpv6Routes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Modify IPv6 routing rules

Default interface request rate limit: 20 times per second.

Interface update time: 2021-11-10 00:34:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyIpv6Routes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
Routes	Yes	No	Array of Route	Routing policy object. It is necessary to specify the routing policy ID (RouteId). Example:View

3. Output Parameters

Parameter name	Type	Description
OldRouteSet	Array of Route	Original routing policy information. Example:View
NewRouteSet	Array of Route	Modified routing policy information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InternalServerError	Internal operation error.

ModifyRouteTableAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyRouteTableAttribute) is used to modify the attributes of routing tables.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-10 06:04:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyRouteTableAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
RouteTableName	Yes	No	String	Route table name. Example: name

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ReplaceRouteTableAssociation

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ReplaceRouteTableAssociation) is used to modify the routing table associated with a subnet.

- A subnet can only be associated with one routing table.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-26 04:45:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ReplaceRouteTableAssociation
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SubnetId	Yes	No	String	Subnet instance ID, e.g., subnet-3x5lf5q0, which can be queried through the DescribeSubnets API. Example: subnet-3x5lf5q0
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ReplaceRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ReplaceRoutes) is used to modify a specified routing policy (Route) based on the touting policy ID (RouteId), supporting batch modifications.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-10-26 03:01:51.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ReplaceRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
Routes	Yes	No	Array of Route	Routing policy object. It is necessary to specify the routing policy ID (RouteId). Example:View

3. Output Parameters

Parameter name	Type	Description
OldRouteSet	OldRouteSet	Old route information Example:View
NewRouteSet	NewRouteSet	New route information Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.VpcCidrConflict	The destination IP range conflicts with the current VPC's CIDR.
InvalidParameterValue.CidrNotInPeerVpc	The destination IP range is not within the CIDR range of the peer VPC.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.
UnsupportedOperation.Ecmp	ECMP is not supported.

ResetRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ResetRoutes) is used to reset the name of a certain routing table and all routing policies.

Note: To call this API, first delete all routing policies in the current routing table, and then save the newly submitted routing policy content, which can cause network interruptions.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-08-03 19:45:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
RouteTableId	Yes	No	String	Routing table instance ID, e.g., rtb-azd4dt1c. Example: rtb-n0yejvje
RouteTableName	Yes	No	String	Routing table name, up to 60 bytes in length. Example: demo
Routes	Yes	No	Array of Route	Routing policy. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.VpcCidrConflict	The destination IP range conflicts with the current VPC's CIDR.
InvalidParameterValue.CidrNotInPeerVpc	The destination IP range is not within the CIDR range of the peer VPC.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.
UnsupportedOperation.Ecmp	ECMP is not supported.

Security Group APIs
CreateDefaultSecurityGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a default security group. If no default security group exists under the project, it will create one; otherwise, it will retrieve the existing default security group.

- The Security group quantity limit applies to each project in each region under each account.
  The inbound and outbound policies of the created security group are set to deny all by default. After creation, you typically need to call CreateSecurityGroupPolicies to configure the policies as needed.
- Tags can be bound to the security group during its creation. The tag list in the response represents the successfully added tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:53:52.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDefaultSecurityGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ProjectId	No	No	String	Project ID. Default value: 0. It can be queried on the project management page in the console. Example: 0

3. Output Parameters

Parameter name	Type	Description
SecurityGroup	SecurityGroup	Security group object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
ResourceNotFound	The resource does not exist

CreateSecurityGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a security group.

- The security group quantity limit applies to each project in each region under each account.
- The inbound and outbound policies of the created security group are set to deny all by default. After creation, you typically need to call CreateSecurityGroupPolicies to configure the policies as needed.
- Tags can be bound to the security group during its creation. The tag list in the response represents the successfully added tags.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-02-14 00:24:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSecurityGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ProjectId	No	No	String	Project ID. Default value: 0. It can be queried on the project management page in the console. Example: 0
GroupName	Yes	No	String	Security group name. The name can be given freely but must not exceed 60 characters. Example: demoGroup
GroupDescription	Yes	No	String	Security group remarks, up to 100 characters. Example: demo-group-desc
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
SecurityGroup	SecurityGroup	Security group object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.

CreateSecurityGroupPolicies

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a security group rule.

- Version indicates the version number of a security group rule. Each time you update a security group rule, the version number automatically increases by 1 to prevent the updated rule from expiring. This parameter is optional.
- The Protocol field supports TCP, UDP, ICMP, ICMPV6, GRE, and ALL.
- The CidrBlock field supports any string conforming to the CIDR format standard (complete form). On a basic network, if the CidrBlock field values contain the private IP addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The Ipv6CidrBlock field supports any string conforming to the IPv6 CIDR format standard (complete form). On a basic network, if the Ipv6CidrBlock field values contain the private IPv6 addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The SecurityGroupId field supports the ID of a security group in the same project as the security group to be modified and the ID of the security group to be modified. The private IP addresses of all CVM instances associated with the security group are used as source IP addresses. When this field is specified, the network packet matching process of the rule will change as the CVM instance associated with the corresponding security group changes. The source IP addresses do not need to be modified again.
- The Port field supports a single port number or a port range. For example, 80 or 8000-8010. The Port field is valid only when the Protocol field is set to TCP or UDP. In other words, when the Protocol field is not set to TCP or UDP, the Protocol and Port fields cannot be specified at the same time. Otherwise, an API error will occur.
- The Action field supports only ACCEPT and DROP.
- CidrBlock, Ipv6CidrBlock, SecurityGroupId, and AddressTemplate cannot be specified at the same time. ServiceTemplate cannot be specified if Protocol or Port is specified.
- One request allows you to create rules in only one direction. If the PolicyIndex parameter needs to be specified, the indexes of multiple rules should be consistent.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-03-31 23:50:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSecurityGroupPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-33ocnj9n
SecurityGroupPolicySet	Yes	No	SecurityGroupPolicySet	Security group policy collection. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
ResourceNotFound	The resource does not exist
UnsupportedOperation.VersionMismatch	The specified security group rule version number is inconsistent with the latest version.
UnsupportedOperation.DuplicatePolicy	Duplicate security group rules.

CreateSecurityGroupWithPolicies

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a security group and add security group rules.

- For the limit on the number of security groups for each project in each region per account, see Security Group Limits.
- The action is Deny all for both inbound and outbound rules of the created security group by default. After a security group is created, you need to call CreateSecurityGroupPolicies to set the security group rules as needed.

Security group rule description:

- Version indicates the version number of a security group rule. Each time you update a security group rule, the version number automatically increases by 1 to prevent the updated rule from expiring. This parameter is optional.
- The Protocol field supports TCP, UDP, ICMP, ICMPV6, GRE, and ALL.
- The CidrBlock field supports any string conforming to the CIDR format standard (complete form). On a basic network, if the CidrBlock field values contain the private IP addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The Ipv6CidrBlock field supports any string conforming to the IPv6 CIDR format standard (complete form). On a basic network, if the Ipv6CidrBlock field values contain the private IPv6 addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The SecurityGroupId field supports the ID of a security group in the same project as the security group to be modified and the ID of the security group to be modified. The private IP addresses of all CVM instances associated with the security group are used as source IP addresses. When this field is specified, the network packet matching process of the rule will change as the CVM instance associated with the corresponding security group changes. The source IP addresses do not need to be modified again.
- The Port field supports a single port number or a port range. For example, 80 or 8000-8010. The Port field is valid only when the Protocol field is set to TCP or UDP. In other words, when the Protocol field is not set to TCP or UDP, the Protocol and Port fields cannot be specified at the same time. Otherwise, an API error will occur.
- The Action field supports only ACCEPT or DROP.
- CidrBlock, Ipv6CidrBlock, SecurityGroupId, and AddressTemplate cannot be specified at the same time. ServiceTemplate cannot be specified if Protocol or Port is specified.
- One request allows you to create rules in only one direction. If the PolicyIndex parameter needs to be specified, the indexes of multiple rules should be consistent.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-10 01:27:31.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSecurityGroupWithPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ProjectId	No	No	String	Project ID. Default value: 0. It can be queried on the project management page in the console. Example: 1
GroupName	Yes	No	String	Security group name. The name can be given freely but must not exceed 60 characters. Example: demo
GroupDescription	Yes	No	String	Security group remarks, up to 100 characters. Example: demo 20230214
SecurityGroupPolicySet	No	No	SecurityGroupPolicySet	Security group policy collection. Example:View

3. Output Parameters

Parameter name	Type	Description
SecurityGroup	SecurityGroup	Security group object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DeleteSecurityGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteSecurityGroup) is used to delete security groups (SecurityGroup).

- Only security groups under the current account are allowed to be deleted.
- If the security group instance ID is referenced in the rules of another security group, it cannot be deleted directly. In such cases, the rules must be modified before the security group can be deleted.
- The deleted security group cannot be recovered. Proceed with caution.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-13 23:22:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSecurityGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-33ocnj9n

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidSecurityGroupID.Malformed	Invalid security group. Invalid security group instance ID.
InvalidParameterValue.Malformed	Invalid input format.
InvalidSecurityGroupID.NotFound	Invalid security group. The security group instance ID does not exist.

DeleteSecurityGroupPolicies

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteSecurityGroupPolicies) is used to delete the security group policies (SecurityGroupPolicy).

- SecurityGroupPolicySet.Version is used to specify the version of the security group to operate on. If the input version number does not match the latest version of the security group, a failure will be returned; if the version is not input, the rule specifying PolicyIndex will be directly deleted.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-07-07 02:13:41.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSecurityGroupPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-ohuuioma
SecurityGroupPolicySet	Yes	No	SecurityGroupPolicySet	Security group policy collection. A single request can only delete one or more rules in one direction. It supports deletion by specifying PolicyIndex and security group policy. Only one method can be used in a request. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
UnsupportedOperation.VersionMismatch	The specified security group rule version number is inconsistent with the latest version.

DescribeDBInstancesWithSecurityGroup

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeDBInstancesWithSecurityGroup) is used for security groups to obtain the bound database instance information.

Default interface request rate limit: 20 times per second.

Interface update time: 2021-10-30 22:48:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDBInstancesWithSecurityGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n. Example: sg-3mf2tgyv
Filters	Yes	No	Array of Filter	Filter criteria. • module - String - (Filter criteria) Database type. • instance-id- String - (Filter criteria) Instance ID. • instance-ip- String - (Filter criteria) Instance IP. Example:View

Parameter name	Required	Allow NULL	Type	Description
Offset	No	No	Int64	Offset. 0 by default. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible objects. Example:
DBInstances	Array of DBInstances	Database instance details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeSecurityGroupAssociationStatistics

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSecurityGroupAssociationStatistics) is used to query the statistics of instances associated with a security group.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-28 18:21:31.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityGroupAssociationStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupIds	Yes	No	Array of String	Security instance ID, e.g., sg-33ocnj9n, which can be obtained through DescribeSecurityGroups. Example: ['sg-75ww503r']

3. Output Parameters

Parameter name	Type	Description
SecurityGroupAssociationStatisticsSet	Array of SecurityGroupAssociationStatistics	Security group associated instance statistics. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeSecurityGroupLimits

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSecurityGroupLimits) is used to query the user's security group quota.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-22 02:10:27.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityGroupLimits
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
SecurityGroupLimitSet	SecurityGroupLimitSet	User security group quota limit. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeSecurityGroupPolicies

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSecurityGroupPolicies) is used to query security group policies.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-11-22 18:58:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityGroupPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be obtained through DescribeSecurityGroups. Example: sg-ohuuioma
Filters	No	No	Array of Filter	Filter criteria. security-group-id - String - The security group ID in the rule. ip - String - IP, supports fuzzy matching for IPv4 and IPv6. address-module - String - IP address template or IP address group template ID. service-module - String - Protocol port template or protocol port group template ID. protocol-type - String - Protocols supported by the security group policy, options: TCP, UDP, ICMP, ICMPV6, GRE, ALL. port - String - Required or Not: No - Protocol port, supports fuzzy matching, ALL for querying all ports. poly - String - Protocol policy, options: ALL for all policies; ACCEPT for allow; DROP for deny. direction - String - Protocol rule, options: ALL for all policies; INBOUND for inbound rules; OUTBOUND for outbound rules. description - String - Protocol description, supports fuzzy matching. Example:View

3. Output Parameters

Parameter name	Type	Description
SecurityGroupPolicySet	SecurityGroupPolicySet	Security group policy collection. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
ResourceNotFound	The resource does not exist

DescribeSecurityGroupReferences

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSecurityGroupReferences) is used to query referenced information of security groups.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:35:10.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityGroupReferences
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupIds	Yes	No	Array of String	An array of security group instance IDs, formatted as ['sg-demoag78']. Example: ['sg-demoag78']

3. Output Parameters

Parameter name	Type	Description
ReferredSecurityGroupSet	Array of ReferredSecurityGroup	Security group reference information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

DescribeSecurityGroups

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSecurityGroups) is used to query security groups.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-21 23:32:36.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupIds	No	No	Array of String	Security group instance ID, e.g., sg-33ocnj9n, which can be obtained through DescribeSecurityGroups. The maximum number of instances per request is 100. The parameter does not support specifying both SecurityGroupIds and Filters simultaneously. Example: ["sg-33ocnj9n"]
Filters	No	No	Array of Filter	Filter criteria. Parameters SecurityGroupIds and Filters must not be specified simultaneously. • security-group-id - String - (Filter criteria) Security group ID. • project-id - Integer - (Filter criteria) Project ID. • security-group-name - String - (Filter criteria) Security group name. • tag-key - String - Required or Not: No - (Filter criteria) Filter by tag key. Refer to example 2 for usage. • tag:tag-key - String - Required or Not: No - (Filter criteria) Filter by tag-key value pair. Replace tag-key with the specific tag-key. Refer to example 3 for usage. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
SecurityGroupSet	Array of SecurityGroup	Security group object. Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifySecurityGroupAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifySecurityGroupAttribute) is used to modify the attributes of a security group (SecurityGroupPolicy).

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-13 23:25:57.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifySecurityGroupAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-33ocnj9n
GroupName	No	No	String	Security group name. The name can be given freely but must not exceed 60 characters. Example: demo
GroupDescription	No	No	String	Security group remarks, up to 100 characters. Example: demo

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifySecurityGroupPolicies

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to reset the outbound and inbound rules of a security group.

- The API deletes all inbound and outbound rules and then adds Egress and Ingress rules. Custom indexes (PolicyIndex) are not supported.
- If SecurityGroupPolicySet.Version is set to 0, all rules will be cleared, but Egress and Ingress rules are skipped.
- The Protocol field supports TCP, UDP, ICMP, ICMPV6, GRE, and ALL.
- The CidrBlock field supports any string conforming to the CIDR format standard (complete form). On a basic network, if the CidrBlock field values contain the private IP addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The Ipv6CidrBlock field supports any string conforming to the IPv6 CIDR format standard (complete form). On a basic network, if the Ipv6CidrBlock field values contain the private IPv6 addresses of devices other than CVM instances under your account, it does not mean that the rule allows you to access these devices. The tenant network isolation rules have a higher priority than the private network rules of security groups.
- The SecurityGroupId field supports the ID of a security group in the same project as the security group to be modified and the ID of the security group to be modified. The private IP addresses of all CVM instances associated with the security group are used as source IP addresses. When this field is specified, the network packet matching process of the rule will change as the CVM instance associated with the corresponding security group changes. The source IP addresses do not need to be modified again.
- The Port field supports a single port number or a port range. For example, 80 or 8000-8010. The Port field is valid only when the Protocol field is set to TCP or UDP.
- The Action field supports only ACCEPT and DROP.
- CidrBlock, Ipv6CidrBlock, SecurityGroupId, and AddressTemplate cannot be specified at the same time. ServiceTemplate cannot be specified if Protocol or Port is specified.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-01 18:27:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifySecurityGroupPolicies
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-ohuuioma
SecurityGroupPolicySet	Yes	No	SecurityGroupPolicySet	Security group rule collection. The SecurityGroupPolicySet object must specify both new egress and ingress rules simultaneously. The SecurityGroupPolicy object does not support custom index (PolicyIndex). Example:View
SortPolicys	No	No	Bool	Sorted security group identifier. When the value is True, it supports sorting of security groups; if SortPolicys does not exist or SortPolicys is False, it modifies the security group rules. Example: False

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ReplaceSecurityGroupPolicy

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ReplaceSecurityGroupPolicy) is used to replace a single security group policy (SecurityGroupPolicy).
A single request can only replace one rule in one direction. You must specify an index (PolicyIndex).

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-01 18:27:56.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ReplaceSecurityGroupPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SecurityGroupId	Yes	No	String	Security group instance ID, e.g., sg-33ocnj9n, which can be accessed through DescribeSecurityGroups. Example: sg-ohuuioma
SecurityGroupPolicySet	Yes	No	SecurityGroupPolicySet	Security group rule collection object. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist
UnsupportedOperation.VersionMismatch	The specified security group rule version number is inconsistent with the latest version.

Subnet APIs
AssignIpv6SubnetCidrBlock

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (AssignIpv6SubnetCidrBlock) is used to allocate IPv6 ranges.

- To allocate an IPv6 range to a subnet, the subnet's VPC must have obtained an IPv6 range. If it is not allocated, allocate an IPv6 range to the subnet's VPC using the AssignIpv6CidrBlock API first. Otherwise, the IPv6 range would be unable to be allocated.
- Each subnet can be allocated only one IPv6 range.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 21:40:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssignIpv6SubnetCidrBlock
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Subnet's VPC ID , e.g., vpc-f49l6u0z . Example: "vpc-cd20bl9o"
Ipv6SubnetCidrBlocks	Yes	No	Array of Ipv6SubnetCidrBlock	List of IPv6 subnet IP ranges allocated. Example:View

3. Output Parameters

Parameter name	Type	Description
Ipv6SubnetCidrBlockSet	Array of Ipv6SubnetCidrBlock	List of IPv6 subnet IP ranges allocated. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
InvalidParameterValue.SubnetRange	Invalid subnet CIDR.
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
MissingParameter	Missing parameters. The request did not carry the required parameter.
LimitExceeded.SubnetCidrBlock	The number of sub-IP range allocated to the sub-net has reached the upper limit.
InvalidParameterValue.Malformed	Invalid input format.

CheckDefaultSubnet

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CheckDefaultSubnet) is used to predict whether it is possible to create a default subnet.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-27 19:52:14.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckDefaultSubnet
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Zone	No	No	String	Availability zone ID where the subnet is located. For different subnets, different availability zones are selected for cross-availability zone disaster recovery. Example: ap-region

3. Output Parameters

Parameter name	Type	Description
Result	Bool	Inspection result. True indicates that a default subnet can be created; False indicates that a default subnet cannot be created. Example: True
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

CheckIpInSubnet

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Determine if an IP is available in a subnet

Default interface request rate limit: 20 times per second.

Interface update time: 2023-07-06 20:23:35.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckIpInSubnet
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPCID Example: vpc-67wlqf6v
SubnetId	Yes	No	String	Subnet instance ID. Example: subnet-8qywqc4y
PrivateIpAddresses	Yes	No	Array of String	VPC IP address Example: 10.2.3.64

3. Output Parameters

Parameter name	Type	Description
message	String	message. ok indicates success. Example: ok
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
ResourceInUse.Address	The specified IP address is already in use.
InvalidParameterValue.Range	The parameter value is not within the specified range.

CreateSubnet

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateSubnet) is used to create a subnet.

- Before a subnet is created, a VPC must be created first.
- After a subnet is successfully created, the subnet IP range cannot be modified. The subnet IP range must fall under the VPC IP range and can be the same as the VPC IP range (when VPC has and only has one subnet). It is recommended to have the subnet IP range in the VPC IP range, and reserve the IP range for other subnets.
- The smallest subnet mask you can create is 28 (with 16 IP addresses), and the largest subnet mask is 16 (with 65,536 IP addresses).
- Within the same VPC, the IP ranges of multiple subnets must not overlap.
- A subnet will automatically be associated with the default routing table upon creation.* When creating a subnet, you can also bind tags, and the list of tags in the response represents the successfully added tags.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:14:22.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSubnet
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	ID of VPC instance to be operated. It can be accessed through VpcId in the returned value of the DescribeVpcs API. Example: vpc-m3ul053f
SubnetName	Yes	No	String	Subnet name, up to 60 bytes in length. Example: demoSubnet
CidrBlock	Yes	No	String	Subnet IP range. The subnet IP range must be within the VPC IP range. Subnet IP ranges must not overlap within a same VPC. Example: 10.8.0.0/16
Zone	Yes	No	String	Availability zone ID where the subnet is located. For different subnets, different availability zones are selected for cross-availability zone disaster recovery. Example: ap-region-1
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
Subnet	Subnet	Subnet object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.SubnetRange	Invalid subnet CIDR.
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.

CreateSubnets

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateSubnets) is for the batch creation of subnets.

- Before a subnet is created, a VPC must be created first.
- After a subnet is successfully created, the subnet IP range cannot be modified. The subnet IP range must fall under the VPC IP range and can be the same as the VPC IP range (when VPC has and only has one subnet). It is recommended to have the subnet IP range in the VPC IP range, and reserve the IP range for other subnets.
- The smallest subnet mask you can create is 28 (with 16 IP addresses), and the largest subnet mask is 16 (with 65,536 IP addresses).
- Within the same VPC, the IP ranges of multiple subnets must not overlap.
- A subnet will automatically be associated with the default routing table upon creation.
- When creating a subnet, you can also bind tags, and the list of tags in the response represents the successfully added tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-15 04:57:52.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSubnets
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-6v2ht8q5. Example: vpc-6v2ht8q5
Subnets	Yes	No	Array of SubnetInput	Subnet object list. Example:View
Tags	No	No	Array of Tag	Specifies the list of tags for binding. Note: These tags are shared by all subnet objects in the list. Specifying a tag separately for each subnet object is not supported. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description
SubnetSet	Array of Subnet	Newly created subnet list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.SubnetRange	Invalid subnet CIDR.
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DeleteSubnet

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteSubnet) is used to delete subnets.

- Before deleting a subnet, clear all resources under the subnet, including CVMs, CLBs, cloud databases, noSql, ENI, and other resources.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-04 23:33:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSubnet
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SubnetId	Yes	No	String	Subnet instance ID, which can be obtained through the SubnetId value returned by the DescribeSubnets API. Example: subnet-pxir56ns

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

DescribeSubnets

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeSubnets) is used to query the list of subnets.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-10-26 03:51:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSubnets
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SubnetIds	No	No	Array of String	Subnet instance ID query, e.g., subnet-pxir56ns. The upper limit of instances per request is 100. Parameters SubnetIds and Filters must not be specified simultaneously. Example: subnet-pxir56ns
Filters	No	No	Array of Filter	Filter criteria. Parameters SubnetIds and Filters must not be specified simultaneously. • subnet-id - String - (Filter criteria) Subnet instance name. • type - Int - (Filter criteria) Subnet type. Default is regular subnet. • vpc-id - String - (Filter criteria) VPC instance ID, e.g., vpc-f49l6u0z. • cidr-block- String - (Filter criteria) Subnet IP range, e.g., 192.168.1.0. • is-default - Boolean - (Filter criteria) Whether it is the default subnet • is-remote-vpc-snat - Boolean - (Filter criteria) Whether it is the VPC SNAT address pool subnet. • subnet name - String - (Filter criteria) Subnet name. • Zone - String - (Filter criteria) Availability zone. • Tag key - String - Required or Not: No - (Filter criteria) Filter by tag key • Tag:tag key - String - Required or Not: No - (Filter criteria) Filter by tag key value. Tag key is replaced with specific tag keys. Refer to example 2 for usage. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example: 10
SubnetSet	Array of Subnet	Subnet object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.Malformed	Invalid input format.

Error Code	Description
ResourceNotFound	The resource does not exist

ModifySubnetAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifySubnetAttribute) is used to modify subnet attributes.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-10 05:51:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifySubnetAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SubnetId	Yes	No	String	Subnet instance ID, e.g., subnet-pxir56ns. Example: subnet-demojkt4
SubnetName	No	No	String	Subnet name, up to 60 bytes in length. Example: NewSubnetName
EnableBroadcast	No	No	String	Whether the Subnet Broadcast is enabled. Example: true

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

UnassignIpv6SubnetCidrBlock

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (UnassignIpv6SubnetCidrBlock) is used to release IPv6 subnet IP ranges.

If a subnet IP range still has IPs occupied which have not been reclaimed, the subnet IP range cannot be released.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-01-10 18:39:42.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UnassignIpv6SubnetCidrBlock
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Subnet's VPC ID , e.g., vpc-f49l6u0z . Example: vpc-q26u781x

Parameter name	Required	Allow NULL	Type	Description
Ipv6SubnetCidrBlocks	Yes	No	Array of Ipv6SubnetCidrBlock	IPv6 subnet IP range list. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied
InvalidParameterValue.Duplicate	Input Parameters are repetitive.

VPC APIs
AssignIpv6CidrBlock

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to allocate IPv6 IP ranges.

- Before using this API, you need to have an existing VPC instance. If you do not have one, you can create it using the API CreateVpc.
- Each VPC can only request one IPv6 IP range.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-30 17:00:18.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssignIpv6CidrBlock
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-f49l6u0z. Example: vpc-f49l6u0z
AddressType	No	No	String	IP range type. 0: GUA, 1: ULA. 0 by default. Example: "GUA"
Ipv6CidrBlock	No	No	String	Ipv6Cidr can be specified only when AddressType is set to an IPv6 CIDR of GUA. For example: 3402:4e00:20:1000::/56. Example: 2001:db8:1a:8000::/56

3. Output Parameters

Parameter name	Type	Description
Ipv6CidrBlock	String	Allocated IPv6 IP ranges, e.g., 3402:4e00:20:1000::/56 Example: 3402:4e00:20:1000::/56
IpAddressType	String	IP address type. IPv4: v4 type; IPv6: v6 type. Example: IPv4/IPv6
ISPType	String	ISP type of the IPv6 CIDR block. Valid values: 'BGP' (default type), 'CMCC', 'CTCC', and 'CUCC'. Example: BGP
AddressType	String	Requested IPv6 CIDR type. Valid values: GUA; ULA. Example: GUA
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
LimitExceeded.CidrBlock	The number of IP ranges allocated to the VPC has reached the upper limit.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceInsufficient.CidrBlock	The IP range resources are insufficient.

AttachClassicLinkVpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create connectivity between a VPC and basic network devices.

- The VPC and basic network devices should be in the same region.
- For more details on the differences between VPC and basic networks, see the VPC product documentation-VPC and Basic Network.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-14 01:26:39.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AttachClassicLinkVpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC Instance ID Example: vpc-gjui0b5t
InstanceIds	Yes	No	Array of String	CVM instance ID Example: ["ins-0x5msjda"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnsupportedOperation.ClassicInstanceIdAlreadyExists	The instance is already bound to the VPC.
UnsupportedOperation.CIDRUnSupportedClassicLink	The specified VPC CIDR range does not support interconnection between the VPC and basic network devices.

CheckAssistantCidr

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CheckAssistantCidr) is used to check whether the auxiliary CIDR conflicts with existing routes, PCs (peer VPC's CIDR), and other resources. If there is an overlap, the overlapping resources will be returned. (This API is in beta. Submit a ticket if you need to use it.)

- Check whether the auxiliary CIDR overlaps with the main CIDR and auxiliary CIDR of the current VPC.
- Check whether the auxiliary CIDR overlaps with the destinations of the routes in the current VPC.
- Check whether the auxiliary CIDR overlaps with the PC, the main CIDR, or auxiliary CIDR under the customer VPC.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-09 22:17:34.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckAssistantCidr
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-6v2ht8q5. Example: vpc-demoag78
NewCidrBlocks	No	No	Array of String	Load CIDR to be added. CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.0.0/24\n"]
OldCidrBlocks	No	No	Array of String	Load balancer CIDR to be deleted. CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.1.0/25\n"]

3. Output Parameters

Parameter name	Type	Description
ConflictSourceSet	Array of ConflictSource	Array of conflicting resource information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

CreateAssistantCidr

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateAssistantCidr) is used to create auxiliary CIDRs in batches.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:13:15.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateAssistantCidr
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-6v2ht8q5. Example: vpc-demoag78
CidrBlocks	Yes	No	Array of String	CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.0.0/24\n"]

3. Output Parameters

Parameter	Type	Description

name		
AssistantCidrSet	Array of AssistantCidr	Auxiliary CIDR array. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.SubnetRange	Invalid subnet CIDR.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

CreateDefaultVpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateDefaultVpc) is used to create a default VPC.

The default VPC is suitable for quick start and launching public instances. You can use it like any other VPC. If you want to create a standard VPC, i.e., specify the VPC name, VPC IP range, subnet IP range, and subnet availability zone, use the regular API for creating VPCs (CreateVpc).

Normally, this API does not necessarily produce a default VPC, but is determined by the network attributes of the user's account (DescribeAccountAttributes).

- It supports basic networks and VPCs, and returns VpcId of 0.
- It supports VPCs only, and returns default VPC information.

You can also force a return of the default VPC through the Force parameter.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-30 17:21:29.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDefaultVpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Zone	No	No	String	Subnet's availability zone ID. If it is not specified, an availability zone will be selected randomly. Example: ap-region-1
Force	No	No	Bool	Whether to force return to the default VPC. Example: true

3. Output Parameters

Parameter name	Type	Description
Vpc	DefaultVpcSubnet	Default VPC and subnet ID Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

CreateLocalGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create the local gateway for CDC.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-06-02 01:16:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLocalGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CdcId	Yes	Yes	String	CDC instance ID. Example: cluster-gbo27yc4
LocalGatewayName	Yes	Yes	String	Local gateway name. Example: demo
VpcId	Yes	Yes	String	VPC instance ID. Example: vpc-m0c2kcun

3. Output Parameters

Parameter name	Type	Description
LocalGateway	LocalGateway	Local gateway information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InternalError	
UnsupportedOperation.LocalGatewayAlreadyExists	The specified CDC instance already has a local gateway.

CreateVpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create a VPC.

- The smallest IP range a user can create has a subnet mask of 28 (16 IP addresses), and the largest IP range has a subnet mask of 16 (65,536 IP addresses). For VPC IP range planning, see the VPC IP range planning documentation.
- The number of VPC resources that can be created in the same region is limited. For details, see VPC Usage Limits. If you need to increase the limit, contact online customer service.
- Tags can be bound to the VPC during its creation. The tag list in the response represents the successfully added tags.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-04-28 20:19:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcName	Yes	No	String	VPC name, up to 60 bytes in length. Example: demoVPC
CidrBlock	Yes	No	String	VPC CIDR, limited to three private IP ranges: 10.0.0.0/16, 172.16.0.0/16, and 192.168.0.0/16. Example: 10.8.0.0/16
EnableMulticast	No	No	String	Whether to enable multicast. True: Enable; False: Disable. Example: true
DnsServers	No	No	Array of String	DNS address, up to 4. Example: ['11.10.1.13', '11.10.1.11']
DomainName	No	No	String	Domain name Example: cloud.com
Tags	No	No	Array of Tag	Specifies the list of tags for binding. For example, [{"Key": "city", "Value": "region"}]. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Vpc	Vpc	VPC object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
MissingParameter	Missing parameters. The request did not carry the required parameter.

DeleteAssistantCidr

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteAssistantCidr) is used to delete an auxiliary CIDR.

Default interface request rate limit: 100 times per second.

Interface update time: 2024-10-31 18:22:42.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteAssistantCidr
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-6v2ht8q5. Example: vpc-demoag78
CidrBlocks	Yes	No	Array of String	CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.0.0/24\n"]

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

DeleteLocalGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to delete the local gateway of CDC.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-06-02 01:16:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLocalGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LocalGatewayId	Yes	Yes	String	Local gateway instance ID. Example: lgw-jkt4rfgt
VpcId	No	Yes	String	VPC instance ID. Example: vpc-m0c2kcun
CdcId	Yes	Yes	String	CDC instance ID. Example: cluster-gbo27yc4

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InternalError	

DeleteVpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteVpc) is used to delete a VPC.

- Before deletion, ensure there are no related resources within the VPC, e.g., CVMs, CDBs, NoSQL, VPN gateways, Direct Connect gateways, CLBs, PCs, interconnecting basic network devices, etc.
- Deleting a VPC is an irreversible operation. Proceed with caution.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-04 23:51:25.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-3ptx9s8b

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

DescribeAccountAttributes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAccountAttributes) is used to query private attributes of a user account.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-17 00:06:43.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAccountAttributes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
AccountAttributeSet	Array of AccountAttribute	User account attribute object Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeAssistantCidr

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeAssistantCidr) is used to query the auxiliary CIDR list.

Default interface request rate limit: 100 times per second.

Interface update time: 2024-10-31 18:22:10.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssistantCidr
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcIds	No	No	Array of String	Array of VPC instance IDs, e.g., [vpc-6v2ht8q5]]. Example: vpc-6v2ht8q5
Filters	No	No	Array of Filter	Filters. Parameters NetworkInterfaceIds and Filters must not be specified simultaneously. • vpc-id - String - (Filters) VPC instance ID, e.g., vpc-f49l6u0z. Example:View
Offset	No	No	Uint64	Offset. 0 by default. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
AssistantCidrSet	Array of AssistantCidr	Eligible auxiliary CIDR array. Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DescribeClassicLinkInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeClassicLinkInstances) is used to query the interconnection list between VPC and basic network devices.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-12-04 23:31:49.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeClassicLinkInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of FilterObject	Filter criteria. • vpc-id - String - (Filter criteria) VPC instance ID. • vm-ip - String - (Filter criteria) Basic network CVM IP. Example:View
Offset	No	No	String	Offset Example: 0

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	String	Returned quantity Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example:
ClassicLinkInstanceSet	Array of ClassicLinkInstance	VPC and basic network interconnection device. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Range	The parameter value is not within the specified range.

DescribeIpv6Section

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

DescribeIpv6Section

Default interface request rate limit: 20 times per second.

Interface update time: 2025-04-28 20:23:41.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIpv6Section
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressType	No	No	String	Address type Example: GUA/ULA
EnableSplit	No	No	Uint64	Whether to support automatic splitting. Example: 0: not supported; 1: customization supported.
Offset	No	No	Uint64	Offset Example: 0
Limit	No	No	Uint64	Returned quantity Example: 100

Parameter name	Required	Allow NULL	Type	Description
Ipv6CidrBlock	No	No	String	IPv6 address range. Example: 3402:4e00:20:1200::/56

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example:
Ipv6SectionSet	Ipv6SectionSet	Array of IPv6 address pool objects. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
UnsupportedOperation.ActionNotFound	The API does not exist.

DescribeIpv6Vpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

DescribeIpv6Vpc

Default interface request rate limit: 20 times per second.

Interface update time: 2024-08-09 18:22:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIpv6Vpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
AddressType	No	No	String	IPv6 address type. Example: GUA/ULA
EnableSplit	No	No	Uint64	Whether to support automatic splitting. Example: 0: not supported; 1: customization supported.
SectionId	No	No	Uint64	Information of the associated IPv6 address pool. Example: 1
Offset	No	No	Uint64	Offset Example: 0

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Returned quantity Example: 100
Ipv6CidrBlock	No	No	String	IPv6 address range. Example: 3402:4e00:20:1200::/56

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example:
Ipv6VpcSet	Array of Ipv6VpcSet	Array of VPC associated with IPv6 objects. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
UnsupportedOperation.ActionNotFound	The API does not exist.

DescribeLocalGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to query the local gateway of CDC.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-28 11:26:17.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLocalGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	Yes	Array of Filter	Query conditions: vpc-id: Filters by VPC ID; local-gateway-name: Filters by local gateway name, supporting fuzzy search; local-gateway-id: Filters by local gateway instance ID; cdc-id: Filters by CDC instance ID. Example:View
Offset	No	Yes	Int64	The offset, with a default value of 0. For more details about Offset , see the relevant section in the API introduction. Example: 0
Limit	No	Yes	Int64	The number of returned results, with a default value of 20 and a maximum value of 100. For more details about Limit , see the relevant section in the API Overview. Example: 20

3. Output Parameters

Parameter name	Type	Description
LocalGatewaySet	Array of LocalGateway	Collection of local gateway information. Example:View
TotalCount	Int64	Total number of local gateways. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InternalError	

DescribeNmsCidrs

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Query non-standard IP ranges

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-22 22:51:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNmsCidrs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
TotalCount	No	No	Uint64	Total number Example: 100
CidrDetailSet	No	No	CidrDetailSet	Non-standard IP range details Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
TotalCount	Uint64	Total number Example:
CidrDetaliSet	CidrDetailSet	Non-standard IP range details Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeUsedIpAddress

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ApplyPrivateIpAddress) is used to query the usage of IP addresses in the subnet or VPC.
If the IP address is occupied, the resource category and ID of the occupied IP address are returned. If it is not occupied, a null value is returned.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-09-01 11:37:29.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeUsedIpAddress
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	Yes	Array of Filter	Filtering condition. The IpAddresses and Filters parameters cannot be specified simultaneously. The supported filtering conditions are as follows: • ip-addresses: IP address. • resource-id: resource ID. Example:View
Offset	No	Yes	Uint64	Offset. 0 by default. Example: 0
Limit	No	Yes	Uint64	Number of returns, 20 by default, up to 100. Example: 10
VpcId	Yes	Yes	String	VPC instance ID. Example: vpc-a26u781x
SubnetId	No	Yes	String	Subnet instance ID. Example: subnet-amqye6ew
IpAddresses	No	Yes	Array of String	Queries the list of occupied IP addresses. These IP addresses need to be within the VPC or subnet. Up to 100 IP addresses can be queried at a time. Example: ["192.168.2.10", "10.0.1.10"]

3. Output Parameters

Parameter name	Type	Description
IpAddressStates	Array of IpAddressStates	Information on resources that occupy the IP addresses. Example:View
TotalCount	Uint64	Returns the number of occupied resources. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.ParameterMismatch	

DescribeVpcInstances

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpcInstances) is used to query the list of CVM instances under a VPC.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-04-10 01:37:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	Yes	No	Array of Filter	Filter criteria. Parameters RouteTableIds and Filters must not be specified simultaneously. • vpc-id - String - (Filter criteria) VPC instance ID, e.g., vpc-f49l6u0z. • instance-id - String - (Filter criteria) CVM instance ID. • instance-name - String - (Filter criteria) CVM name. Example:View
Offset	No	No	Uint64	Offset. Example: 0
Limit	No	No	Uint64	Number of request objects. Example: 20

3. Output Parameters

Parameter name	Type	Description
InstanceSet	Array of CvmInstance	CVM instance list. Example:View
TotalCount	Uint64	Number of CVM instances that meet the criteria. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.Range	The parameter value is not within the specified range.

DescribeVpcIpv6Addresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpcIpv6Addresses) is used to query VPC IPv6 information.
Only used IPv6 addresses can be queried. When an unused IP is queried, this API does not report an error, but it does not appear in the return result.

Default interface request rate limit: 20 times per second.

Interface update time: 2019-03-13 02:10:08.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcIpv6Addresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-f49l6u0z. Example: vpc-rkxd3pgh
Ipv6Addresses	No	No	Array of String	IP address list. Batch query supports up to 10 items in a single request. Example: ["2402:4e00:1015:4a00::/56"]
Offset	No	No	Uint64	Offset. Example: 0
Limit	No	No	Uint64	Returned quantity. Example: 20

3. Output Parameters

Parameter name	Type	Description
Ipv6AddressSet	Array of	IPv6 address list.

Parameter name	Type	Description
	VpcIpv6Address	Example:View
TotalCount	Uint64	Total number of IPv6 addresses. Example: 6
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeVpcLimits

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Obtain VPC quota. Some VPC quotas have region attributes.
Value range of LimitTypes:

- appid-max-vpcs (number of VPCs each developer can create per region)
- vpc-max-subnets (number of subnets each VPC can have)
- vpc-max-route-tables (number of routing tables each VPC can have)
- route-table-max-policies (number of policies each routing table can have)
- vpc-max-vpn-gateways (number of VPN gateways each VPC can have)
- appid-max-custom-gateways (number of customer gateways each developer can create)
- appid-max-vpn-connections (number of VPN tunnels each developer can create)
- custom-gateway-max-vpn-connections (number of VPN tunnels each customer gateway can have)
- vpn-gateway-max-custom-gateways (number of tunnels each VPNGW can have)
- vpc-max-network-acls (number of network ACLs each VPC can have)
- network-acl-max-inbound-policies (number of inbound rules each network ACL can have)
- network-acl-max-outbound-policies (number of outbound rules each network ACL can have)
- vpc-max-vpcpeers (number of PCs each VPC can have)
- vpc-max-available-vpcpeers (number of effective PCs each VPC can have)
- vpc-max-basic-network-interconnections (number of interconnections between the basic network CVM and VPC that each VPC can have)
- direct-connection-max-snats (number of SNATs each Direct Connect gateway can have)
- direct-connection-max-dnats (number of DNATs each Direct Connect gateway can have)
- direct-connection-max-snapts (number of SNAPTs each Direct Connect gateway can have)
- direct-connection-max-dnapts (number of DNAPTs each Direct Connect gateway can have)
- vpc-max-nat-gateways (number of NAT gateways each VPC can have)
- nat-gateway-max-eips (number of public IPs each NAT can purchase)
- vpc-max-enis (number of ENIs each VPC can have)
- vpc-max-havips (number of HAVIPs each VPC can have)
- eni-max-private-ips (number of private IPs each ENI can bind (ENI not bound to a child machine))
- nat-gateway-max-dnapts (number of DNAPTs each NAT gateway can have)
- vpc-max-ipv6s (number of IPv6 addresses that can be allocated to each VPC)
- eni-max-ipv6s (number of IPv6 addresses that can be allocated to each ENI)
- vpc-max-assistant_cidrs (number of auxiliary CIDR blocks that can be allocated to each VPC).

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-27 19:48:40.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcLimits
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LimitTypes	Yes	No	Array of String	Quota name. A maximum of 100 quota types can be queried at once. Example: appid-max-vpcs

3. Output Parameters

Parameter name	Type	Description
VpcLimitSet	Array of VpcLimit	VPC quota Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

DescribeVpcPrivateIpAddresses

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpcPrivateIpAddresses) is used to query VPC private IP information.

Only used IPs can be queried. When an unused IP is queried, this API does not report an error, but it does not appear in the return result.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-01-10 18:58:39.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcPrivateIpAddresses
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-f49l6u0z. Example: vpc-rkxd3pgh
PrivateIpAddresses	Yes	No	Array of String	Private IP address list. Batch query supports up to 10 items in a single request. Example: ["10.4.2.2\n","10.4.2.3\n","10.4.2.17\n"]

3. Output Parameters

Parameter name	Type	Description
VpcPrivateIpAddressSet	Array of VpcPrivateIpAddress	List of private IP address information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

Error Code	Description
ResourceNotFound	The resource does not exist
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

DescribeVpcs

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpcs) is used to query the list of VPCs.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-04-17 00:08:55.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcIds	No	No	Array of String	VPC instance ID, e.g., vpc- f49l6u0z. The upper limit of instances per request is 100. Parameters VpcIds and Filters must not be specified simultaneously. Example: vpc-f49l6u0z
Filters	No	No	Array of Filter	Filter criteria. Parameters VpcIds and Filters must not be specified simultaneously. • vpc-name - String - (Filter criteria) VPC instance name. • is-default - String - (Filter criteria) Whether it is defaulted to VPC. • vpc-id - String - (Filter criteria) VPC instance ID, e.g., vpc-f49l6u0z. • cidr-block - String - (Filter criteria) CIDR of VPC. • tag-key - String - Required or Not: No - (Filter criteria) Filter by tag key. • tag:tag-key - String - Required or Not: No - (Filter criteria) Filter by tag-key value pair. Replace tag-key with the specific tag-key. Refer to example 2 for usage. Example:View
Offset	No	No	String	Offset. 0 by default. Example: 0
Limit	No	No	String	Number of returns, 20 by default, up to 100. Example: 2

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible objects. Example: 1
VpcSet	Array of Vpc	VPC object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
UnauthorizedOperation	Unauthorized operation

Error Code	Description
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DetachClassicLinkVpc

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DetachClassicLinkVpc) is used to delete the intercommunication between a VPC and a basic network device.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-18 03:40:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DetachClassicLinkVpc
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-gjui0b5t
InstanceIds	Yes	No	Array of String	Query of CVM instance ID, e.g., ins-r8hr2upy. Example: ["ins-0x5msjda"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyAssistantCidr

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyAssistantCidr) is used for batch modification of auxiliary CIDRs, supporting both addition and deletion.

Default interface request rate limit: 100 times per second.

Interface update time: 2024-10-31 18:23:14.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAssistantCidr
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-6v2ht8q5. Example: vpc-demoag78
NewCidrBlocks	No	No	Array of String	Load CIDR to be added. CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.0.0/24\n"]
OldCidrBlocks	No	No	Array of String	Load balancer CIDR to be deleted. CIDR array, e.g., ["10.0.0.0/16", "172.16.0.0/16"]. Example: ["172.16.0.0/24\n"]

3. Output Parameters

Parameter name	Type	Description
AssistantCidrSet	Array of AssistantCidr	Auxiliary CIDR array. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.

ModifyLocalGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify the local gateway of CDC.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-06-02 01:16:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLocalGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LocalGatewayName	Yes	Yes	String	Local gateway name. Example: demo
CdcId	Yes	Yes	String	CDC instance ID. Example: cluster-gbo27yc4
VpcId	No	Yes	String	VPC instance ID. Example: vpc-m0c2kcun
LocalGatewayId	Yes	Yes	String	Local gateway instance ID. Example: lgw-jkt4ceww

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InvalidParameter	Invalid input parameters.
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InternalError	

ModifyVpcAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyVpcAttribute) is used to modify the related attributes of a VPC.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-04-25 01:06:30.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpcAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc- f49l6u0z. The upper limit of instances per request is 100. Parameters VpcIds and Filters must not be specified simultaneously. Example: vpc-m7sr81gh
VpcName	No	No	String	VPC name, which can be named arbitrarily, but must not exceed 60 characters. Example: Mydemo
EnableMulticast	No	No	String	Whether multicast is enabled. True: Enabled, False: Disabled. Example: true
DnsServers	No	No	Array of String	DNS address, up to 4 addresses. The first one is defaulted to the primary one, and the rest are backups. Example: ['11.10.1.13', '11.10.1.11']
DomainName	No	No	String	Domain name Example: vpc.cloud.com

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ResetHaVip

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to unbind an ENI from an HAVIP.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-06-21 10:36:48.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetHaVip
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HaVipId	Yes	No	String	Unique ID of HAVIP , e.g., havip-9o233uri . Example: havip-7tqt5jn6
NetworkInterfaceId	No	No	String	Currently, only null strings are supported for unbinding ENIs. Example: eni-7tqt5jn6

3. Output Parameters

Parameter name	Type	Description
taskId	Int64	Des task taskId Example: 213415
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

UnassignIpv6CidrBlock

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (UnassignIpv6CidrBlock) is used to release IPv6 ranges.

If an IP range still has IPs occupied which have not been reclaimed, the IP range cannot be released.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-01-10 18:46:12.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UnassignIpv6CidrBlock
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, e.g., vpc-f49l6u0z. Example: vpc-f49l6u0z
Ipv6CidrBlock	No	No	String	IPv6 IP range, e.g., 3402:4e00:20:1000::/56 . Example: 3402:4e00:20:1000::/56

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
ResourceInUse	Resources occupied

VPN Gateway APIs
CreateCustomerGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateCustomerGateway) is used to create customer gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2025-09-28 11:23:43.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateCustomerGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CustomerGatewayName	Yes	No	String	Customer gateway name, which can be named arbitrarily, but must not exceed 60 characters. Example: demo-cgw
IpAddress	Yes	No	String	Public IP of customer gateway. Example: 58.211.1.12

3. Output Parameters

Parameter name	Type	Description
CustomerGateway	CustomerGateway	Customer gateway object Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
VpcLimitExceeded	The application number of VPC resources in the specified region has reached the upper limit.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.

CreateGatewayVpnSSLClient

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to create an SSL VPN client.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 23:00:58.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateGatewayVpnSSLClient
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	E.g., vpc-7izaqk5h. Example: vpc-jaxf2k23
VpnGatewayId	Yes	No	String	VPN gateway instance ID, which is in the format of vpngw-goa5jz6j. Example: vpngw-1u2xtmbz
SSLVpnServerId	Yes	No	String	SSL VPN server instance ID. Example: vpns-jaif7k23
SSLVPNClientName	Yes	No	String	SSL VPN Client Name Example: client-name

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	taskid Example:
SslVpnClientId	String	SSL VPN client ID, which is in the format of vpnc-a4151cac. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.
ResourceNotFound	The resource does not exist

CreateVpnConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateVpnConnection) is used to create a VPN tunnel.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-01-18 01:22:36.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpnConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-gapcv96p
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-1w9tue3d
CustomerGatewayId	Yes	No	String	Customer gateway ID, e.g., cgw-2wqq41m9, which can be queried through the DescribeCustomerGateways API. Example: cgw-qa9sxpy7
VpnConnectionName	Yes	No	String	Channel name. The name can be given arbitrarily, but must not exceed 60 characters. Example: demo_CONN
PreShareKey	Yes	No	String	Preshared key. Example: 654321
SecurityPolicyDatabases	Yes	No	Array of SecurityPolicyDatabase	SPD policy group, for example: {"10.0.0.5/24": ["172.jkt.10.5/16"]}. Here, 10.0.0.5/24 represents the VPC's private IP range, and 172.jkt.10.5/16 represents the IDC's IP range. Users can specify which IP ranges within the VPC are allowed to communicate with specific IP ranges in their IDC. Example:View
IKEOptionsSpecification	No	No	IKEOptionsSpecification	IKE (Internet Key Exchange) configuration, which involves a set of self-protection mechanisms for user-configured network security protocols. Example:View
IPSECOptionsSpecification	No	No	IPSECOptionsSpecification	IPSec session security settings. Example:View

3. Output Parameters

Parameter name	Type	Description
VpnConnection	VpnConnection	Tunnel instance object. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidParameterValue.VpcCidrConflict	The destination IP range conflicts with the current VPC's CIDR.

CreateVpnGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (CreateVpnGateway) is used to create VPN gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2020-11-12 00:12:20.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpnGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	VPC instance ID, which can be obtained through the VpcId returned by the DescribeVpcs API. Example: vpc-ngenl4az
VpnGatewayName	Yes	No	String	VPN gateway name, up to 60 bytes in length. Example: demo_POSTPAID_VPNGW
InstanceChargeType	No	No	String	VPN gateway billing mode. PREPAID: prepaid, i.e., monthly subscription, POSTPAID_BY_HOUR: postpaid, i.e., pay-as-you-go. The default is POSTPAID_BY_HOUR. If a prepaid mode is specified, the parameter InstanceChargePrepaid is required. Example: POSTPAID_BY_HOUR
InternetMaxBandwidthOut	Yes	No	Uint64	Public network bandwidth setting. Available bandwidth options: 5, 10, 20, 50, 100. Unit: Mbps. Example: 5
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, namely setting of parameters related to monthly subscription. Through this parameter, you can specify the duration of purchase for monthly subscription instances, whether to set auto-renewal, and other attributes. This parameter is required when the specified instance is subject to a payment mode of prepaid. Example:View
Zone	No	No	String	Availability zone. For example, ap-region-2. Example: ap-region
Type	No	No	String	VPN gateway type. Value CCN indicates CCN type VPN gateway. Example: CCN
IspType	No	No	String	Public IP ISP Example: 5
VsModelTag	No	No	String	VPN model tag, e.g., VS_VPN_INTEL. Example: vs_vpn_intel

3. Output Parameters

Parameter name	Type	Description
VpnGateway	VpnGateway	VPN gateway object Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.VpnConnCidrConflict	The destination IP range conflicts with the CIDR of current VPN tunnel.
InvalidVpcId.Malformed	Invalid VPC. The VPC instance ID is invalid.
InvalidVpcId.NotFound	Invalid VPC. The VPC resource does not exist.
InvalidParameterValue	The parameter value is invalid.

CreateVpnGatewaySSLServer

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

Create SSL VPN service

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 22:59:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateVpnGatewaySSLServer
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcId	Yes	No	String	Unique VPC ID, e.g., vpc-7izaqk5h. Example: vpc-cd20bl9o
VpnGatewayId	Yes	No	String	VPN instance ID, e.g., vpngw-7izaqk5h. Example: vpngw-1u2xtmbz
SSLVpnServerName	Yes	No	String	SSL VPN service name Example: server-name
LocalAddress	Yes	No	String	Local IP range Example: 10.0.0.0/16
RemoteAddress	Yes	No	String	Peer IP range Example: 172.0.0.0/16
SSLVpnProtocol	No	No	String	SSL VPN server listening protocol. The default value is UDP. Currently, only UDP is supported (UDP by default). Example: UDP
SSLVpnPort	No	No	Int64	SSL VPN server listening protocol port. The default value is 1194. Currently, only 1194 is supported (1194 by default). Example: 1194
EncryptAlgorithm	No	No	String	Encryption algorithm, AES-128 by default. Only AES-128 is supported in phase I (AES-128 by default). Example: AES-128-CBC
IntegrityAlgorith	No	No	String	Encryption algorithm. The default is HMAC-SHA1, supporting only HMAC-SHA1 in phase I (HMAC-SHA1 by default). Example: SHA1
Compress	No	No	Bool	Support for compression. Default is false, which indicates no compression. Only false is supported in phase I (true is 1; false is 0. Default: 0) Example: False
MaxConnection	No	No	Int64	Maximum number of connections. Values: 5, 10, 20, 50, 100 (a default value is required) (Default value: 5) Example: 5

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	Des task taskId Example:
SslVpnServerId	String	SSL VPN server instance ID. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DeleteCustomerGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteCustomerGateway) is used to delete customer gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-23 01:08:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteCustomerGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CustomerGatewayId	Yes	No	String	Customer gateway ID, e.g., cgw-2wqq41m9, which can be queried through the DescribeCustomerGateways API. Example: cgw-2wqq41m9

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DeleteVpnConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteVpnConnection) is used to delete VPN tunnels.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-02 18:25:50.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpnConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-4wx012fv
VpnConnectionId	Yes	No	String	VPN tunnel instance ID, e.g., vpnx-f49l6u0z. Example: vpnx-f49l6u0z

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DeleteVpnGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DeleteVpnGateway) is used to delete VPN gateways. Currently, only the deletion of running pay-as-you-go IPSEC gateway instances is supported.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-02-08 01:36:41.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpnGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-ox3thdg1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidVpnGatewayId.Malformed	Invalid VPN gateway. VPN instance ID is invalid.
InvalidVpnGatewayId.NotFound	Invalid VPN gateway. The VPN instance does not exist. Verify whether the resource information you entered is correct.

DeleteVpnGatewaySSLClient

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to delete an SSL VPN client.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 23:01:22.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpnGatewaySSLClient
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	The VPN gateway ID, such as vpngw-demoag78. Example: vpngw-1u2xtmbz
SSLVpnClientId	Yes	No	String	SSL VPN client ID, which is in the format of vpnc-a4151cac. Example: vpnc-a4151cac
VpcId	Yes	No	String	VPC ID, which is in the format of vpc-124axafc. Example: vpc-124axafc

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	taskid Example: 65535
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DeleteVpnGatewaySSLServer

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to delete an SSL VPN server.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 22:59:39.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteVpnGatewaySSLServer
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway ID, which is in the format of vpngw-goa5jz6j. Example: vpngw-1u2xtmbz
SSLVpnServerId	Yes	No	String	SSL VPN Client Instance ID Example: vpns-awe1241c
VpcId	Yes	No	String	VPC Instance ID Example: vpc-67wlqf6v

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	taskid Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DescribeCustomerGatewayVendors

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeCustomerGatewayVendors) is used to query the information on supported customer gateway vendors.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-23 01:15:16.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCustomerGatewayVendors
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
CustomerGatewayVendorSet	Array of CustomerGatewayVendor	Object of customer gateway vendor information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeCustomerGateways

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeCustomerGateways) is used to query the list of customer gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-03-29 19:27:35.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCustomerGateways
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CustomerGatewayIds	No	No	Array of String	Customer gateway ID, e.g., cgw-2wqq41m9. The upper limit of instances per request is 100. Parameters CustomerGatewayIds and Filters must not be specified simultaneously. Example: cgw-2wqq41m9
Filters	No	No	Array of Filter	Filtering conditions are detailed in the table below: Instance Filtering Conditions Table. Each request can include up to 10 Filters, with a maximum of 5 values for each Filter.Values. The parameters CustomerGatewayIds and Filters cannot be specified simultaneously. • customer-gateway-id - String - (filtering condition) unique ID of the user gateway, such as cgw-mgp33pll . • customer-gateway-name - String - (filtering condition) name of the user gateway, such as demo-cgw . • ip-address - String - (filtering condition) public network address, such as 58.211.1.12 . Example:View
Offset	No	No	Uint64	Offset. The default value is 0. For further introduction about Offset, refer to the relevant sections in the API Overview. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
CustomerGatewaySet	Array of CustomerGateway	Customer gateway object list Example:View
TotalCount	Uint64	Number of eligible instances. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeVpcResourceDashboard

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpcResourceDashboard) is used to view the VPC resource information.

Default interface request rate limit: 100 times per second.

Interface update time: 2022-10-27 02:55:24.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpcResourceDashboard
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpcIds	Yes	No	Array of String	VPC instance ID, e.g., vpc-f1xjkw1b. Example: ['vpc-q26u781x', 'vpc-1yfqkcw1']

3. Output Parameters

Parameter name	Type	Description
ResourceDashboardSet	Array of ResourceDashboard	Resource object list. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

DescribeVpnConnections

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpnConnections) is used to query the VPN tunnel list.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-10-23 04:36:13.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpnConnections
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnConnectionIds	No	No	Array of String	VPN tunnel instance ID, e.g., vpnx-f49l6u0z. The maximum number of instances per request is 100. Parameters VpnConnectionIds and Filters must not be specified simultaneously. Example: vpnx-f49l6u0z
Filters	No	No	Array of Filter	Filtering conditions. Each request can include up to 10 Filters, with a maximum of 5 values for each Filter.Values. The parameters VpnConnectionIds and Filters cannot be specified simultaneously. • vpc-id - String - VPC instance ID, such as vpc-0a36uwkr . • vpn-gateway-id - String - VPN gateway instance ID, such as vpngw-p4lmqawn . • customer-gateway-id - String - customer gateway instance ID, such as cgw-l4rblw63 . • vpn-connection-name - String - channel name, such as demo-vpn . • vpn-connection-id - String - channel instance ID, such as vpnx-5p7vkch8" . Example:View
Offset	No	No	Uint64	Offset. The default value is 0. For further introduction about Offset, refer to the relevant sections in the API Overview. Example: 0
Limit	No	No	Uint64	Number of returns, 20 by default, up to 100. Example: 10

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example: 1
VpnConnectionSet	Array of VpnConnection	VPN tunnel instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter.Coexist	The parameters must not be specified simultaneously.

DescribeVpnGatewayCcnRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpnGatewayCcnRoutes) is used to query VPN Gateway CCN routes.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-31 20:12:32.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpnGatewayCcnRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID Example: vpngw-jj72x8gx
Offset	No	No	Uint64	Offset Example: 0
Limit	No	No	Uint64	Returned quantity Example: 10

3. Output Parameters

Parameter name	Type	Description
RouteSet	Array of VpngwCcnRoutes	List of CCN routes (IDC IP ranges). Example:View
TotalCount	Uint64	Number of eligible objects. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.

DescribeVpnGatewaySSLClients

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to query an SSL VPN client.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 23:02:00.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpnGatewaySSLClients
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SSLVpnClientIds	No	No	Array of String	SSL VPN client instance ID. Example: ['vpnc-n5hvzrbk', 'vpnc-jbm6ft08']
Filters	No	No	Array of Filter	Filter Criteria Example:View
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Returned quantity Example: 10

3. Output Parameters

Parameter name	Type	Description
SSLVpnClientSet	Array of SSLVpnClient	SSL VPN client instance. Example:View
TotalCount	Int64	Quantity Example: 3
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see

public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DescribeVpnGatewaySSLServers

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to query an SSL VPN server.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 21:00:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpnGatewaySSLServers
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SSLVpnServerIds	No	No	Array of String	SSL VPN Client Instance ID Example: ['vpns-n5hvzrbk', 'vpns-jbm6ft08']
Filters	No	No	Array of Filter	Filter Criteria Example:View
Offset	No	No	Int64	Offset. Default value: 0 Example: 0
Limit	No	No	Int64	Returned quantity Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible instances. Example: 3
SSLVpnSeverSet	Array of SSLVpnServer	SSL VPN client instance ID. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see

public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DescribeVpnGateways

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DescribeVpnGateways) is used to query a list of VPN gateways.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-11-09 00:58:10.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVpnGateways
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayIds	No	No	Array of String	VPN gateway instance ID, e.g., vpngw-f49l6u0z. The maximum number of instances per request is 100. Parameters VpnGatewayIds and Filters must not be specified simultaneously. Example: vpngw-5aluhh9t
Filters	No	No	Array of FilterObject	Filter conditions. The parameters VpnGatewayIds and Filters cannot be specified at the same time. • vpc-id - String - VPC instance ID for filtering. For example, vpc-f49l6u0z. • vpn-gateway-id - String - VPN gateway instance ID for filtering. For example, vpngw-5aluhh9t. • vpn-gateway-name - String - VPN gateway instance name for filtering. • type - String - VPN gateway type for filtering. Valid values: 'IPSEC' and 'SSL'. • public-ip-address - String - Public IP address for filtering. • renew-flag - String - Gateway renewal type. 'NOTIFY_AND_MANUAL_renew': manual renewal; 'NOTIFY_AND_AUTO_renew': automatic renewal. • zone - String - VPN gateway availability zone for filtering. For example, ap-region-2. Example:View
Offset	No	No	Uint64	Offset Example: 0
Limit	No	No	Uint64	Number of Request Objects Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of eligible instances. Example: 1
VpnGatewaySet	Array of VpnGateway	VPN gateway instance detail list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidVpnGatewayId.Malformed	Invalid VPN gateway. VPN instance ID is invalid.
InvalidVpnGatewayId.NotFound	Invalid VPN gateway. The VPN instance does not exist. Verify whether the resource information you entered is correct.

DisableVpnGatewaySSLClientCert

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to disable a client certificate.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 23:00:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisableVpnGatewaySSLClientCert
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VpngwID, e.g., vpngw-goa5jz6j. Example: vpngw-1u2xtmbz
SSLVpnClientId	Yes	No	String	SSL VPN Client Instance ID Example: vpnc-cawt213
VpcId	Yes	No	String	VPC instance ID. Example: vpc-12awc5ac

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	TaskId Example: 12412545
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

DownloadCustomerGatewayConfiguration

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (DownloadCustomerGatewayConfiguration) is used to download VPN tunnel configuration.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-02 18:01:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DownloadCustomerGatewayConfiguration
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-p4lmbqwn
VpnConnectionId	Yes	No	String	VPN tunnel instance ID, e.g., vpnx-f49l6u0z. Example: vpnx-4p6vkch3
CustomerGatewayVendor	Yes	No	CustomerGatewayVendor	Customer gateway vendor information object, which can be obtained through DescribeCustomerGatewayVendors. Example:View
InterfaceName	Yes	No	String	Physical API name of the channel access device. Example: eth0

3. Output Parameters

Parameter name	Type	Description
CustomerGatewayConfiguration	String	XML format configuration information. Example: # VPC utilizes unique identifiers to manipulate the configuration of\r\n# a VPN Connection. Each VPN Connection is assigned an identifier and is\r\n# associated with Virtual Private Gateway ...
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist
InvalidParameter	Invalid input parameters.

DownloadVpnGatewaySSLClientCert

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to download an SSL VPN client certificate.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 22:35:57.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DownloadVpnGatewaySSLClientCert
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SSLVpnClientId	Yes	No	String	SSL VPN client ID, which is in the format of vpnc-cawt213. Example: vpnc-cawt213

3. Output Parameters

Parameter name	Type	Description
Data	Array of	Client configuration

Parameter name	Type	Description
	SslVpnClientConfig	Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

EnableVpnGatewaySSLClientCert

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to enable an SSL VPN client certificate.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 23:00:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EnableVpnGatewaySSLClientCert
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway ID, which is in the format of vpngw-goa5jz6j. Example: vpngw-1u2xtmbz
VpcId	Yes	No	String	VPC Instance ID Example: vpc-napeigw5
SSLVpnClientId	Yes	No	String	SSL VPN Client Instance ID Example: vpnc-1dac13ac

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	taskid Example: jkt45
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

InquiryPriceCreateVpnGateway

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (InquiryPriceCreateVpnGateway) is used to create VPN Gateway inquiries.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-24 00:48:57.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceCreateVpnGateway
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceChargeType	No	No	String	VPN gateway billing mode. PREPAID: prepaid, i.e., monthly subscription, POSTPAID_BY_HOUR: postpaid, i.e., pay-as-you-go. The default is POSTPAID_BY_HOUR. If a prepaid mode is specified, the parameter InstanceChargePrepaid is required. Example: PREPAID
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, namely setting of parameters related to monthly subscription. Through this parameter, you can specify the duration of purchase for monthly subscription instances, whether to set auto-renewal, and other attributes. This parameter is required when the specified instance is subject to a payment mode of prepaid. Example:View
InternetMaxBandwidthOut	Yes	No	Uint64	Public network bandwidth setting. Optional bandwidths: 5, 10, 20, 50, and 100; unit: Mbps. Example: 5

3. Output Parameters

Parameter name	Type	Description
Price	Price	Commodity price. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

InquiryPriceResetVpnGatewayInternetMaxBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (InquiryPriceResetVpnGatewayInternetMaxBandwidth) is used to adjust the price inquiry of the VPN gateway bandwidth cap.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-24 00:49:26.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceResetVpnGatewayInternetMaxBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-kjllekna
InternetMaxBandwidthOut	Yes	No	Uint64	Public network bandwidth setting. Optional bandwidths: 5, 10, 20, 50, and 100; unit: Mbps. Example: 10

3. Output Parameters

Parameter name	Type	Description
Price	Price	Commodity price. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyCustomerGatewayAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyCustomerGatewayAttribute) is used to modify customer gateway information.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-23 01:16:33.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyCustomerGatewayAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
CustomerGatewayId	Yes	No	String	Customer gateway ID, e.g., cgw-2wqq41m9, which can be queried through the DescribeCustomerGateways API. Example: cgw-mgp33pll
CustomerGatewayName	Yes	No	String	Customer gateway name, which can be named arbitrarily, but must not exceed 60 characters. Example: NewName

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyVpnConnectionAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyVpnConnectionAttribute) is used to modify VPN tunnels.

Default interface request rate limit: 100 times per second.

Interface update time: 2019-01-18 01:22:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpnConnectionAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnConnectionId	Yes	No	String	VPN tunnel instance ID, e.g., vpnx-f49l6u0z. Example: vpnx-i0f4fo4m
VpnConnectionName	No	No	String	VPN tunnel name. The name can be given arbitrarily, but must not exceed 60 characters. Example: new_name
PreShareKey	No	No	String	Preshared key. Example: presharedkey
SecurityPolicyDatabases	No	No	Array of SecurityPolicyDatabase	SPD policy group, for example: {"10.0.0.5/24": ["172.jkt.10.5/16"]}. Here, 10.0.0.5/24 represents the VPC's private IP range, and 172.jkt.10.5/16 represents the IDC's IP range. Users can specify which IP ranges within the VPC are allowed to communicate with specific IP ranges in their IDC. Example:View
IKEOptionsSpecification	No	No	IKEOptionsSpecification	IKE (Internet Key Exchange) configuration, which involves a set of self-protection mechanisms for user-configured network security protocols. Example:View
IPSECOptionsSpecification	No	No	IPSECOptionsSpecification	IPSec session security settings. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
UnsupportedOperation	Operation unsupported.
LimitExceeded	Exceeded the limit

ModifyVpnGatewayAttribute

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyVpnGatewayAttribute) is used to modify VPN gateway attributes.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-05-23 00:53:42.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpnGatewayAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-edvft32x
VpnGatewayName	No	No	String	VPN gateway name, up to 60 bytes in length. Example: demo-vpn
InstanceChargeType	No	No	String	VPN gateway billing mode, currently supports only the conversion from prepaid (i.e., monthly subscription) to postpaid (i.e., pay-as-you-go). The parameter only supports: POSTPAID_BY_HOUR. Example: POSTPAID_BY_HOUR

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

ModifyVpnGatewayCcnRoutes

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ModifyVpnGatewayCcnRoutes) is used to modify VPN gateway CCN routes.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-03-31 20:11:58.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpnGatewayCcnRoutes
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID Example: vpngw-qol17bja
Routes	Yes	No	Array of VpngwCcnRoutes	CCN Route (IDC IP Range) List Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist
InternalServerError	Internal operation error.

ModifyVpnGatewaySSLClient

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API is used to modify an SSL VPN client.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-03 22:36:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVpnGatewaySSLClient
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SSLVpnClientId	Yes	No	String	SSL VPN Client Instance ID Example: vpnc-awq341c
SSLVpnClientName	Yes	No	String	SSL VPN Client Name Example: client-name
VpcId	Yes	No	String	VPC Instance ID Example: vpc-napeigw5

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter	Invalid input parameters.

ResetVpnConnection

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ResetVpnConnection) is used to reset the VPN tunnel.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-03-02 18:15:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetVpnConnection
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-kjllnkew
VpnConnectionId	Yes	No	String	VPN tunnel instance ID, e.g., vpnx-f49l6u0z. Example: vpnx-f29e6u0z

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist

ResetVpnGatewayInternetMaxBandwidth

1. Interface Description

Interface request domain name: vpc.api3.convergecloud.com.

This API (ResetVpnGatewayInternetMaxBandwidth) is used to adjust the bandwidth cap of the VPN gateway. It currently supports upgrading configurations. For subscription-based VPN gateways, this needs to be within the valid period.

Default interface request rate limit: 100 times per second.

Interface update time: 2018-06-01 01:32:35.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetVpnGatewayInternetMaxBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VpnGatewayId	Yes	No	String	VPN gateway instance ID. Example: vpngw-ajclakqw
InternetMaxBandwidthOut	Yes	No	Uint64	Public network bandwidth setting. Optional bandwidths: 5, 10, 20, 50, and 100; unit: Mbps. Example: 5

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.Malformed	Invalid input format.
ResourceNotFound	The resource does not exist

Data structure

Vpc

VPC object.

Referenced by the following interfaces: CreateVpc, DescribeVpcInternal, DescribeVpcs

name	required	NULL allowed	type	description
VpcName	yes	no	String	VPC name. Example: demo
VpcId	yes	no	String	VPC instance ID , e.g., vpc-axd4dt1c. Example: vpc-axd4dt1c
CidrBlock	yes	no	String	IPv4 CIDR of VPC . Example: 10.0.0.0/16
IsDefault	no	no	Bool	Whether it is VPC by default. Example: true
EnableMulticast	yes	no	Bool	Whether to enable multicast. Example: true
CreatedTime	no	no	String	Creation time. Example: 2021-01-03 22:25:45
DnsServerSet	yes	no	Array of String	DNS list. Example: -
DomainName	yes	no	String	DHCP domain option. Example: demo
DhcpOptionsId	yes	no	String	ID of DHCP option set. Example: -
EnableDhcp	yes	no	Bool	Whether DHCP is enabled. Example: false
Ipv6CidrBlock	no	no	String	IPv6 CIDR of VPC . Example: -
TagSet	yes	no	Array of Tag	Tag Key-value Pairs Example:View
AssistantCidrSet	no	yes	Array of AssistantCidr	Auxiliary CIDR Example:View
BmsNum	no	yes	Int64	BMS quantity. Example: 2
ExtendCidrSet	no	yes	Array of ExtendCidr	Extended CIDR list. Example:View
IsShare	no	no	Bool	Whether it is a shared resource. Example: True
EnableCdcPublish	no	no	Bool	Switch for publishing the CDC subnet to CCN. true: publish; false: not publish. Example: False
EnableRouteVpcPublish	no	no	Bool	Route publishing policy when VPC is associated with CCN. true: enable CIDR route publishing; false: enable subnet route publishing. By default, subnet route publishing is enabled when a VPC is created. Example: True
CdcId	no	no	String	Unique ID of CDC. Example: cdc-2kxwx7x
VpcFlag	no	no	Uint64	Whether it is a self-developed VPC: 0: no; 1: yes. Example:
Region	no	no	String	Region. Example: sz

VpcOssDockerRequest

Complex type: VpcOssDockerRequest.

Referenced by the following interfaces: CreateDockerInternal

name	required	NULL allowed	type	description
Subnet	no	no	String	Subnet address Example: 10.0.0.0
IntMask	no	no	Int64	Integer mask. Example: 16
UniqueVpcId	no	no	String	Unique VPC ID. Example: vpc-7zayowkt
VpcId	no	no	Int64	Integer VPCID. Example: 1

AddressBasic

EIP Basic Information

Referenced by the following interfaces: DescribeAddressesHistory

name	required	NULL allowed	type	description
AddressIp	no	no	String	Public Network IP Address Example: 10.23.32.2
AddressId	yes	no	String	ID of EIP , which is the unique identifier of EIP . Example: eip-d97jnd1o
AddressType	yes	no	String	EIP resource types, including "CalcIP", "WanIP", "EIP", and "AnycastEIP". Where, "CalcIP" indicates device IP; "WanIP" indicates general public network IP; "EIP" indicates elastic public IP; and "AnycastEip" indicates accelerated EIP. Example: EIP
InternetServiceProvider	yes	no	String	EIP ISP information, including CMCC, CTCC, CUCC, and BGP, where CMCC indicates Mobile, CTCC indicates Telecom, CUCC indicates Unicom, and BGP indicates BGP interfacing ISP. Example: BGP
Status	yes	no	String	EIP usage status. "used" indicates that the IP address is occupied in the current region; "unused" indicates that the IP address is not occupied in the current region. Example: Used
AnycastZone	yes	no	String	An Anycast publishing domain is a region for accelerating IP address publishing. It is the POP access point for publishing VIP addresses of Anycast CLB instances. The client accesses the nearest POP access point. Currently, Anycast CLB instances support the following publishing domains: Publishing domain A (ANYCAST_ZONE_A): Mainly contains regions in Europe and America. VIP addresses will be published simultaneously in Toronto, Silicon Valley, Frankfurt, Virginia, and Moscow. Publishing domain B (ANYCAST_ZONE_B): Mainly contains regions in Southeast Asia. VIP addresses will be published simultaneously in Singapore, Seoul, Mumbai, Bangkok, and Tokyo. Example: ap-region-1
Address	no	no	String	Public IP address. Example: eip-37axd8t

AddressChargePrepaid

Cost Object for Describing EIP

Referenced by the following interfaces: AllocateAddresses, InquiryPriceAllocateAddresses

name	required	NULL allowed	type	description
Period	yes	no	Int64	Instance Purchase Duration Example: 0
RenewFlag	no	no	String	Auto-renewal Flag Example: AutoRenewFlag

DfwOssUSGQuotaResult

Complex type: DfwOssUSGQuotaResult.

Referenced by the following interfaces: DescribeUSGQuotaInternal

name	required	NULL allowed	type	description
SgId	no	no	String	Name of the original DFW API (v2): getUSGQuota.sgId. Example: 251197522
Quota	no	no	DfwOssUSGQuota	Name of the original DFW API (v2): getUSGQuota.quota. Example:View

GatewayFlowMonitorDetail

Gateway Traffic Monitoring Details

Referenced by the following interfaces: DescribeGatewayFlowMonitorDetail

name	required	NULL allowed	type	description
PrivateIpAddress	yes	no	String	Source IP . Example: 10.0.1.21
InPkg	yes	no	Uint64	Input packet volume. Example: 100
OutPkg	yes	no	Uint64	Packet output quantity. Example: 100
InTraffic	yes	no	Uint64	Inbound bandwidth, in Byte . Example: 100
OutTraffic	yes	no	Uint64	Outbound bandwidth, in Bytes. Example: 100

LocalDestinationIpPortTranslationNatRule

Local Destination IP Port Translation Complex Structure

Referenced by the following interfaces: CreateLocalDestinationIpPortTranslationNatRule, DeleteLocalDestinationIpPortTranslationNatRule, DescribeLocalDestinationIpPortTranslationNatRules

name	required	NULL allowed	type	description
Protocol	yes	no	String	Protocol Example: tcp
OriginalPort	yes	no	Int64	Source Port Example: 80
OriginalIp	yes	no	String	Source IP Example: 10.0.0.5
TranslationPort	yes	no	Int64	Destination port Example: 80
TranslationIp	yes	no	String	Destination IP Example: 2.2.2.2
Description	no	no	String	Description Example: for_demo

PrivateIpAddressSpecification

Private IP Information

Referenced by the following interfaces: AssignPrivateIpAddresses, CreateAndAttachNetworkInterface, CreateNetworkInterface, CreateNetworkInterfaceEx, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra, ModifyPrivateIpAddressesAttribute, UnassignPrivateIpAddresses

name	required	NULL allowed	type	description
PrivateIpAddress	yes	no	String	Private IP address. Example: 192.168.0.10
Primary	no	no	Bool	Whether it is the primary IP. Example: true
PublicIpAddress	no	no	String	Public IP address. Example: jkl.10.100.171
AddressId	no	no	String	EIP instance ID, such as eip-jrkzpvgt. Example: eip-29mdigub

name	required	NULL allowed	type	description
Description	no	no	String	Private IP description information. Example: demo
IsWanIpBlocked	no	no	Bool	Whether the public IP is blocked. Example: true
State	no	no	String	IP Status: PENDING: In production MIGRATING: Migrating DELETING: Deleting AVAILABLE: Available. Example: AVAILABLE

ConflictItem

Conflicting resource entry information.

Referenced by the following interfaces: CheckAssistantCidr

name	required	NULL allowed	type	description
ConflictId	yes	no	String	ID of the Conflicting Resource Example: rtt-kngiybtl
DestinationItem	yes	no	String	Conflicting Destination Resources Example: 10.0.0.0/24

ServiceTemplateGroup

Protocol Port Template Collection

Referenced by the following interfaces: CreateServiceTemplateGroup, DescribeServiceTemplateGroups

name	required	NULL allowed	type	description
ServiceTemplateGroupId	yes	no	String	Instance ID of protocol port template collection, e.g., ppmg-2klmrefu. Example: ppmg-p4oaqaeq
ServiceTemplateGroupName	yes	no	String	Protocol port template collection name. Example: demo
ServiceTemplateIdSet	yes	no	Array of String	Protocol port template instance ID. Example: ["ppm-529rnwsjll", "ppm-4dw6aagho"]
CreatedTime	no	no	String	Creation time. Example: 2018-06-21 11:32:29
ServiceTemplateSet	yes	no	Array of ServiceTemplate	Protocol port template instance information. Example:View

InternetPrice

Public Network Inquiry Output Parameters

Referenced by the following interfaces: InquiryPriceAllocateAddresses

name	required	NULL allowed	type	description
AddressPrice	no	no	InternetPriceDetail	Detailed parameters of Public IP inquiry. Example:View

VpcOssRouteInfoRequest

Complex type: VpcOssRouteInfoRequest.

Referenced by the following interfaces: CreateRouteInternal, DeleteRouteInternal

name	required	NULL allowed	type	description
RouteSet	no	no	Array of VpcOssRouteForDeleteRouteInternal	Original VPC OSS APIv2 name: DelRoute.route. Example:View
VpcId	no	no	Int64	Integer VPCID. Example: 1
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywf6r
GroupId	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.groupId. Example: 0
Type	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.type. Example: 0
Protocol	no	no	String	Original VPC OSS APIv2 name: DelRoute.proto. Example: tcp
VirtualPort	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.vport. Example: 22
Vip	no	no	String	Original VPC OSS APIv2 name: DelRoute.vip. Example: 172.16.0.18

CcnAttachedInstance

CCN Associated Instance Object

Referenced by the following interfaces: DescribeCcnAttachedInstances

name	required	NULL allowed	type	description
CcnId	yes	no	String	CCN instance ID. Example: ccn-31zf3vlb
InstanceType	yes	no	String	Associated instance type: • VPC : Virtual Private Cloud • DIRECTCONNECT : Direct Connect gateway • BMVPC : BM VPC . Example: VPC
InstanceId	yes	no	String	Associated instance ID. Example: vpc-ll6ork07
InstanceName	yes	no	String	Associated instance name. Example: demo
InstanceRegion	yes	no	String	Region of the associated instance. For example, ap-region. Example: ap-region
InstanceUin	yes	no	String	Associated instance UIN (root account). Example: 100000072292
CidrBlock	yes	no	Array of String	Associated instance CIDR. Example: 10.1.0.0/16
State	yes	no	String	Associated instance status: • PENDING : Applying • ACTIVE : Connected • EXPIRED : Expired • REJECTED : Rejected • DELETED : Deleted • FAILED : Failed (will be forcefully detached asynchronously after 2 hours) • ATTACHING : Attaching • DETACHING : Detaching • DETACHFAILED : Detaching failed (will be forcefully detached asynchronously after 2 hours). . Example: ACTIVE
AttachedTime	yes	no	Datetime	Association time. Example: 2021-03-03 16:19:44
CcnUin	yes	no	String	UIN of CCN (root account). Example: 100000072292

Ipv6SectionSet

IPv6 address pool object.

Referenced by the following interfaces: DescribeIpv6Section

name	required	NULL allowed	type	description
SectionId	no	no	Uint64	Unique ID of an IPv6 address pool. Example: 31
CidrBlock	no	no	String	IPv6 address pool IP range. Example: 3402:4e00:20:1200::/56
AddressType	no	no	Uint64	IPv6 address type. Example: 0/1
EnableSplit	no	no	Uint64	Whether to support automatic splitting. Example: 0: not supported; 1: customization supported.

NatGateway

NAT gateway object.

Referenced by the following interfaces: CreateNatGateway, DescribeNatGateways

name	required	NULL allowed	type	description
NatGatewayId	yes	no	String	ID of NAT gateway. Example: "nat-demoaq78"
NatGatewayName	yes	no	String	NAT gateway name. Example: "demo"
CreatedTime	yes	no	String	NAT gateway creation time. Example: "2021-05-24 19:28:31"
State	yes	no	String	NAT gateway status. PENDING: Pending, DELETING: Deleting, AVAILABLE: Available, UPDATING: Upgrading, FAILED: Failed. Example: "AVAILABLE"
InternetMaxBandwidthOut	yes	no	Uint64	Maximum public outbound bandwidth of gateway (unit: Mbps). Example: 10
MaxConcurrentConnection	yes	no	Uint64	Upper limit of gateway concurrent connections. Example: 10000000
PublicIpAddressSet	yes	no	Array of NatGatewayAddress	Array of public IP objects bound to the NAT gateway. Example:View
NetworkState	yes	no	String	NAT gateway network status. "AVAILABLE": Available, "UNAVAILABLE": Unavailable, "INSUFFICIENT": Service suspended for overdue payments. Example: "AVAILABLE"
DestinationIpPortTranslationNatRuleSet	yes	no	Array of DestinationIpPortTranslationNatRule	Port forwarding rules of the NAT gateway. Example:View
VpcId	yes	no	String	VPC instance ID. Example: "vpc-demoaq78"
Zone	yes	no	String	Availability zone of the NAT gateway. Example: "ap-region-2"
GatewayType	no	yes	String	Underlying gateway type. Values are NORMAL and HYPER. Example: NORMAL
TagSet	yes	no	Array of Tag	Tag key-value pairs. Example:View
SourceIpTranslationNatRuleSet	no	no	Array of SourceIpTranslationNatRule	SNAT rules of the NAT gateway. Example:View
StrictSnatMode	no	no	Bool	Whether to only allow forwarding for traffic that matches SNAT rules. Example: false

name	required	NULL allowed	type	description
NatType	yes	no	String	NAT workload type. Example: "NAT"
RestrictState	yes	no	String	Whether the NAT gateway is blocked. Example: "NORMAL"
SecurityGroupSet	yes	no	Array of String	List of security groups bound to the NAT gateway. Example: ["sg-12345678"]
ExclusiveGatewayBandwidth	no	no	Uint64	Bandwidth (unit: Mbps) of the gateway cluster of the dedicated NAT gateway. Example: 50000
DedicatedClusterId	yes	no	String	Unique CDC ID. Example: cluster-gbo27yc4
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-hj1hxf929
NatProductVersion	yes	no	Uint64	NAT gateway type. 1: Classic NAT gateway; 2: Standard NAT gateway. Example: 1
InternetMaxBandwidthIn	no	no	Uint64	Maximum public network inbound bandwidth of the gateway (unit: Mbps). Example: 10
DirectConnectGatewayIds	yes	no	Array of String	ID of the bound direct connect gateway. Example: ["dcg-12345678"]
SmartScheduleMode	yes	no	Bool	Whether to enable the feature of selecting the EIP used for SNAT based on the destination CIDR block. Example: false
IsExclusive	yes	no	Bool	Whether the NAT gateway is a dedicated one. Example: false
SharedCount	yes	no	Uint64	Number of sub-instances associated with the shared NAT gateway. Example: 0

SecurityGroup

Security Group Object

Referenced by the following interfaces: CloneSecurityGroup, CreateDefaultSecurityGroup, CreateSecurityGroup, CreateSecurityGroupWithPolicies, DescribeSecurityGroups

name	required	NULL allowed	type	description
ProjectId	no	no	String	Project ID. Default value: 0. It can be queried on the project management page in the console. Example: 0
SecurityGroupId	yes	no	String	Security group instance ID, e.g., sg-ohuuioma. Example: sg-05bb4upy
SecurityGroupName	yes	no	String	Security Group Name: can be freely named but the name must not exceed 60 characters. Example: demoGroup
SecurityGroupDesc	yes	no	String	Security group remarks, up to 100 characters. Example: demo-group-desc
IsDefault	no	no	Bool	Whether it is the default security group. The default security group cannot be deleted. Example: false
CreatedTime	no	no	String	Security group creation time. Example: 2017-04-18 21:02:30
TagSet	no	no	Array of Tag	Tag key-value pairs. ExampleView
UpdateTime	no	no	String	Security group update time. Example: 2017-04-18 21:02:30
Region	no	no	String	Region. Example: sz

VpcOssGlobalRouteRequest

Complex type: VpcOssGlobalRouteRequest.

Referenced by the following interfaces: CreateGlobalRouteInternal, DeleteGlobalRouteInternal

name	required	NULL allowed	type	description
VpcId	no	no	Int64	Integer VPCID. Example: 1
Subnet	no	no	String	Subnet address Example: 10.0.0.0
IntMask	no	no	Int64	Integer mask. Example: 16
Remote	no	no	String	Name of the original VPC OSS API (v2): DelGlobalRoute.remote. Example: 172.16.0.18
Type	no	no	Int64	Name of the original VPC OSS API (v2): DelGlobalRoute.type. Example: 0
CanEcmpFlag	no	no	Int64	Whether ECMP is supported. Default value: 1, indicating that ECMP is supported. Example: 1

AddressPrice

Adjust bandwidth inquiry result.

Referenced by the following interfaces: InquiryPriceCreateIp6Translators, InquiryPriceModifyAddressesBandwidth

name	required	NULL allowed	type	description
ChargeUnit	no	no	String	Billing Unit Example: HOUR
UnitPrice	no	no	Float	Unit price Example: 21
DiscountPrice	no	no	Float	Discount Price Example: 21

SecurityGroupLimitSet

User security group quota limit.

Referenced by the following interfaces: DescribeSecurityGroupLimits

name	required	NULL allowed	type	description
SecurityGroupLimit	yes	no	Uint64	Number of security groups that can be created per project per region. Example: 100
SecurityGroupPolicyLimit	yes	no	Uint64	Maximum Number of Rules under a Security Group Example: 100
ReferedSecurityGroupLimit	yes	no	Uint64	Number of Nested Security Group Rules under a Security Group Example: 100
SecurityGroupInstanceLimit	yes	no	Uint64	Number of Instances Associated with Single Security Group Example: 100
InstanceSecurityGroupLimit	yes	no	Uint64	Number of Security Groups Associated with an Instance Example: 100
SecurityGroupReferedCvmAndEniLimit	yes	no	Uint64	Security Group Associated ENI Quota Example: 100
SecurityGroupReferedSvcLimit	yes	no	Uint64	Associated Service Quota of Security Group Example: 100
SecurityGroupExtendedPolicyLimit	yes	no	Uint64	Security Group Extension Policy Quota Example: 100

DfwOssUSGPolicyItem

Complex type: DfwOssUSGPolicyItem.

Referenced by the following interfaces: CreateUSGRuleInternal, DescribeUSGPolicyInternal

name	required	NULL allowed	type	description
ServiceModule	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.serviceModule. Example: ppm-ni1vf0zg
AddressModule	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.addressModule. Example: ipmg-liaxelm6
Id	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.id. Example: sg-e5qn5sl9
ModifyTime	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.modifytime. Example: 2022-06-21 10:46:42
Desc	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.desc. Example: test
Action	no	no	String	Name of the original DFW API (v2): getUSGPolicy.action. Example: ACCEPT
Ip	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.ip. Example: 10.0.0.0/8
Protocol	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.protocol. Example: tcp
Port	no	yes	String	Name of the original DFW API (v2): getUSGPolicy.port. Example: 80

VpcEndPointServiceUser

Details on the allowlist object of endpoint services.

Referenced by the following interfaces: DescribeVpcEndPointServiceWhiteList

name	required	NULL allowed	type	description
Owner	yes	no	Uint64	AppId. Example: 1255000100
UserUin	yes	no	String	Uin. Example: jkt
Description	yes	no	String	Description information. Example: demo
CreateTime	yes	no	String	Creation Time Example: 2021-01-14 15:58:40
EndPointServiceId	yes	no	String	Endpoint service ID. Example: vpcssc-b2mmmx7

CcnInstance

CCN associated instance object.

Referenced by the following interfaces: AcceptAttachCcnInstances, AttachCcnInstances, DetachCcnInstances, RejectAttachCcnInstances

name	required	NULL allowed	type	description
InstanceType	no	no	String	Associated instance type, options: ▸ VPC : Virtual Private Cloud ▸ DIRECTCONNECT : Direct Connect gateway ▸ BMVPC : BM VPC. Example: VPC
InstanceId	yes	no	String	Associated instance ID. Example: vpc-86or4il7

name	required	NULL allowed	type	description
InstanceRegion	yes	no	String	Region of the associated instance ID. For example, ap-region. Example: ap-region

VpcNum

Numeric ID of VPC

Referenced by the following interfaces: DescribeVpcIds

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-napeigw5
VpcNumId	yes	no	Uint64	Numeric ID of VPC instance. Example: 67087

DBInstances

Database instance details.

Referenced by the following interfaces: DescribeDBInstancesWithSecurityGroup

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Instance ID format, e.g., crs-1newjcob. Example: crs-1newjcob
InstanceIp	yes	no	String	Instance IP, e.g., 172.16.32.18. Example: 172.16.32.18
InstanceName	yes	no	String	Instance name. Example: cfs-qci
VpcId	yes	no	String	Unique VPC ID, e.g., vpc-q9iejftlr. Example: vpc-67wlqf6v

DfwOssPolicies

Complex type: DfwOssPolicies.

Referenced by the following interfaces: AttachPolicyToVMInternal, DeletePolicyFromVmInternal, DescribeVmPolicyInternal

name	required	NULL allowed	type	description
Action	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.action. Example: ACCEPT
Ip	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.ip. Example: 10.0.0.0/8
Protocol	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.protocol. Example: tcp
Port	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.port. Example: 80
Direction	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.direction. Example: INPUT

Quota

Description of Quota Information

Referenced by the following interfaces: DescribeAddressActionQuota, DescribeAddressQuota, DescribeIp6TranslatorQuota

name	required	NULL allowed	type	description
QuotaId	no	no	String	Quota name. The values are • TOTAL_EIP_QUOTA : EIP quota count under the user's current region. • DAILY_EIP_APPLY : Number of subscriptions today under the user's current region. • DAILY_PUBLIC_IP_ASSIGN : Number of times a public IP is reassigned in the user's current region. Example: TOTAL_EIP_QUOTA
QuotaCurrent	no	no	Int64	Current quantity Example: 10
QuotaLimit	no	no	Int64	Quota Example: 10
QuotaGroup	no	no	String	Regions where the quota takes effect. Example: sz

VpcExtendCidr

VPC Expansion CIDR

Referenced by the following interfaces: DescribeVpcExtendCidrs

name	required	NULL allowed	type	description
VpcId	yes	no	String	VpcId Example: vpc-67wlqf6v
CidrBlock	yes	no	String	CIDR Example: 192.241.0.0/24
CreateTime	yes	no	Date	Creation Time Example: 2018-06-21 11:32:29

Tag

Tag Key-value Pairs

Referenced by the following interfaces: AllocateAddresses, CloneSecurityGroup, CreateAndAttachNetworkInterface, CreateAssistantCidr, CreateDefaultSecurityGroup, CreateDirectConnectGateway, CreateHaVip, CreateIpv6Routes, CreateNatGateway, CreateNetworkAcl, CreateNetworkInterface, CreateRouteTable, CreateRoutes, CreateSecurityGroup, CreateSecurityGroupWithPolicies, CreateSubnet, CreateSubnets, CreateVpc, DescribeAddresses, DescribeAssistantCidr, DescribeDirectConnectGateways, DescribeHaVips, DescribeIp6Addresses, DescribeNatGateways, DescribeNetworkAcls, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra, DescribeRouteTables, DescribeSecurityGroups, DescribeSubnets, DescribeVpcInternal, DescribeVpcPeeringConnections, DescribeVpcs, ModifyAssistantCidr

name	required	NULL allowed	type	description
Key	yes	yes	String	Tag Key Example: tag-key
Value	yes	yes	String	Tag Value Example: tag-value

VpcOssSubnetForDescribeSubnetInternal

Complex type: VpcOssSubnetForDescribeSubnetInternal.

Referenced by the following interfaces: DescribeSubnetInternal

name	required	NULL allowed	type	description
DhcpFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.dhcpFlag. Example: 0
Max	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.max. Example: 167772415
GatewayIp	no	no	String	Name of the original VPC OSS API (v2): GetSubnet.gwIp. Example: 0.0.0.0
BroadcastFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.broadcastFlag. Example: 0
SyncAclToTgwFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.syncAclToTgwFlag. Example: 0
UniqueCidcId	no	no	String	Name of the original VPC OSS API (v2): GetSubnet.uniqCidcId. Example: xx
Name	no	no	String	Name Example: test
LocalZoneFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.bLocalZone. Example: 0
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-1ufvulum
Owner	no	no	String	User app ID Example: 251197522
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-7sayowkt
ZoneId	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.zoneId. Example: 100001
VpcId	no	no	Int64	Integer VPCID. Example: 16769060
SubnetId	no	no	Int64	Integer subnetId. Example: 2007467
Min	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.min. Example: 167772160
IntMask	no	no	Int64	Integer mask. Example: 24
Type	no	no	Int64	Name of the original VPC OSS API (v2): GetRoute.type. Example: 0
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetSubnet.createTime. Example: 2021-05-10 15:40:12
RemoteVpcSnatFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.bRemoteVpcSnat. Example: 0
Mask	no	no	String	Mask Example: 255.255.255.0
DefaultFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.bDefault. Example: 0
CdcFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetSubnet.bCdc. Example: 0
Subnet	no	no	String	Subnet address Example: 10.0.0.0

VpcOssNatServiceForCreateNatGatewayServiceInternal

Complex type: VpcOssNatServiceForCreateNatGatewayServiceInternal.

Referenced by the following interfaces: CreateNatGatewayServiceInternal

name	required	NULL allowed	type	description
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywf6r
Vip	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.vip. Example: 9.241.203.205
PrivateIp	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.pip. Example: 172.16.0.18
VirtualPort	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.vport. Example: 13803
Bandwidth	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.bandwidth. Example: 0
SubnetId	no	no	Int64	Integer subnetId. Example: 1990866
Business	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.business. Example: xx

name	required	NULL allowed	type	description
VirtualGatewayType	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.vgwType Example: 0
Protocol	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.proto. Example: tcp
CreateTime	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.createTime. Example: 2021-12-27 18:09:40
UniqueVpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.uniqVgwIndex. Example: 172.16.0.18
GatewayIp	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.gwip. Example: 9.241.203.205
ProtocolPort	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.pport. Example: 554
PoolId	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.poolId. Example: 33362
VpcId	no	no	Int64	Integer VPCID. Example: 78257
Owner	no	no	String	User app ID Example: 251198225
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-am4aebsm
VpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.vgwIndex. Example: 172.16.0.18
BusinessOwner	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.businessOwner. Example: xx

NetworkAcl

Network ACL

Referenced by the following interfaces: CreateNetworkAcl, DescribeNetworkAcls

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-q26u781x
NetworkAclId	yes	no	String	Network ACL instance ID . Example: acl-fy0yu3bq
NetworkAclName	yes	no	String	Network ACL name, up to 60 bytes in length. Example: demo
CreatedTime	yes	no	String	Creation time. Example: 2021-03-22 20:59:55
SubnetSet	yes	no	Array of Subnet	Network ACL associated subnet array. Example:View
IngressEntries	yes	no	Array of NetworkAclEntry	Network ACL inbound rules. Example:View
EgressEntries	yes	no	Array of NetworkAclEntry	Network ACL outbound rules. Example:View

HaVipSet

HaVip Binding CVM ENI Information

Referenced by the following interfaces: FlushHaVip

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-67wlqf6v
Vip	yes	no	String	Virtual IP address. Example: 10.2.3.12
IfnName	no	no	String	ENI interface name. Example: veth_21CF5180
MacAddress	no	no	String	ENI MAC address. Example: 20:90:6F:69:CA:7F

VpcOssNatService

Complex type: VpcOssNatService.

Referenced by the following interfaces: DeleteNatGatewayServiceInternal

name	required	NULL allowed	type	description
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywf6r
GatewayIp	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.gwip. Example: 9.241.203.205
UniqueVpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.uniqVgwIndex. Example: 172.16.0.18
SubnetId	no	no	Int64	Integer subnetId. Example: 1990866
Owner	no	no	String	User app ID Example: 251198225
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-am4aebsm
PrivateIp	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.pip. Example: 172.16.0.18
Business	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.business. Example: bus
VpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.vgwIndex. Example: 172.16.0.18
BusinessOwner	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.businessOwner. Example: 12345
SkipReturnSnatIpFlag	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.bSkipReturnSnatip. Example: 1
VpcId	no	no	Int64	Integer VPCID. Example: 78257
Protocol	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.proto Example: tcp
ProtocolPort	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.pport. Example: 554
Bandwidth	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.bandwidth. Example: 0
VirtualGatewayType	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.vgwType. Example: 0
Vip	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.vip. Example: 9.241.203.205
VirtualPort	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.vport. Example: 13803
VipBusiness	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.vipBusiness. Example: vipbus
CreateTime	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.createTime. Example: 2021-12-27 18:09:40
PoolId	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.poolId. Example: 33362

DefaultVpcSubnet

Default VPC and Subnet

Referenced by the following interfaces: CreateDefaultVpc

name	required	NULL allowed	type	description
VpcId	yes	no	String	Default VpcId Example: vpc-6vbg797r
SubnetId	yes	no	String	Default Subnet Id Example: subnet-3opmksyg
VpcName	no	no	String	Default VPC name. Example: Default-VPC
CidrBlock	no	no	String	Default subnet CIDR. Example: 172.16.0.0/16
DhcpOptionsId	no	no	String	ID of DHCP option set. Example: dopt-7t8bojl2
DnsServerSet	no	no	String	DNS list. Example: ['183.60.82.98']
DomainName	no	no	String	DHCP domain option. Example: demo

ServiceTemplate

Protocol port template

Referenced by the following interfaces: CreateServiceTemplate, CreateServiceTemplateGroup, DescribeServiceTemplateGroups, DescribeServiceTemplates

name	required	NULL allowed	type	description
ServiceTemplateId	yes	no	String	Protocol port instance ID, e.g., ppm-f5n1f8da. Example: ppm-f5n1f8da
ServiceTemplateName	yes	no	String	Template name. Example: name
ServiceSet	no	no	Array of String	Protocol port information. Example: ["tcp:80"]
CreatedTime	no	no	String	Creation time. Example: 2021-03-02 14:41:15

Subnet

Subnet Object

Referenced by the following interfaces: CreateAssistantCidr, CreateNetworkAcl, CreateSubnet, CreateSubnets, CreateVpc, DescribeAssistantCidr, DescribeNetworkAcls, DescribeSubnets, DescribeVpcInternal, DescribeVpcs, ModifyAssistantCidr

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-m0c2kcun
SubnetId	yes	no	String	Subnet instance ID , e.g., subnet-bthucmmy. Example: subnet-bthucmmy
SubnetName	yes	no	String	Subnet name. Example: demo
CidrBlock	yes	no	String	IPv4 CIDR of Subnet. Example: 10.0.0.0/24

name	required	NULL allowed	type	description
IsDefault	yes	no	Bool	Whether it is the default subnet. Example: true
EnableBroadcast	yes	no	Bool	Whether to enable broadcast. Example: true
Zone	yes	no	String	Availability zone. Example: region
RouteTableId	no	no	String	Route table instance ID, e.g., rtb-l2h8d7c2. Example: rtb-l2h8d7c2
CreatedTime	no	no	String	Creation time. Example: 2018-04-04T10:15:16+08:00
AvailableIpAddressCount	yes	no	Uint64	Number of available IP . Example: 254
Ipv6CidrBlock	no	no	String	Subnet's IPv6 CIDR . Example: 3402:4e00:20:1200::/64
NetworkAclId	no	no	String	Associated ACL ID Example: acl-l2h8d7c2
IsRemoteVpcSnat	no	no	Bool	Whether it is a SNAT address pool subnet. Example: true
TotalIpAddressCount	yes	no	Uint64	Total IP count within the subnet. Example: 254
TagSet	yes	no	Array of Tag	Tag key-value pairs. Example:View
Type	no	no	Uint64	Subnet type. Example: 0/9
VmNum	no	yes	Uint64	Number of VMs. Example: 2
ZoneId	no	yes	Uint64	Availability zone ID. Example: 50001
LocalZone	no	no	Bool	Whether it is a local region. Example: 1
IsCdcSubnet	no	no	Uint64	Whether it is a CDC-controlled subnet. Example: 0
CdcId	no	no	String	CDC ID Example: cluster-gbo27yc4
BmsNum	no	no	Uint64	Bare Metal Quantity Example: 2
IsShare	no	no	Bool	Whether it is a shared resource. Example: True
Region	no	no	String	Region. Example: sz

VpcOssRoute

Complex type: VpcOssRoute.

Referenced by the following interfaces: DescribeServiceByRealServerInternal

name	required	NULL allowed	type	description
HostIp	no	no	String	Original VPC OSS APIs2 name: GetServiceByRs.hostIp. Example: 0.0.0.0
PrivateIp	no	no	String	Original VPC OSS APIs2 name: GetServiceByRs.pip. Example: 10.112.65.50
Weight	no	no	Int64	Original VPC OSS APIs2 name: GetServiceByRs.weight. Example: 16
PrivatePort	no	no	Int64	Original VPC OSS APIs2 name: GetServiceByRs.privatePort. Example: 443
ZoneId	no	no	Int64	Original VPC OSS APIs2 name: GetServiceByRs.zoneId. Example: 50001
UdpOption	no	no	Int64	Original VPC OSS APIs2 name: GetServiceByRs.udpOption. Example: 0

LocalIpTranslationAclRule

Local IP Translation ACL Rule Complex Type

Referenced by the following interfaces: CreateLocalIpTranslationAclRule, DescribeLocalIpTranslationAclRules

name	required	NULL allowed	type	description
Protocol	yes	no	String	Protocol Example: tcp
SourcePort	yes	no	String	Source Port Example: 80
DestinationCidr	yes	no	String	Destination IP Example: 1.1.1.0/16
DestinationPort	yes	no	String	Destination port Example: 80
Action	no	no	Int64	0 or 1 Example: 0
AclRuleId	no	no	Int64	ACL Rule ID Example: 26

VpcOssVpcPeerRequest

Complex type: VpcOssVpcPeerRequest.

Referenced by the following interfaces: UpdateVpcPeerInternal

name	required	NULL allowed	type	description
State	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.state. Example: 0
Bandwidth	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bandwidth. Example: 0
OwedFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.owedFlag. Example: 0
UniqueVpcPeerId	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.uniqVpcPeerId. Example: pcx-fh7xs34s
VpcPeerId	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.vpcPeerId. Example: 2
Owner	no	no	String	User app ID Example: 251198225
Name	no	no	String	Name Example: 11
VirtualSafeGroupIp	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.vsgIp. Example: 1.2.3.5
NewAclFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bNewAlc. Example: 1
PublishDockerCidrFlag	no	no	Uint64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bPublishDockerCidr. Example: 0

ZoneSet

Zone Array

Referenced by the following interfaces: DescribeNatGatewayZones

name	required	NULL allowed	type	description
Zone	yes	yes	String	Zone Name Example: ap-region-2
ZoneId	yes	no	Uint64	Availability Zone ID Example: 50001

RouteTableAssociation

Route Table Association

Referenced by the following interfaces: CreateIpv6Routes, CreateRouteTable, CreateRoutes, DescribeRouteTables

name	required	NULL allowed	type	description
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-8qywqc4y
RouteTableId	yes	no	String	Route table instance ID. Example: rtb-q8o2z892

IpAddressStates

Information on resources that occupy the IP addresses.

Referenced by the following interfaces: DescribeUsedIpAddress

name	required	NULL allowed	type	description
ResourceType	yes	no	String	Resource Type Example: ENI
ResourceId	yes	no	String	Resource ID Example: eni-bjekqlf1
VpcId	yes	no	String	VPC instance ID. Example: vpc-mcqaoy0f
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-j4oluywm
IpAddress	yes	no	String	IP address. Example: 172.16.0.16

AlgType

ALG Protocol Type

Referenced by the following interfaces: DescribeAddresses, DescribeIp6Addresses

name	required	NULL allowed	type	description
Ftp	yes	no	Bool	Whether the FTP protocol ALG feature is enabled. Example: Ture
Sip	yes	no	Bool	Whether the SIP Protocol ALG feature is enabled. Example: Ture

DfwOssDeletePolicyFromVmRequest

Complex type: DfwOssDeletePolicyFromVmRequest.

Referenced by the following interfaces: DeletePolicyFromVmInternal

name	required	NULL allowed	type	description
Uuid	no	no	String	Name of the original DFW API (v2): delPolicyFromVM.uuid. Example: 123123
Policies	no	no	Array of DfwOssPolicies	Name of the original DFW API (v2): delPolicyFromVM.policies. Example:View

IKEOptionsSpecification

IKE (Internet Key Exchange) configuration, which involves a set of self-protection mechanisms for user-configured network security protocols.

Referenced by the following interfaces: CreateVpnConnection, DescribeVpnConnections, ModifyVpnConnectionAttribute

name	required	NULL allowed	type	description
PropoEncryAlgorithm	no	no	String	Encryption algorithms. Options: '3DES-CBC', 'AES-CBC-128', 'AES-CBS-192', 'AES-CBC-256', and 'DES-CBC'. Default: 3DES-CBC. Example: 3DES-CBC
PropoAuthenAlgorithm	no	no	String	Authentication algorithm. Options: MD5, and SHA1. The default is MD5. Example: MD5
ExchangeMode	no	no	String	Negotiation mode. Options: AGGRESSIVE and MAIN. The default is MAIN. Example: MAIN
LocalIdentity	no	no	String	Local identifier type. Options are ADDRESS and FQDN. ADDRESS by default. Example: ADDRESS
RemoteIdentity	no	no	String	Peer identifier type: options include: 'ADDRESS', 'FQDN'. Default: ADDRESS. Example: ADDRESS
LocalAddress	no	no	String	Local identifier. When LocalIdentity is selected as ADDRESS, LocalAddress is required. The default localAddress is the public IP of VPN gateway. Example: 1.2.3.4
RemoteAddress	no	no	String	Peer identifier. When RemoteIdentity is set to ADDRESS, RemoteAddress is required. Example: 4.3.2.1
LocalFqdnName	no	no	String	Local identifier. When LocalIdentity is selected as FQDN, LocalFqdnName is required. Example: LocalName
RemoteFqdnName	no	no	String	Customer identifier. When remoteIdentity is selected as FQDN, RemoteFqdnName is required. Example: RemoteName
DhGroupName	no	no	String	DH group, specifying the DH group used in key exchange (IKE). Options: GROUP1, GROUP2, GROUP5, GROUP14, and GROUP24. Example: GOURP1
IKESaLifetimeSeconds	no	no	Uint64	IKE SA lifetime, in seconds. It sets the lifespan of IKE SA, value range: 60-604,800. Example: 60
IkeVersion	no	no	String	IKE Version Example: 1

VpnConnection

VPN channel object.

Referenced by the following interfaces: CreateVpnConnection, DescribeVpnConnections

name	required	NULL allowed	type	description
VpnConnectionId	yes	no	String	Channel instance ID. Example: vpnx-7m38k0z
VpnConnectionName	yes	no	String	Tunnel name. Example: tunnel_name
VpcId	yes	no	String	VPC instance ID. Example: vpc-cd20bf9ox
VpnGatewayId	yes	no	String	VPN gateway instance ID. Example: vpngw-myjuqp2tj
CustomerGatewayId	yes	no	String	Customer gateway instance ID. Example: cgw-gj1n0n24
PreShareKey	yes	no	String	Pre-shared key. Example: presharekey
VpnProto	yes	no	String	Channel transmission protocol. Example: IPSEC
EncryptProto	yes	no	String	Tunnel encryption protocol. Example: IKE
RouteType	yes	no	String	Route type. Example: StaticRoute
CreatedTime	yes	no	Datetime	Creation time. Example: 0000-00-00 00:00:00
State	yes	no	String	Tunnel status. PENDING: pending, AVAILABLE: available, DELETING: deleting. Example: AVAILABLE
NetStatus	yes	no	String	Channel connection status. AVAILABLE: Connected. Example: AVAILABLE
SecurityPolicyDatabaseSet	yes	no	Array of SecurityPolicyDatabase	SPD. Example:View
IKEOptionsSpecification	yes	no	IKEOptionsSpecification	IKE options. Example:View
IPSECOptionsSpecification	yes	no	IPSECOptionsSpecification	IPSEC selection. Example:View
NegotiationType	no	no	String	Negotiation type, which is default to active (active negotiation). Example: active
DpdEnable	no	no	Int64	DPD detection switch. The default value is 0, which indicates that DPD detection is disabled. Valid values: 0 (disabled); 1 (enabled). Example: 0
DpdTimeout	no	no	String	DPD timeout duration, which is the time required to confirm the absence of the peer. This is effective when dpdEnable is set to 1 (enabled). The default value is 30 seconds. Example: 30
DpdAction	no	no	String	The action to take after DPD timeout. The default is clear. Example: clear

ServiceRoute

Service routing information.

Referenced by the following interfaces: DescribeServiceInternal

name	required	NULL allowed	type	description
Weight	no	no	Uint64	Weight. Example: 12
ProtocolPort	no	no	Uint64	Protocol port number. Example: 21
ZoneId	no	no	Uint64	Availability Zone ID Example: 10002
HostIp	no	no	String	Host IP Example: 193.0.0.1
PrivateIP	no	no	String	Private IP Example: 10.0.0.1
ForwardingMode	no	no	Uint64	Forwarding mode. Example: 0

SourceIpTranslationNatRule

SNAT Rules of NAT

Referenced by the following interfaces: CreateNatGateway, CreateNatGatewaySourceIpTranslationNatRule, DescribeNatGatewaySourceIpTranslationNatRules, DescribeNatGateways, ModifyNatGatewaySourceIpTranslationNatRule

name	required	NULL allowed	type	description
NatGatewaySnatId	no	no	String	SNAT Rule ID Example: snat-3nptcfvp
ResourceId	yes	no	String	Resource ID Example: subnet-7aed90al
ResourceType	yes	yes	String	Resource type, currently including SUBNET and NETWORKINTERFACE. Example: SUBNET
PrivateIpAddress	yes	no	String	Source IP/IP Range Example: 172.168.100.0/24
PublicIpAddresses	yes	no	Array of String	Elastic IP Address Pool Example: ['180.12.59.43']
Description	yes	no	String	Description Example: demo
NatGatewayId	no	yes	String	ID of NAT gateway. Example: nat-3nptcfvp
VpcId	no	yes	String	VPC ID. Example: vpc-oty76xyl
CreatedTime	no	yes	String	Creation time of NAT gateway SNAT rule. Example: 2021-03-14 11:59:00

VpcLimit

VPC Quota

Referenced by the following interfaces: DescribeVpcLimits

name	required	NULL allowed	type	description
LimitType	yes	no	String	VPC Quota Description Example: appid-max-vpcs
LimitValue	yes	no	Uint64	VPC Quota Value Example: 0

DfwOssGetUSGCountFromSGRequest

Complex type: DfwOssGetUSGCountFromSGRequest.

Referenced by the following interfaces: DescribeUSGCountFromSgInternal, DescribeUSGQuotaInternal

name	required	NULL allowed	type	description
SgId	no	no	String	Name of the original DFW API (v2): getUSGQuota.sgId. Example: 132131231
Project	no	no	String	Name of the original DFW API (v2): getUSGQuota.project. Example: 132132231

DfwOssDeleteUSGRuleRequest

Complex type: DfwOssDeleteUSGRuleRequest.

Referenced by the following interfaces: DeleteUSGRuleInternal

name	required	NULL allowed	type	description
Indexes	no	no	Array of Int64	Name of the original DFW API (v2): deleteUSGRule.indexes. Example: [1, 2]
UsgId	no	no	String	Name of the original DFW API (v2): deleteUSGRule.usgId. Example: 123123
Direction	no	no	String	Name of the original DFW API (v2): deleteUSGRule.direction. Example: inbound
Version	no	no	Int64	Name of the original DFW API (v2): deleteUSGRule.version. Example: 12

NewRouteSet

New Route Name

Referenced by the following interfaces: ReplaceRoutes

name	required	NULL allowed	type	description
RouteId	no	no	String	Route ID Example: 16820
DestinationCidrBlock	no	no	String	Target IP Range Example: 169.254.128.0/17
GatewayType	no	no	String	Gateway type Example: NORMAL_CVM
GatewayId	no	no	String	Gateway ID Example: 172.16.16.37
RouteDescription	no	no	String	Route Description Example: demo

EndPoint

Endpoint details.

Referenced by the following interfaces: CreateVpcEndPoint, CreateVpcEndPointService, DescribeVpcEndPoint, DescribeVpcEndPointService

name	required	NULL allowed	type	description
EndPointId	yes	no	String	Terminal node ID. Example: vpce-7cz6ogk8
VpcId	yes	no	String	VPCID. Example: vpc-67wlqf6v
SubnetId	yes	no	String	Subnet ID. Example: subnet-8qywqc4y
EndPointOwner	yes	no	String	APPID. Example: jkt45567
EndPointName	yes	no	String	Endpoint name. Example: demo
ServiceVpcId	yes	no	String	VPCID of terminal node service. Example: vpc-67wlqf6v
ServiceVip	yes	no	String	VIP of endpoint service. Example: 10.23.11.12
EndPointServiceId	yes	no	String	ID of endpoint service. Example: vpcsvc-demoaq78
EndPointVip	yes	no	String	VIP of endpoints. Example: 10.23.11.12
State	yes	no	String	Endpoint statuses. ACTIVE: Available, PENDING: Pending, ACCEPTING: Accepting, REJECTED: Rejected, FAILED: Failed. Example: 0/1/2/3/4
CreateTime	yes	no	String	Creation time. Example: 2018-06-21 11:32:29
GroupSet	no	no	Array of String	Security group instance ID list bound to the endpoint. Example: ["sg-demoaq78"]
ServiceName	no	no	String	Endpoint service name. Example: demo
IpAddressType	no	no	String	Address Type Example: IPv4/IPv6

AddressTemplateItem

Address Information

Referenced by the following interfaces: CreateAddressTemplateGroup, DescribeAddressTemplateGroups

name	required	NULL allowed	type	description
AddressTemplateName	no	no	String	Address Template Name Example: demo
AddressTemplateId	yes	no	String	Address template ID Example: ipm-ig8epno8

EipStatistics

Structure Describing EIP Statistical Information

Referenced by the following interfaces: DescribeEipStatistics

name	required	NULL allowed	type	description
Region	yes	no	String	English Identifier of Region Example: sz
RegionName	yes	no	String	Region Example: sz
TotalCount	yes	no	Int64	Total Number of Region EIP Example: 10

Ip6Translator

IPv6 Translation Instance Information

Referenced by the following interfaces: DescribeIp6Translators

name	required	NULL allowed	type	description
Ip6TranslatorId	yes	no	String	The unique ID of the IPv6 translation instance, such as ip6-37xao8t. Example: ip6-mhmrv51i
Ip6TranslatorName	yes	no	String	Name of IPv6 Translation Instance Example: demo
Vip6	yes	no	String	IPv6 Address Example: 2402:4e00:4040::2:2a6
IspName	yes	no	String	ISP of the IPv6 Translation Address Example: BGP
TranslatorStatus	yes	no	String	Translation instance status, limited to CREATING, RUNNING, DELETING, and MODIFYING. Example: RUNNING
CreatedTime	yes	no	Datetime_iso	IPv6 Translation Instance Creation Time Example: 2020-01-30 00:00:00
Ip6RuleCount	yes	no	Int64	Number of IPV6 Conversion Rules Bound Example: 2
Ip6RuleSet	yes	no	Array of Ip6Rule	IPv6 Conversion Rule Information Example:View
CreatedTimeLocal	no	no	Datetime	Local Time for Creation of IPv6 Translation Instances Example: 2023-07-13T11:12:06

NetworkInterface

ENI

Referenced by the following interfaces: CreateAndAttachNetworkInterface, CreateNetworkInterface, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra

name	required	NULL allowed	type	description
NetworkInterfaceId	yes	no	String	ENI instance ID, e.g., eni-f1xjkw1b. Example: eni-b44as8qbz
NetworkInterfaceName	yes	no	String	ENI name. Example: demo
NetworkInterfaceDescription	no	no	String	ENI description. Example: demo
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-l0ykcjvl
VpcId	yes	no	String	VPC instance ID. Example: vpc-29mdcjub
GroupSet	no	no	Array of String	Security group bound. Example: sg-2edhcclz
Primary	no	no	Bool	Whether it is the primary network interface. Example: true
MacAddress	yes	no	String	MAC address. Example: 20:90:6F:EE:57:E2
State	yes	no	String	ENI status: • PENDING : Creating • AVAILABLE : Available • ATTACHING : Attaching • DETACHING : Detaching • DELETING : Deleting. Example: AVAILABLE
PrivateIpAddressSet	yes	no	Array of PrivateIpAddressSpecification	Private IP information. Example:View
Attachment	no	yes	NetworkInterfaceAttachment	Bound CVM object. Example:View
Zone	no	no	String	Availability zone. Example: region
CreatedTime	no	no	String	Creation time. Example: 2020-10-28 08:23:59
Ipv6AddressSet	yes	no	Array of Ipv6Address	IPv6 address list. Example:View
TagSet	yes	no	Array of Tag	Tag key-value pairs. Example:View
EniType	no	no	Uint64	Network interface types: 0 - ENI; 1 - EVM ENI. Example: 0
FlowLogsSet	no	yes	Array of FlowLog	Stream log list. Example:View
QosLevel	no	no	String	QoS Level Example: AG
AttachType	no	no	Uint64	Binding Level Example: 0
Business	no	no	String	Business Party Example: TKE
CdcId	no	no	String	Unique ID of CDC Example: cluster-g5o27yc4
SubNetworkInterfaces	no	no	Array of String	List of relay ENI instances associated with this ENI. Example: ["eni-pq0vhykj"]
Region	no	no	String	Region. Example: sz
DeleteOnTermination	no	no	Bool	Whether to terminate the ENI when an instance is deleted. Example: true
FlushSubEniHavipFlag	no	no	Bool	Whether to migrate zi wang kahavip. Example: true

name	required	NULL allowed	type	description
ResourceId	no	no	String	The resource ID for retaining the primary IP address of the ENI. It is used as an input parameter when the ENI is deleted. Example: cls-j85c20d4-reserved
InstanceId	no	no	String	Cloud host instance ID. Example: ins-20113wkl
taskId	no	no	Int64	Des task taskId Example: 213415

SslVpnClientConfig

ssl-vpn-client-client-config Configuration

Referenced by the following interfaces: DownloadVpnGatewaySSLClientCert

name	required	NULL allowed	type	description
SSLVpnClientConfiguration	yes	yes	String	Configure on client Example: client,dev tun,proto udp,remote...
SSLVpnRootCert	yes	yes	String	Root certificate Example: BEGIN CERTIFICATE...
SSLVpnKey	yes	yes	String	Client Key Example: BEGIN PRIVATE KEY...
SSLVpnCert	yes	yes	String	Client certificate Example: BEGIN CERTIFICATE...

HaVipAssociation

CVM instance or ENI bound to HAVIP (used to limit the scope of HAVIP switching, which does not trigger a real switch operation).

Referenced by the following interfaces: CreateHaVip, DescribeHaVips

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Unique ID of the instance or ENI bound to HAVIP. Example: ins-3qx9e8b
HaVipId	no	no	String	Unique instance ID of HAVIP. Example: havip-7tqt5jn6
InstanceType	no	no	String	Type of the object bound to HAVIP. Valid values: CVM and ENI. Example: CVM

IdcSet

NAT64 IDC information.

Referenced by the following interfaces: DescribeIp6SbIdcInfo

name	required	NULL allowed	type	description
RegionId	no	no	Int64	RegionId Example: 50090001
RegionName	no	no	String	RegionName Example: cq
ZoneId	no	no	Int64	ZoneId Example: 50090001
ZoneName	no	no	String	ZoneName Example: cq
IdcId	no	no	Int64	IdcId Example: 50080005
IdcName	no	no	String	IdcName Example: iaasidc

IPSECOptionsSpecification

IPSec session security settings.

Referenced by the following interfaces: CreateVpnConnection, DescribeVpnConnections, ModifyVpnConnectionAttribute

name	required	NULL allowed	type	description
EncryptAlgorithm	no	no	String	Encryption algorithms. Options: '3DES-CBC', 'AES-CBC-128', 'AES-CBC-192', 'AES-CBC-256', 'DES-CBC', and 'NULL'. Default: AES-CBC-128. Example: AES-CBC-128
IntegrityAlgorith	no	no	String	Authentication algorithm. Options: MD5, SHA1. The default is Example: SHA1
IPSECSaLifetimeSeconds	no	no	Uint64	IPsec SA lifetime (s): In seconds, range: 180-604,800 Example: 180
PfsDhGroup	no	no	String	PFS options: 'NULL', 'DH-GROUP1', 'DH-GROUP2', 'DH-GROUP5', 'DH-GROUP14', and 'DH-GROUP24'. The default is NULL. Example: NULL
IPSECSaLifetimeTraffic	no	no	Uint64	IPsec SA lifetime (KB): In KB, range: 2,560-604,800. Example: 2560

ModifyBandwidthPrice

Adjust bandwidth inquiry result.

Referenced by the following interfaces: InquiryPriceModifyAddressesBandwidth

name	required	NULL allowed	type	description
AddressPrice	no	no	AddressPrice	Adjust bandwidth inquiry result. Example:View

NatGatewayQuota

NAT Gateway Quota

Referenced by the following interfaces: DescribeNatGatewayQuota

name	required	NULL allowed	type	description
BandwidthQuota	yes	no	Uint64	NAT Gateway Bandwidth Quota Example: 5000

CustomerGateway

Customer gateway

Referenced by the following interfaces: CreateCustomerGateway, DescribeCustomerGateways

name	required	NULL allowed	type	description
CustomerGatewayId	yes	no	String	Unique ID of User Gateway Example: cgw-ea2fck23
CustomerGatewayName	yes	no	String	Gateway name Example: demo-name
IpAddress	yes	no	String	Public network address Example: 1.1.1.5.5
CreatedTime	yes	no	String	Creation Time Example: 2021-02-03 00:00:00
VpnConnNum	no	no	Uint64	The number of associated channels. Example: 1
BgpAsn	no	no	Int64	BGP ASN. Example: 6000

CustomerGatewayVendor

Customer gateway vendor information object.

Referenced by the following interfaces: DescribeCustomerGatewayVendors, DownloadCustomerGatewayConfiguration

name	required	NULL allowed	type	description
Platform	yes	no	String	Platform. Example: comware
SoftwareVersion	yes	no	String	Software version. Example: V1.0
VendorName	yes	no	String	Vendor name. Example: h3c

NetworkInterfaceExtendIp

ENI Expanded IP Range

Referenced by the following interfaces: DescribeNetworkInterfaceExtendIps

name	required	NULL allowed	type	description
VpcId	yes	no	Uint64	VPC Integer ID Example: 6757
UniqVpcId	yes	no	String	Unique ID of VPC Example: vpc-67wlqf6v
EniId	yes	no	Uint64	Integer ID of ENI Example: 324
UniqEniId	yes	no	String	Unique ID of ENI Example: eni-ltbabo1ev
Ip	yes	no	String	Extended IP Example: 10.2.3.12

DfwOssGetUSGFromVMRequest

Complex type: DfwOssGetUSGFromVMRequest.

Referenced by the following interfaces: DescribeVmPolicyInternal

name	required	NULL allowed	type	description
Uuid	no	no	String	Name of the original DFW API (v2): getVMPolicy.uuid. Example: 84f9a2ad-6659-4864-808c-bd17f3c2acea

DfwOssUSGOperateResult

Complex type: DfwOssUSGOperateResult.

Referenced by the following interfaces: CreateUSGRuleInternal, DeleteUSGInternal, DeleteUSGRuleInternal

name	required	NULL allowed	type	description
UsgId	no	no	String	Name of the original DFW API (v2): insertUSGRule.usgId. Example: sg-dn7qcw21
ErrorCode	no	no	Int64	Name of the original DFW API (v2): insertUSGRule.errorCode. Example: 0
ErrorInfo	no	no	String	Name of the original DFW API (v2): insertUSGRule.errorInfo. Example: success

EndPointService

Endpoint service object.

Referenced by the following interfaces: CreateVpcEndPointService, DescribeVpcEndPointService

name	required	NULL allowed	type	description
EndPointServiceId	yes	no	String	Endpoint Service ID Example: vpcsvc-diemoag78
VpcId	yes	no	String	VPCID. Example: vpc-gjux0b5t
ServiceOwner	yes	no	String	APPID. Example: 251007979
ServiceName	yes	no	String	Endpoint service name. Example: demo
ServiceVip	yes	no	String	VIP of backend service. Example: 10.1.1.1
ServiceInstanceId	yes	no	String	Backend service ID, e.g., lb-xxx. Example: lb-was1z62s
AutoAcceptFlag	yes	no	Bool	Whether it is auto-accepted. Example: True
EndPointCount	yes	yes	Uint64	Number of associated endpoints. Example: 0
EndPointSet	yes	yes	Array of EndPoint	Endpoint object array. Example:View
CreateTime	yes	no	String	Creation time. Example: 2018-06-21 11:32:29
IpAddressType	no	no	String	Address Type Example: IPv4/IPv6

Ipv6Address

IPv6 address information.

Referenced by the following interfaces: AssignIpv6Addresses, CreateAndAttachNetworkInterface, CreateNetworkInterface, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra, InquiryPriceAllocateIpv6AddressesBandwidth, ModifyIpv6AddressesAttribute, UnassignIpv6Addresses

name	required	NULL allowed	type	description
Address	yes	no	String	IPv6 address, e.g., 3402:4e00:20:100:0:8cd9:2a67:71f3 . Example: 2409:8c60:2501:1002:aebe:e74c:7a3c:3
Primary	no	no	Bool	Whether it is the primary IP . Example: Ture
AddressId	no	no	String	EIP instance ID , e.g., eip-hxbjja90 . Example: eip-d97pxd1o
Description	no	no	String	Description information. Example: demo
IsWanIpBlocked	no	no	Bool	Whether the public IP is blocked. Example: Ture
State	no	no	String	IPv6 address status: • PENDING : Pending • MIGRATING : Migrating • DELETING : Deleting • AVAILABLE : Available. Example: AVAILABLE

PeerConnection

Peering connection instance information.

Referenced by the following interfaces: DescribeVpcPeeringConnections

name	required	NULL allowed	type	description
VpcId	yes	no	String	Unique ID of the local VPC. Example: vpc-67whpf6v
VpcName	yes	no	String	Local VPC name. Example: demo
VpcCidrBlock	yes	no	String	IPv4 CIDR of local VPC. Example: 10.0.0.0/8
PeerVpcId	yes	no	String	Unique ID of the customer VPC. Example: vpc-demo5678
PeerVpcName	yes	no	String	Customer VPC name. Example: demo
PeerVpcCidrBlock	yes	no	String	IPv4 CIDR of the customer VPC. Example: 172.0.0.0/8
PeeringConnectionId	yes	no	String	Unique ID of peering connection. Example: pcx-demojk64
PeeringConnectionName	yes	no	String	Peering connection name. Example: Example
State	yes	no	String	Peering connection status. PENDING: Pending, ACTIVE: Active, REJECTED: Rejected, DELETED: Deleted, and FAILED: Failed. Example: PEDNING
Type	yes	no	Int64	0: Basic network interconnection; 1: Inter-VPC interconnection; 2: Interconnection between VPC and BM. Example: VPC_PEER
IsNgw	yes	no	Int64	0: NewAsc; 1: Not. Example: true
Bandwidth	yes	no	Int64	Bandwidth value of peering connection. Example: 10
SrcRegion	yes	no	String	Local region. Example: 500001
DstRegion	yes	no	String	Customer region. Example: 500002
CreateTime	yes	no	String	Creation time. Example: 2019-01-15 11:07:15
AppId	yes	no	Int64	Local APPID. Example: jkl456789
PeerAppId	yes	no	Int64	Customer APPID. Example: jkl456789
Uin	yes	no	Uint64	UIN. Example: 100000072292
TagSet	no	yes	Array of Tag	Tag Information Example:View
PeerUin	no	no	Uint64	Customer UIN Example: 100000072292
ChargeType	no	no	String	Recent Change Type Example: POSTPAID_BY_DAY_MAX

Route

Routing Policy Object

Referenced by the following interfaces: CreateIpv6Routes, CreateRouteTable, CreateRoutes, DeleteIpv6Routes, DeleteRoutes, DescribeRouteConflicts, DescribeRouteTables, DescribeRoutes, DescribeRoutesWithLocal, ModifyIpv6Routes, ReplaceRoutes, ResetRoutes

name	required	NULL allowed	type	description
RouteId	no	no	Uint64	Routing policy ID. Example: 1289089
DestinationCidrBlock	no	no	String	Destination IP range. The value must not be within the VPC IP range, e.g.: 112.20.51.0/24. Example: 10.0.0.0/24
GatewayType	no	no	String	Type of next hop. The types supported currently are CVM: Public network gateway type CVM; VPN: VPN gateway; DIRECTCONNECT: Direct Connect gateway; PEERCONNECTION: Peering connection; SSLVPN: sslvpn gateway; NAT: NAT gateway; NORMAL_CVM: Ordinary CVM; EIP: Public IP of CVM; CCN: CCN. Example: VPN
GatewayId	no	no	String	Next hop address: only the gateway ID of different next hop types needs to be specified, and the system will automatically match the next hop address. Special note: When GatewayType is EIP, GatewayId has a fixed value '0'. Example: vpn-acxurf9p
RouteDescription	no	no	String	Routing policy description. Example: demo
Enabled	no	no	Bool	Enable/Disable Example: true
RouteType	no	no	String	Route type currently supported: USER: User route; NETD: Network probe route, automatically issued by the system when creating a network probe instance, and cannot be edited or deleted; CCN: CCN route, automatically issued by the system, and cannot be edited or deleted. Users can only add and manage USER type routes. Example: USER
RouteTableId	no	no	String	Route table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
RouteItemId	no	no	String	Routing policy string ID. Example: rtl-9bpel08h
DestinationIpv6CidrBlock	no	no	String	Create a destination IPv4 CIDR, and the value cannot be within the VPC CIDR. For example: 112.20.51.0/24. Example: 10.0.0.0/24
CreatedTime	no	no	Datetime	Routing policy creation time. Example: 2021-03-02 14:41:15
IsCdc	no	no	String	Whether it is a CDC route. Example: true
PublishedToVbc	no	no	Bool	Whether the routing policy is published to CCN. This field is only used as an output parameter and is invalid when used as an input parameter. Example: true
SubnetRouteAlgorithm	no	no	String	Supported ECMP algorithms: ECMP_QUINTUPLE_HASH: five tuple hash; ECMP_SOURCE_DESTINATION_IP_HASH: source and target IP address hash; ECMP_DESTINATION_IP_HASH: target IP address hash; ECMP_SOURCE_IP_HASH: source IP address hash. Example: ECMP_SOURCE_DESTINATION_IP_HASH
CdcId	no	no	String	cluster-d8htgb6k Example: Unique ID of the CDC cluster

DfwOssDelObjectsFromUSGRequest

Complex type: DfwOssDelObjectsFromUSGRequest.

Referenced by the following interfaces: DeleteObjectFromUSGInternal

name	required	NULL allowed	type	description
VIPS	no	no	Array of String	Name of the original VPC OSS API (v2): delObjectsFromUSG.vips. Example: ['xxx']
Services	no	no	Array of String	Name of the original VPC OSS API (v2): delObjectsFromUSG.svcs. Example: ['xxx']
UsgId	no	no	String	Name of the original VPC OSS API (v2): delObjectsFromUSG.usgId. Example: sg-aosmqpxs
Vms	no	no	Array of String	Name of the original VPC OSS API (v2): delObjectsFromUSG.vms. Example: ['84f9a2ad-6659-4864-808c-bd17f3c2acea']

TrafficMirrorTarget

Traffic Mirror Collection Target Type

Referenced by the following interfaces: CreateTrafficMirror, DescribeTrafficMirrors, ResetTrafficMirrorTarget

name	required	NULL allowed	type	description
TargetIps	yes	no	Array of String	Receiving IP of Traffic Mirror Example: ["10.0.0.0"]
AlgHash	yes	no	String	Traffic mirror receiver IP group. Load balancing rule. ENI/FIVE_TUPLE_FLOW supported. Example: FIVE_TUPLE_FLOW

NetDetectIpState

Validation result for network probe destination IP.

Referenced by the following interfaces: CheckNetDetectState, DescribeNetDetectStates

name	required	NULL allowed	type	description
DetectDestinationIp	yes	no	String	Probe destination IPv4 address. Example: ["1.1.1.3", "1.1.1.8"]
State	yes	no	Int64	Probe results. 0: Succeeded; -1: Route packet loss query failed; -2: Outgoing ACL packet loss; -3: Inbound ACL packet loss; -4: Other errors. Example: 0
Delay	yes	no	Uint64	Latency, in milliseconds. Example: 0
PacketLossRate	yes	no	Uint64	Packet Loss Rate Example: 0

VpcOssRouteWeightRequest

Complex type: VpcOssRouteWeightRequest.

Referenced by the following interfaces: UpdateRouteWeightInternal

name	required	NULL allowed	type	description
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmwywf6r
GroupId	no	no	Int64	Original VPC OSS APIv2 name: UpdateRouteWeight.groupId. Example: 1
Protocol	no	no	String	Original VPC OSS APIv2 name: UpdateRouteWeight.proto. Example: tcp
Vip	no	no	String	Original VPC OSS APIv2 name: UpdateRouteWeight.vip. Example: 172.16.0.18
VirtualPort	no	no	Int64	Original VPC OSS APIv2 name: UpdateRouteWeight.vport. Example: 22
RouteSet	no	no	Array of VpcOssRouteForUpdateRouteWeightInternal	Original VPC OSS APIv2 name: UpdateRouteWeight.route. Example:View
VpcId	no	no	Int64	Integer VPCID. Example: 1

QuotaSet

Quota Information

Referenced by the following interfaces: DescribeAddressAssociationQuota

name	required	NULL allowed	type	description
QuotaId	no	yes	String	Quota ID. Example: NETWORK_INTERFACE_ADDRESS_ASSOCIATION
NetworkInterfaceId	no	yes	String	network interface card ID Example: eni-2dr67vx9
QuotaCurrent	no	yes	Int64	Used quota Example: 2
QuotaLimit	no	yes	Int64	Total quota Example: 10
DefaultInternetServiceProvider	no	yes	Bool	Default Example: true

VpcOssNewService

Complex type: VpcOssNewService.

Referenced by the following interfaces: CreateServiceInternal

name	required	NULL allowed	type	description
UniqueVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: AddService.uniqVpcgwId. Example: vpcgw-7hk7255d
VpcGatewayZoneId	no	no	Int64	Original VPC OSS APIv2 name: AddService.vpcgwZoneId. Example: 1002
Sip	no	no	String	Original VPC OSS APIv2 name: AddService.sip. Example: 1.1.1.1
SubnetRouteAlgorithm	no	no	Int64	Original VPC OSS APIv2 name: AddService.subnetRouteAlgorithm. Example: 0
FakeToaIp	no	yes	String	Original VPC OSS APIv2 name: AddService.fakeToaIp. Example: 192.168.0.1
Vip	no	no	String	Original VPC OSS APIv2 name: AddService.vip. Example: 172.16.0.18
StickyTimeout	no	no	Int64	Original VPC OSS APIv2 name: AddService.stickyTimeout. Example: 0
RouteGroupId	no	no	Int64	Original VPC OSS APIv2 name: AddService.routeGroupId. Example: 1
Type	no	no	Int64	Original VPC OSS APIv2 name: AddService.type. Example: 0
Protocol	no	no	String	Original VPC OSS APIv2 name: AddService.proto. Example: tcp
RemoteVpcId	no	no	Int64	Original VPC OSS APIv2 name: AddService.remoteVpcId. Example: 1
VpcGatewayType	no	no	Int64	Original VPC OSS APIv2 name: AddService.vpcGwType. Example: 1
StickyFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.stickyFlag. Example: 0
LbType	no	no	Int64	Original VPC OSS APIv2 name: AddService.lbType. Example: 0
ResetFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.rstFlag. Example: 0
NoSnatFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.noSnatFlag. Example: 0
BypassFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.bypassFlag. Example: 0
Business	no	no	String	Original VPC OSS APIv2 name: AddService.business. Example: dockerMaster
GroupId	no	yes	Int64	Original VPC OSS APIv2 name: AddService.groupId. Example: 1
VpcId	no	no	Int64	Integer VPCID. Example: 1
VirtualPort	no	no	Int64	Original VPC OSS APIv2 name: AddService.vport. Example: 22
UniqueClassicVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: AddService.uniqClassicVpcgwId. Example: vpcgw-7hk70tq
VpcGatewayAttrFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.bVpcgwAttrFlag. Example: 0
StickyMaxCount	no	no	Int64	Original VPC OSS APIv2 name: AddService.stickyMaxCount. Example: 0
RouteSet	no	no	Array of VpcOssRouteForDeleteRouteInternal	Original VPC OSS APIv2 name: AddService.route. Example:View
DelPipRouteFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.bDelPipRoute. Example: 0
VipVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: AddService.uniqVpcGwIpVpcgwId. Example: vpcgw-7hk7255d
VpcGatewayIp	no	no	String	Original VPC OSS APIv2 name: AddService.vpcGwIp. Example: 1.1.1.1
UniqueRouteGroupId	no	no	String	Original VPC OSS APIv2 name: AddService.uniqRouteGroupId. Example: vpcgw-7hk7255d
CdcFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.bCdc. Example: 0
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmwywf6r
RouteGroupFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.routeGroupFlag. Example: 0
UniqueCdcId	no	no	String	Original VPC OSS APIv2 name: AddService.uniqCdcId. Example: cluster-pwqp4055

RouteConflict

Route Conflict Object

Referenced by the following interfaces: DescribeRouteConflicts

name	required	NULL allowed	type	description
RouteTableId	yes	no	String	Route table instance ID, e.g., rtb-aad4dt1c. Example: rtb-q8o2d892
DestinationCidrBlock	yes	no	String	Conflicting Destination Port to be Checked Example: 192.241.0.0/24
ConflictSet	yes	no	Array of Route	Conflicting Routing Policy List Example:View

VpcOssRoutingTable

Complex type: VpcOssRoutingTable.

Referenced by the following interfaces: DescribeRoutingTableListDetailInternal

name	required	NULL allowed	type	description
VpcDefaultFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.vpcBDefault. Example: 1

name	required	NULL allowed	type	description
Subnet	no	no	Array of VpcOssSubnet	Subnet address Example:View
Name	no	no	String	Name Example: default
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jrnwyxf6r
RoutingTableId	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.rtbId. Example: 213266
RouterId	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.routerId. Example: 196826
SubnetNum	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.subnetNum. Example: 1
UniqueRouterId	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.uniqRouterId. Example: router-omtmjmr6
Owner	no	no	String	User app ID Example: 251198225
UniqueRoutingTableId	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.uniqRtbId. Example: rtb-c6mxqmvy
Type	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.type. Example: 1
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.createTime. Example: 2021-03-22 20:59:55
VpcId	no	no	Int64	Integer VPCID. Example: 78257
VpcIntMask	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.vpcIntMask. Example: 16
VpcMask	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.vpcMask. Example: 255.255.0.0
VpcSubnet	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.vpcSubnet. Example: 172.16.0.0
VpcName	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.vpcName. Example: Default-VPC

TemplateLimit

Parameter Template Quota

Referenced by the following interfaces: DescribeTemplateLimits

name	required	NULL allowed	type	description
AddressTemplateMemberLimit	yes	no	Uint64	Parameter template IP address member quota. Example: 2
AddressTemplateGroupMemberLimit	yes	no	Uint64	Quota for IP address group member of parameter template. Example: 2
ServiceTemplateMemberLimit	yes	no	Uint64	Parameter template l protocol port member quota. Example: 2
ServiceTemplateGroupMemberLimit	yes	no	Uint64	Member quota of parameter template protocol port group. Example: 2

ZoneInfo

EIP Availability Zone List Information

Referenced by the following interfaces: DescribeAvailableZone

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability zone name. For example, ap-region-1. Example: ap-region-2
ZoneName	yes	no	String	Availability zone description. For example, Zone 1. Example: ap-region-2
ZoneId	yes	no	Int64	Availability Zone ID Example: 50001
ZoneState	yes	no	String	Availability zone status, currently including only two statuses: UNAVAILABLE and AVAILABLE. Example: UNAVAILABLE

AccountAttribute

Account Attribute Object

Referenced by the following interfaces: DescribeAccountAttributes

name	required	NULL allowed	type	description
AttributeName	yes	no	String	Attribute Name Example: supported-platforms
AttributeValues	yes	no	Array of String	Attribute Value Example: ["VPC"]

DfwOssGetUSGCountFromSGResult

Complex type: DfwOssGetUSGCountFromSGResult.

Referenced by the following interfaces: DescribeUSGCountFromSgInternal

name	required	NULL allowed	type	description
SgId	no	no	String	Name of the original DFW API (v2): getUSGCountFromSG.sgId. Example: 251197522
USGCount	no	no	Int64	Name of the original DFW API (v2): getUSGCountFromSG.uSGCount. Example: 17

CcnRegionBandwidthLimit

CCN Regional Outbound Bandwidth Limit

Referenced by the following interfaces: DescribeCcnRegionBandwidthLimits, GetCcnRegionBandwidthLimits, SetCcnRegionBandwidthLimits

name	required	NULL allowed	type	description
Region	yes	no	String	Region. For example, ap-region. Example: region
BandwidthLimit	yes	no	Uint64	Outbound bandwidth cap, in Mbps. Example: 10
IsBm	no	no	Bool	Whether it is a Blackstone region. Default: false. Example: true
DstRegion	no	yes	String	Destination region. For example, ap-region. Example: ap-region
DstIsBm	no	no	Bool	Whether the destination region is a BM region, false by default. Example: true

ResourceDashboard

VPC Resource Dashboard (Number of Each Resource)

Referenced by the following interfaces: DescribeVpcResourceDashboard

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID, e.g., vpc-f1ajkw1b. Example: vpc-by4tzqqj
SubnetId	yes	no	String	Subnet instance ID, e.g., subnet-bthucmmy. Example: subnet-bthucmmy
ClassicLink	yes	no	Uint64	Basic network intercommunication. Example: 0
Dcg	yes	no	Uint64	Direct Connect gateway. Example: 1
Pcx	yes	no	Uint64	Peering connection. Example: 0
Ip	yes	no	Uint64	Total number of IPs used. Example: 0
Nat	yes	no	Uint64	NAT gateway. Example: 1
Vpngw	yes	no	Uint64	VPN gateway. Example: 0
FlowLog	yes	no	Uint64	Flow logs. Example: 0
NetworkDetect	yes	no	Uint64	Network probe. Example: 0
NetworkACL	yes	no	Uint64	Network ACL. Example: 0
CVM	yes	no	Uint64	Cloud host. Example: 2
LB	yes	no	Uint64	Cloud Load Balancer. Example: 0
CDB	yes	no	Uint64	Relational database. Example: 0
Cmem	yes	no	Uint64	Memcached. Example: 0
CTSDB	yes	no	Uint64	Time series database. Example: 0
MariaDB	yes	no	Uint64	MariaDB. Example: 0
SQLServer	yes	no	Uint64	SQL Server. Example: 0
Postgres	yes	no	Uint64	TDSQL for PostgreSQL. Example: 0
NAS	yes	no	Uint64	Network attached storage. Example: 0
Greenplumn	yes	no	Uint64	Snova cloud database. Example: 0
Ckafka	yes	no	Uint64	Message queue CKAFKA. Example: 0
Grocery	yes	no	Uint64	Grocery. Example: 0
HSM	yes	no	Uint64	Data encryption service. Example: 0
Tcaplus	yes	no	Uint64	Game storage Tcaplus. Example: 0
Cnas	yes	no	Uint64	Cnas. Example: 0

name	required	NULL allowed	type	description
TiDB	yes	no	Uint64	HTAP database TiDB. Example: 0
Emr	yes	no	Uint64	EMR cluster. Example: 0
SEAL	yes	no	Uint64	SEAL. Example: 0
CFS	yes	no	Uint64	Cloud File Storage (CFS). Example: 0
Oracle	yes	no	Uint64	Oracle. Example: 0
ElasticSearch	yes	no	Uint64	ElasticSearch service. Example: 0
TBaaS	yes	no	Uint64	Blockchain service. Example: 0
Itop	yes	no	Uint64	Itop. Example: 0
DBAudit	yes	no	Uint64	Cloud database auditing. Example: 0
CynosDBPostgres	yes	no	Uint64	Enterprise-level cloud database CynosDB for Postgres. Example: 0
Redis	yes	no	Uint64	Cloud Redis. Example: 0
MongoDB	yes	no	Uint64	Cloud MongoDB. Example: 0
DCDB	yes	no	Uint64	TDSQL for MySQL. Example: 0
CynosDBMySQL	yes	no	Uint64	Enterprise-level cloud database CynosDB for MySQL. Example: 0
Subnet	yes	no	Uint64	Subnet. Example: 1
RouteTable	yes	no	Uint64	Route table. Example: 1
JNS	no	no	Uint64	JNS Service Example: 2
ENI	no	no	Uint64	ENI Example: 2
CDM	no	no	Uint64	CDM Example: 2
CCN	no	no	Uint64	CCN Example: 2
HAVIP	no	no	Uint64	Highly Available Virtual IP Example: 2

ConflictSource

Conflicting resource information.

Referenced by the following interfaces: CheckAssistantCidr

name	required	NULL allowed	type	description
ConflictSourceId	yes	no	String	Conflicting Resource ID Example: rtb-4t7fr3fi
SourceItem	yes	no	String	Conflicting Resources Example: 10.0.0.0/16
ConflictItemSet	yes	no	Array of ConflictItem	Conflicting Resource Entry Information Example:View

LocalSourceIpPortTranslationAclRuleNeedId

Local Source IP Port Translation ACL Mapping Rules

Referenced by the following interfaces: ModifyLocalSourceIpPortTranslationAclRule

name	required	NULL allowed	type	description
Protocol	yes	no	String	Protocol Example: tcp
SourceCidr	yes	no	String	Source Address Example: 1.1.1.0/16
SourcePort	yes	no	String	Source Port Example: 80
DestinationCidr	yes	no	String	Destination address Example: 2.2.2.0/16
DestinationPort	yes	no	String	Destination port Example: 80
Action	no	no	Int64	Action. 0: Allow, 1: Reject. Example: 0
AclRuleId	yes	no	Int64	ACL Rule ID Example: 100

Ip6RuleInfo

IPv6 Translation Rules

Referenced by the following interfaces: AddIp6Rules

name	required	NULL allowed	type	description
Vport6	yes	no	Int64	IPv6 port number, ranging from 0 to 65,535. Example: 80
Protocol	yes	no	String	Protocol type, supporting TCP/UDP. Example: TCP
Vip	yes	no	String	IPv4 Address Example: 172.0.0.0
Vport	yes	no	Int64	IPv4 port number, ranging from 0 to 65,535. Example: 80

VpcOssServiceRequest

Complex type: VpcOssServiceRequest.

Referenced by the following interfaces: DeleteServiceInternal

name	required	NULL allowed	type	description
VirtualPort	no	no	Int64	Original VPC OSS APIv2 name: DelService.vport. Example: 22
Sip	no	no	String	Original VPC OSS APIv2 name: DelService.sip. Example: 1.1.1.1
GroupId	no	no	Int64	Original VPC OSS APIv2 name: DelService.groupId. Example: 1
VpcId	no	no	Int64	Integer VPCID. Example: 1
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywfor
Type	no	no	Int64	Original VPC OSS APIv2 name: DelService.type. Example: 0
Protocol	no	no	String	Original VPC OSS APIv2 name: DelService.proto. Example: tcp
Vip	no	no	String	Original VPC OSS APIv2 name: DelService.vip. Example: 172.16.0.18
RemoteVpcId	no	no	Int64	Original VPC OSS APIv2 name: DelService.remoteVpcId. Example: 1
DeleteRouteFlag	no	no	Int64	Original VPC OSS APIv2 name: DelService.bDelRoute. Example: 0

SecurityGroupPolicySet

Security Group Rule Collection

Referenced by the following interfaces: CreateSecurityGroupPolicies, CreateSecurityGroupWithPolicies, DeleteSecurityGroupPolicies, DescribeSecurityGroupPolicies, ModifySecurityGroupPolicies, ReplaceSecurityGroupPolicy

name	required	NULL allowed	type	description
Version	no	no	String	Current version of the security group rules. Every time a user updates the security rules, the version will automatically increase by 1 to prevent the updated route rules from being outdated. If not specified, conflicts will not be considered. Example: 0
Egress	no	no	Array of SecurityGroupPolicy	Outbound rules. Example:View
Ingress	no	no	Array of SecurityGroupPolicy	Inbound rules. Example:View

SecurityGroupPolicyCheckInfo

Security Group Policy Detection Result Object

Referenced by the following interfaces: CheckSecurityGroupPolicies

name	required	NULL allowed	type	description
Direction	yes	no	String	Data flow direction. Values are inbound and outbound. Example: EGRESS
Protocol	yes	no	String	Protocol, value: TCP, UDP, and ICMP. Example: TCP
Port	yes	no	String	Port number. It is the destination port for inbound, and the source port for outbound. Example: 122
Action	yes	no	String	Whether the data flow is accepted. Valid values: ACCEPT (accepted), DROP (rejected). Example: DROP

VpcOssVpc

Complex type: VpcOssVpc.

Referenced by the following interfaces: DescribeVpcAndSubnetInternal

name	required	NULL allowed	type	description
Subnet	no	no	String	u9a50u7f51u6730u5740 Example: 172.16.0.0
SubnetSet	no	no	Array of VpcOssSubnetForDescribeVpcAndSubnetInternal	u539fVPC OSS APIv2u540du79f0: GetVpcAndSubnet.subnets Example:View
VpcId	no	no	Int64	u6574u6570vpcId Example: 78257
IntMask	no	no	Int64	u6574u6570u63a9u7801 Example: 16

name	required	NULL allowed	type	description
OwnedFlag	no	no	Int64	u662fu5426u81eaeu7814 Example: 0
DhcpFlag	no	no	Int64	u539fVPC OSS APIe2u540du79f0: GetVpcAndSubnet.dhcpFlag Example: 1
CreateTime	no	no	String	u539fVPC OSS APIe2u540du79f0: GetVpcAndSubnet.createTime Example: 2021-03-22 20:59:55
Name	no	no	String	u540du79f0 Example: Default-VPC
UniqueVpcId	no	no	String	u5bf9u5916u552fu4e00Vpcid Example: vpc-jmaywf6r
DefaultFlag	no	no	Int64	u539fVPC OSS APIe2u540du79f0: GetVpcAndSubnet.bDefault Example: 1
BraceLinkFlag	no	no	Int64	u539fVPC OSS APIe2u540du79f0: GetVpcAndSubnet.braceLinkFlag Example: 0
OwnerLevel	no	no	Int64	u539fVPC OSS APIe2u540du79f0: GetVpcAndSubnet.ownerLevel Example: -1
Owner	no	no	String	u7528u6237Appid Example: 251198225

SecurityGroupPolicy

Security Group Rule Object

Referenced by the following interfaces: CreateSecurityGroupPolicies, CreateSecurityGroupWithPolicies, DeleteSecurityGroupPolicies, DescribeSecurityGroupPolicies, DescribeSecurityGroupPolicyTemplates, ModifySecurityGroupPolicies, ReplaceSecurityGroupPolicy

name	required	NULL allowed	type	description
PolicyIndex	no	no	Int64	Index number of security group rule. Example: 0
Protocol	no	no	String	Protocol, value: TCP, UDP, and ICMP. Example: TCP
Port	no	no	String	Port (all, discrete, and range). Example: 22
ServiceTemplate	no	no	ServiceTemplateSpecification	Protocol port ID or protocol port group ID. ServiceTemplate and Protocol+Port are mutually exclusive. Example:View
CidrBlock	no	no	String	IP Range or IP (mutually exclusive). Example: 0.0.0.0/16
Ipv6CidrBlock	no	no	String	IP Range or IPv6 (mutually exclusive). Example: ::/0
SecurityGroupId	no	no	String	Security group instance ID, e.g., sg-ohuuioma. Example: sg-ohuuioma
AddressTemplate	no	no	AddressTemplateSpecification	IP address ID or IP Address Group ID. Example:View
Action	no	no	String	ACCEPT or DROP. Example: ACCEPT
PolicyDescription	no	no	String	Security group rule description. Example: Desc
ModifyTime	no	no	String	Last modified time of security group. Example: 2021-03-02 14:41:15

CcnBandwidthInfo

Information Describing CCN Inter-Region Speed Limited Bandwidth Instance

Referenced by the following interfaces: GetCcnRegionBandwidthLimits

name	required	NULL allowed	type	description
CcnId	yes	yes	String	CCN ID of the bandwidth. Example: ccn-ef5nuflh
CreatedTime	yes	yes	String	Instance creation time. Example: 2018-12-18 20:11:37
ExpiredTime	yes	yes	String	Instance Expiration Time Example: 2019-01-18 20:11:37
RegionFlowControlId	yes	yes	String	Unique ID of bandwidth instance. Example: fcr-6fda09za
RenewFlag	yes	yes	String	Flag of whether the bandwidth is auto-renewed. Example: NOTIFY_AND_AUTO_RENEW
CcnRegionBandwidthLimit	yes	yes	CcnRegionBandwidthLimit	Describe the bandwidth region and the speed limit information. Example:View

TrafficMirror

Traffic Mirror Instance

Referenced by the following interfaces: CreateTrafficMirror, DescribeTrafficMirrors

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC Instance ID Example: vpc-7zayowkt
TrafficMirrorId	yes	no	String	Traffic Mirror Instance Example: img1-oc2mpbni
TrafficMirrorName	yes	no	String	TrafficImageName Example: demo_vxlan
TrafficMirrorDescribe	yes	no	String	Traffic Mirror Description Example: desc
State	yes	no	String	Traffic Mirror Status Example: RUNNING
Direction	yes	no	String	Traffic Mirror Collection Direction Example: ALL
CollectorSrcs	yes	no	Array of String	Traffic Mirror Collection Object Example: ["vpc-7zayowkt"]
NatId	yes	no	String	NAT Gateway Instance ID of Traffic Mirror Filter Example: ""
CollectorNormalFilters	yes	no	Array of TrafficMirrorFilter	Quintuple Rules for Traffic Mirror Filter Example:View
CollectorTarget	yes	no	TrafficMirrorTarget	Traffic mirror receiving target Example:View
CreateTime	yes	no	String	Traffic Mirror Creation Time Example: 2021-03-02 14:41:15

VpcOssDocker

Complex type: VpcOssDocker.

Referenced by the following interfaces: DescribeDockerInternal, DescribeDockerSubnetInternal

name	required	NULL allowed	type	description
Mask	no	no	String	Mask Example: 255.255.0.0
IntMask	no	no	Int64	Integer mask. Example: 16
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetDockerSubnet.createTime. Example: 2021-12-28 16:42:40
Subnet	no	no	String	Subnet address Example: 10.0.0.0
VpcId	no	no	Int64	Integer VPCID. Example: 78257
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywf6r

OldRouteSet

Legacy Route Collection

Referenced by the following interfaces: ReplaceRoutes

name	required	NULL allowed	type	description
RouteId	no	no	String	Route ID Example: 16820
DestinationCidrBlock	no	no	String	Target IP Range Example: 169.254.128.0/17
GatewayType	no	no	String	Gateway type Example: NORMAL_CVM
GatewayId	no	no	String	Gateway ID Example: 172.16.16.37
RouteDescription	no	no	String	Route Description Example: demo

SubnetNum

Numeric ID of Subnet

Referenced by the following interfaces: DescribeSubnetIds

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-demoag78
VpcNumId	yes	no	Uint64	Numeric ID of VPC instance. Example: 10
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-demoag78
SubnetNumId	yes	no	Uint64	Numeric ID of the subnet instance. Example: 4643
SubnetName	no	no	String	Subnet name, up to 60 bytes in length. Example: 4643

ExtendCidr

Extended CIDR.

Referenced by the following interfaces: CreateVpc, DescribeVpcInternal, DescribeVpcs

name	required	NULL allowed	type	description
ExtendCidrBlock	yes	no	String	Extended CIDR. Example: 192.241.0.0/24

Filter

Filter

Referenced by the following interfaces: BandwidthLimitForCcnAlarmOnly, DescribeAddressTemplateGroups, DescribeAddressTemplates, DescribeAddresses, DescribeAssistantCidr, DescribeCcnAttachedInstances, DescribeCcnLimits, DescribeCcnRoutes, DescribeCustomerGateways, DescribeDBInstancesWithSecurityGroup, DescribeDirectConnectGateways, DescribeEipStatistics, DescribeHaVips, DescribeIp6Addresses, DescribeIp6Translators, DescribeLocalDestinationIpPortTranslationNatRules, DescribeLocalGateway, DescribeLocalIpTranslationAclRules, DescribeLocalIpTranslationNatRules, DescribeLocalSourceIpPortTranslationAclRules, DescribeLocalSourceIpPortTranslationNatRules, DescribeNatGatewayDestinationIpPortTranslationNatRules, DescribeNatGateways, DescribeNetDetectStates, DescribeNetDetects, DescribeNetworkAcls, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra, DescribePeerIpTranslationNatRules, DescribeRouteTables, DescribeRoutes, DescribeRoutesWithLocal, DescribeSecurityGroupPolicies, DescribeSecurityGroups, DescribeServicesInternal, DescribeServiceTemplateGroups, DescribeServiceTemplates, DescribeSubnets, DescribeTrafficMirrors, DescribeUsedIpAddress, DescribeVpcEndPoint, DescribeVpcEndPointService, DescribeVpcEndPointServiceWhiteList, DescribeVpcInstances, DescribeVpcInternal, DescribeVpcPeeringConnections, DescribeVpcs, DescribeVpnConnections, DescribeVpnGatewaySSLClients, DescribeVpnGatewaySSLServers, GetCcnRegionBandwidthLimits

name	required	NULL allowed	type	description
Name	yes	no	String	Attribute name. When there are multiple Filters, the relationship between Filters is logical AND. Example: tag-key
Values	yes	no	Array of String	Attribute value. If a filter has multiple values, the relationship among the values under the same filter is logical OR (OR). When the value type is boolean, it can be directly set to the string "TRUE" or "FALSE". Example: ["TagKey1", "TagKey2"]

InternetPriceDetail

Public IP Inquiry Output Parameters

Referenced by the following interfaces: InquiryPriceAllocateAddresses

name	required	NULL allowed	type	description
UnitPrice	no	no	Float	Unit price, unit:USD. Example: 1
DiscountPrice	no	no	Float	Discounted unit price, unit: USD. Example: 1
ChargeUnit	no	no	String	Billing unit. The value range is as follows. HOUR: Indicates that the billing unit is calculated hourly. The scenarios currently involving this billing unit include TRAFFIC_POSTPAID_BY_HOUR and BANDWIDTH_POSTPAID_BY_HOUR. MONTH: Indicates that the billing unit is calculated monthly. The scenarios currently involving this billing unit include: BANDWIDTH_POSTPAID_BY_MONTH, BANDWIDTH_PREPAID_BY_MONTH, and BANDWIDTH_PACKAGE. Example: HOUR

VpcGateway

Gateway Information under VPC

Referenced by the following interfaces: DescribeVpcGateways

name	required	NULL allowed	type	description
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-8qywqc4y
Pip	yes	no	String	Private IP address. Example: 10.12.2.12
WanIp	yes	no	String	Public IP address. Example: 10.12.2.12

VpngwCcnRoutes

VPN Gateway CCN Route Information

Referenced by the following interfaces: DescribeVpnGatewayCcnRoutes, ModifyVpnGatewayCcnRoutes

name	required	NULL allowed	type	description
RouteId	yes	no	String	Route Information ID Example: vpnr-gjl1n0n6
Status	no	no	String	Whether route information is enabled. ENABLE: Enable this route DISABLE: Disable this route. Example: ENABLE

SubnetInput

Subnet Object

Referenced by the following interfaces: CreateSubnets

name	required	NULL allowed	type	description
CidrBlock	yes	no	String	Subnet CIDR . Example: 192.241.0.0/24
SubnetName	yes	no	String	Subnet name. Example: demo
Zone	yes	no	String	Availability zone. For example, ap-region-2 . Example: 50001
RouteTableId	no	no	String	Designated associated route table, e.g., rtb-3ryrwzuu . Example: rtb-q8oz2d92
Type	no	no	Uint64	Specify the subnet type to be created. Example: 0

ClassicLinkInstance

VPC and Basic Network Interconnection Device

Referenced by the following interfaces: DescribeClassicLinkInstances

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC Instance ID Example: vpc-67wlqf6v
InstanceId	yes	no	String	Unique ID of CVM instance Example: ins-kngiybal

FlowLog

Flow log

Referenced by the following interfaces: CreateAndAttachNetworkInterface, CreateNetworkInterface, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra

name	required	NULL allowed	type	description
VpcId	no	no	String	VPC ID or unified ID. It is recommended to use Unified ID. Example: vpc-demoag78
FlowLogId	no	no	String	Unique ID of Flow Log Example: fl-demoag78
FlowLogName	no	no	String	Flow Log Instance Name Example: demo-flowlog
ResourceType	no	no	String	The resource type of stream log, VPC
ResourceId	no	no	String	Unique Resource ID Example: eni-demoag78
TrafficType	no	no	String	Flow log collection type: ACCEPT
CloudLogId	no	no	String	Flow Log Storage ID Example:
CloudLogState	no	no	String	Flow Log Storage ID Status Example: SUCCESS
FlowLogDescription	no	no	String	Flow Log Description Information Example: demo
CreatedTime	no	no	String	Flow log creation time Example: 2020-01-30 00:00:00

GatewayQos

Gateway Traffic Control Bandwidth Information

Referenced by the following interfaces: DescribeGatewayFlowQos

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-67wlqf6v
IpAddress	yes	no	String	Private IP of CVM. Example: 192.168.3.23
Bandwidth	yes	no	Uint64	Traffic control bandwidth value. Example: 50
CreateTime	yes	no	String	Creation time. Example: 2023-12-25 12:30:00

AvailabilitySet

Remaining resource details.

Referenced by the following interfaces: DescribeAddressAvailability

name	required	NULL allowed	type	description
AddressCount	no	yes	Int64	Quantity Example: 1
AddressType	no	yes	String	IP Type Example: EIP
ApplicableForCLB	no	yes	Bool	clb Example: False
ResourceType	no	yes	String	Resource Type Example: EIP
Availability	no	yes	String	Availability Example: Available
InternetServiceProvider	no	yes	String	Line Type Example: BGP
Zone	no	yes	String	Availability Zone Example: cqyfm7
NetworkGroup	no	yes	String	Network grouping. Example: cq

FilterObject

Filter Key-Value Pair

Referenced by the following interfaces: DescribeClassicLinkInstances, DescribeVpnGateways, DescribeVpnSellingModelTagList

name	required	NULL allowed	type	description
Name	yes	no	String	Attribute name. When there are multiple Filters, the relationship between Filters is logical AND. Example: vpc-id
Values	yes	no	Array of String	Attribute value. If multiple values exist for the same Filter, the relationship between values under the same Filter is logical OR. Example: ["vpc-pnpc6ll"]

SingleIspZone

Mapping Relationships between Availability Zone and the Three ISPs

Referenced by the following interfaces: DescribeSingleIspRegion

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability Zone Example: region
ZoneId	yes	no	Uint64	Availability Zone ID Example: 50001
SingleIsp	yes	no	Array of String	3 ISPs, including CMCC, CTCC, and CUCC. Example: CTCC

CcnRoute

CCN Routing Policy Object

Referenced by the following interfaces: DescribeCcnRoutes

name	required	NULL allowed	type	description
RouteId	no	no	String	Routing Policy ID. Example: ccnr-hs2yc3ha
DestinationCidrBlock	yes	no	String	Destination Example: 10.1.19.0/24
InstanceType	yes	no	String	Type of next hop (associated instance type). All types include VPC and DIRECTCONNECT. Example: VPC
InstanceId	yes	no	String	Next hop (associated instance) Example: vpc-fc21z82c
InstanceName	yes	no	String	Next Hop Name (Associated Instance Name) Example: demo
InstanceRegion	yes	no	String	Region of next hop (associated instance region) Example: region
UpdateTime	yes	no	Datetime	Update time Example: 2022-11-19 15:20:25
Enabled	yes	no	Bool	Whether route is enabled. Example: True
InstanceUin	yes	no	String	Associated Instance UIN (Root Account) Example: 100000072292

NetworkAclEntry

Network ACL rule.

Referenced by the following interfaces: CreateNetworkAcl, DescribeNetworkAcls, ModifyNetworkAclEntries

name	required	NULL allowed	type	description
Protocol	no	no	String	Protocol, value: TCP, UDP, ICMP, and ALL. Example: TCP
Port	no	no	String	Port (all, single, and range). When the protocol is ALL or ICMP, the port cannot be specified. Example: 2132
CidrBlock	no	no	String	IP Range or IP (mutually exclusive). Example: 192.168.0.0/24
Ipv6CidrBlock	no	no	String	IP Range or IPv6 (mutually exclusive). Example: 2001:89b:3c51:f5ff::f0db
Action	no	no	String	ACCEPT or DROP. Example: Accept
Description	no	no	String	Rule description, up to 100 in length. Example: demo
NetworkAclIpv4EntryId	no	no	String	Unique ID for the IPv4 network ACL entry. When an ACL entry is modified, either NetworkAclIpv4EntryId or NetworkAclIpv6EntryID should be provided. Example:
Priority	no	no	Int64	Priority, starting from 1. Example: 1
ModifyTime	no	no	String	Modify the time. Example: 2019-11-11 22:16:17

LocalSourceIpPortTranslationNatRule

Direct Connect Gateway Local Source IP Port NAT Mapping Address Pool

Referenced by the following interfaces: CreateLocalSourceIpPortTranslationNatRule, DeleteLocalSourceIpPortTranslationNatRule, DescribeLocalSourceIpPortTranslationNatRules, ModifyLocalSourceIpPortTranslationNatRule

name	required	NULL allowed	type	description
IpPool	yes	no	String	IP Address Pool Example: 2.2.2.2/16
Description	yes	no	String	Description Example: for_demo

SecurityPolicyDatabase

SecurityPolicyDatabase Policy

Referenced by the following interfaces: CreateVpnConnection, DescribeVpnConnections, ModifyVpnConnectionAttribute

name	required	NULL allowed	type	description
LocalCidrBlock	yes	no	String	Local IP address range Example: 11.0.0.0/8
RemoteCidrBlock	yes	no	Array of String	Peer IP range Example: 11.0.0.0/8

DelRoute

Delete Routing Policy Object

Referenced by the following interfaces: DeleteRoutes

name	required	NULL allowed	type	description
RouteId	no	no	Uint64	Route Object Example: 167
RouteDescription	no	no	String	Routing policy description. Example: demo
Enabled	no	no	Bool	Enable/Disable Example: true
RouteType	no	no	String	Route type. Types supported currently are as follows. USER: User route; NETD: Network probe route, which is automatically issued by the system when creating a network probe instance, and cannot be edited or deleted; CCN: CCN route, which is automatically issued by the system, and cannot be edited or deleted. Users can only add and operate USER type routes. Example: NETD
RouteTableId	no	no	String	Route table instance ID, e.g., rtb-azd4dt1c. Example: rtb-azd4dt1c
RouteItemId	no	no	String	Routing policy string ID. Example: rule-azd4dt1c

LocalIpTranslationAclRuleNeedId

Local IP Translation ACL Rule Complex Type

Referenced by the following interfaces: ModifyLocalIpTranslationAclRule

name	required	NULL allowed	type	description
Protocol	yes	no	String	Protocol Example: tcp
SourcePort	yes	no	String	Source Port Example: 80
DestinationCidr	yes	no	String	Destination IP Example: 2.2.2.0/16
DestinationPort	yes	no	String	Destination port Example: 80
Action	no	no	Int64	0 or 1 Example: 0
AclRuleId	yes	no	Int64	Rule ID Example: 100

TrafficMirrorFilter

Quintuple Filter Rule Object for Traffic Mirror

Referenced by the following interfaces: CreateTrafficMirror, DescribeTrafficMirrors, ResetTrafficMirrorFilter, UpdateTrafficMirrorAllFilter

name	required	NULL allowed	type	description
SrcNet	yes	no	String	Source IP Range of the Filtering Rule Example: 10.0.0.0/24
DstNet	yes	no	String	Destination IP Range of the Filtering Rule Example: 192.168.0.0/24
SrcPort	no	no	String	Source port of the filtering rules. The default value is 1-65,535. Example: 5000
DstPort	no	no	String	Destination port of filter rules. Default: 1-65535. Example: 3456
Protocol	yes	no	String	Protocol of the Filtering Rules Example: ALL

AnycastRegionInfo

Information on Regions that Support AnycastEIP

Referenced by the following interfaces: DescribeAnycastRegion

name	required	NULL allowed	type	description
Region	yes	no	String	Region Example: ap-region
RegionName	yes	no	String	Region Example: ap-region
RegionState	yes	no	String	Current Status of Region Example: Used
AnycastZone	yes	no	String	AnycastEIP Release Domain Example: ap-region-1

DfwOssAddPolicyToVMRequest

Complex type: DfwOssAddPolicyToVMRequest.

Referenced by the following interfaces: AttachPolicyToVMInternal

name	required	NULL allowed	type	description
IsTop	no	no	Bool	Name of the original DFW API (v2): addPolicyToVM.isTop. Example: True
Policies	no	no	Array of DfwOssPolicies	Name of the original DFW API (v2): addPolicyToVM.policies. ExampleView
Uuid	no	no	String	Name of the original DFW API (v2): addPolicyToVM.uuid. Example: 84f9a2ad-6659-4864-808c-bd17f3c2acea

Ip6Rule

IPv6 Translation Rules

Referenced by the following interfaces: DescribeIp6Translators

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
Ipv6RuleId	yes	no	String	Unique ID of the IPv6 translation rule, such as rule6-7v3vwgec. Example: rule6-7v3vwgec
Ipv6RuleName	yes	no	String	Name of IPV6 Conversion Rules Example: demo
Vip6	yes	no	String	IPv6 Address Example: 3402:4e00:20:1200::/64
Vport6	yes	no	Int64	IPv6 Port Number Example: 443
Protocol	yes	no	String	Protocol type, supporting TCP/UDP. Example: TCP
Vip	yes	no	String	IPv4 Address Example: 10.0.0.14
Vport	yes	no	Int64	IPv4 Port Number Example: 443
RuleStatus	yes	no	String	Conversion rule status, limited to CREATING, RUNNING, DELETING, and MODIFYING. Example: RUNNING
CreatedTime	yes	no	Datetime_iso	Translation Rule Creation Time Example: 2019-01-10T16:29:37

DfwOssUSGPolicy

Complex type: DfwOssUSGPolicy.

Referenced by the following interfaces: DescribeUSGPolicyInternal

name	required	NULL allowed	type	description
Version	no	no	Int64	Name of the original DFW API (v2): getUSGPolicy.version. Example: 17
UsgId	no	no	String	Name of the original DFW API (v2): getUSGPolicy.usgId. Example: sg-5q4brrmt
ErrorCode	no	no	Int64	Name of the original DFW API (v2): getUSGPolicy.errorCode. Example: 0
Inbound	no	no	Array of DfwOssUSGPolicyItem	Name of the original DFW API (v2): getUSGPolicy.inbound. Example:View
Outbound	no	no	Array of DfwOssUSGPolicyItem	Name of the original DFW API (v2): getUSGPolicy outbound. Example:View

AddressTemplateSpecification

IP Address Template

Referenced by the following interfaces: CreateSecurityGroupPolicies, CreateSecurityGroupWithPolicies, DeleteSecurityGroupPolicies, DescribeSecurityGroupPolicies, DescribeSecurityGroupPolicyTemplates, ModifySecurityGroupPolicies, ReplaceSecurityGroupPolicy

name	required	NULL allowed	type	description
AddressId	yes	no	String	IP address ID, e.g., ipm-2uw6ujo6. Example: ipm-2uw6ujo6
AddressGroupId	yes	no	String	IP address group ID, e.g., ipmg-2uw6ujo6. Example: ipmg-2uw6ujo6

DfwOssUSGQuota

Complex type: DfwOssUSGQuota.

Referenced by the following interfaces: DescribeUSGQuotaInternal

name	required	NULL allowed	type	description
UsgCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.usgCount. Example: 1
InstanceUsgCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.instanceUsgCount. Example: 1
ReferedUsgCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById. referedUsgCount. Example: 1
CvmVifCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.cvmVifCount. Example: 1
ExtendedPolicyCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.extendedPolicyCount. Example: 1
PolicyCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.policyCount. Example: 1
SvcCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.svcCount. Example: 1
UsgInstanceCount	yes	no	Uint64	Name of the original VPC OSS API (v2): getUSGById.usgInstanceCount. Example: 1

VpcOssOverlap

Complex type: VpcOssOverlap.

Referenced by the following interfaces: CheckRoutingTableRouteSubnetOverlapInternal

name	required	NULL allowed	type	description
VpcId	no	no	Int64	Integer VPCID. Example: 6
UniqueVpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): CheckRtbRouteSubnetOverlap.uniqVgwIndex. Example: pcs-sjlzxwhm
Mask	no	no	String	Mask Example: 255.255.0.0
RoutingTableId	no	no	Int64	Name of the original VPC OSS API (v2): CheckRtbRouteSubnetOverlap.rtbId. Example: 29
UniqueRoutingTableId	no	no	String	Name of the original VPC OSS API (v2): CheckRtbRouteSubnetOverlap.uniqRtbId. Example: rtb-o9u877nw
Name	no	no	String	Name Example: testss2
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-pe0kssdp
VirtualGatewayType	no	no	Int64	Name of the original VPC OSS API (v2): CheckRtbRouteSubnetOverlap.vgwType. Example: 4
IntMask	no	no	Int64	Integer mask. Example: 16
VpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): CheckRtbRouteSubnetOverlap.vgwIndex. Example: 19
Owner	no	no	String	User app ID Example: toyacao
Subnet	no	no	String	Subnet address Example: 10.2.0.0

DfwOssGetUSGPolicyRequest

Complex type: DfwOssGetUSGPolicyRequest.

Referenced by the following interfaces: DescribeUSGPolicyInternal

name	required	NULL allowed	type	description
UsgId	no	no	String	Name of the original DFW API (v2): getUSGPolicy.usgId. Example: sg-aaxsaa

EIPIspInfo

EIP ISP Information

Referenced by the following interfaces: DescribeEIPIspInfo

name	required	NULL allowed	type	description
Type	yes	no	String	ISP Type CTCC CUCC CMCC BGP Example: CTCC
Name	yes	no	String	ISP Name Example: ISP Name
Id	no	no	Int64	ISP ID. Example: 5
IspStatus	no	no	Int64	IPv4 ISP status. Example: 1
IspStatusIPv6	no	no	Int64	IPv6 ISP status. Example: 1
DefaultIsp	no	no	Int64	Whether it is an IPv4 default ISP. Example: 1
V4Alias	no	yes	String	IPv4 alias Example: name
V6Alias	no	yes	String	IPv6 alias. Example: name

Ipv6VpcSet

IPv6 address pool information.

Referenced by the following interfaces: DescribeIpv6Vpc

name	required	NULL allowed	type	description
SectionId	no	no	Uint64	ID of the associated IPv6 address pool. Example: 1
CidrBlock	no	no	String	IPv6 address range. Example: 3402:4e00:20:1200::/56
AddressType	no	no	Uint64	IPv6 address type. Example: 0/1
EnableSplit	no	no	Uint64	Whether to support automatic splitting. Example: 0: not supported; 1: customization supported.
Flag	no	no	Uint64	Whether it is idle. Example:
Description	no	no	String	Description information. Example:

VpcOssEniForDescribeEniInternal

Complex type: VpcOssEniForDescribeEniInternal.

Referenced by the following interfaces: DescribeEniInternal

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
Business	no	no	String	Name of the original VPC OSS API (v2): GetEni.business. Example: xxx
Owner	no	no	String	User app ID Example: 251198225
SubnetId	no	no	Int64	Integer subnetId. Example: 1990867
ArpLearningFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetEni.bArpLearning. Example: 1
EniId	no	no	Int64	Name of the original VPC OSS API (v2): GetEni.eniId. Example: 2660066
UniqueEniId	no	no	String	Name of the original VPC OSS API (v2): GetEni.uniqEniId. Example: eni-kj7karc5
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaynr6r
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-dbrazzr0
ElasticNetworkCardName	no	no	String	Name of the original VPC OSS API (v2): GetEni.ifrName. Example: veni_vFspLEfU
Type	no	no	Int64	Name of the original VPC OSS API (v2): GetEni.type. Example: 0
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetEni.createTime. Example: 2021-07-06 09:52:34
State	no	no	Int64	Name of the original VPC OSS API (v2): GetEni.state. Example: 1
Name	no	no	String	Name Example: TEST
VpcId	no	no	Int64	Integer VPCID. Example: 78257
Description	no	no	String	Name of the original VPC OSS API (v2): GetEni.description. Example: xxx
BusinessOwner	no	no	String	Name of the original VPC OSS API (v2): GetEni.businessOwner. Example: xxx
Mac	no	no	String	Name of the original VPC OSS API (v2): GetEni.mac. Example: 20:90:6F:BF:08:D2

AddressInfo

IP address template information

Referenced by the following interfaces: CreateAddressTemplate

name	required	NULL allowed	type	description
Address	yes	no	String	IP address. Example: 2.2.2.2
Description	no	no	String	Remarks. Example: desc
UpdatedTime	no	no	String	Update time. Example: 2020-08-10 18:10:12

UpdateVpcAssistCidrResult

Result of updating the secondary CIDR blocks of VPC.

Referenced by the following interfaces: UpdateVpcAssistCidrInternal

name	required	NULL allowed	type	description
NewAcfFlag	yes	no	Int64	Original parameter: bNewAfc. Example: 1
CreateTime	yes	no	String	Original parameter: createTime. Example: 2021-05-17 19:55:20
OwnedFlag	yes	no	Int64	Original parameter: ownedFlag. Example: 0
OldOperationRouteToVbcFlag	yes	no	Int64	Original parameter: oldBOpRouteToVbc. Example: 0
VpcId	yes	no	Int64	Original parameter: vpcId. Example: 16769060
UniqueVpcId	yes	no	String	Original parameter: uniqVpcId. Example: vpc-7zayowkt
VpgId	yes	no	Int64	Original parameter: vpgId. Example: 53786
Owner	yes	no	String	Original parameter: owner. Example: 251197522
IntMask	yes	no	Int64	Original parameter: intMask. Example: 16
OperationRouteToVbcFlag	yes	no	Int64	Original parameter: bOpRouteToVbc. Example: 1
VpcSubnet	yes	no	String	Original parameter: vpcSubnet. Example: 10.0.0.0
ZoneVpgFlag	yes	no	Int64	Original parameter: bZoneVpg. Example: 0
OldPublishVpgFlag	yes	no	Int64	Original parameter: oldBPublishVpg. Example: 1
VpcAssistCidrId	yes	no	Int64	Original parameter: vpcAssistCidrId. Example: 22811
AssistType	yes	no	Int64	Original parameter: assistType. Example: 0
Subnet	yes	no	String	Original parameter: subnet. Example: 10.4.0.0
Mask	yes	no	String	Original parameter: mask. Example: 255.255.0.0
VpcIntMask	yes	no	Int64	Original parameter: vpcIntMask. Example: 16

AddressTemplateGroup

IP Address Template Collection

Referenced by the following interfaces: CreateAddressTemplateGroup, DescribeAddressTemplateGroups

name	required	NULL allowed	type	description
AddressTemplateGroupName	yes	no	String	Name of IP address template collection. Example: demo
AddressTemplateGroupId	yes	no	String	IP address template collection instance ID, e.g., ipmg-dih8xdbq. Example: ipmg-oono4p1w
AddressTemplateIdSet	yes	no	Array of String	IP address template ID. Example: ["ipm-88620l7k","ipm-mdunqeb6"]
CreatedTime	no	no	String	Creation time. Example: 2018-06-21 11:32:29
AddressTemplateSet	yes	no	Array of AddressTemplateItem	IP address template instance. Example:View

SecurityGroupAssociationStatistics

Statistics of Instances Associated with Security Group

Referenced by the following interfaces: DescribeSecurityGroupAssociationStatistics

name	required	NULL allowed	type	description
SecurityGroupId	yes	no	String	Security group instance ID. Example: sg-o62agjal
CVM	yes	no	Uint64	CVM instance count. Example: 2
CDB	yes	no	Uint64	Database instance count. Example: 2
ENI	yes	no	Uint64	ENI instance count. Example: 2
SG	yes	no	Uint64	Number of references by security groups. Example: 2
CLB	yes	no	Uint64	Number of CLB instances. Example: 2
InstanceStatistics	yes	no	Array of InstanceStatistic	Full instance binding statistics. Example:View
TotalCount	yes	no	Uint64	Total count of all resources (excluding those referenced by security groups). Example: 10

VpcOssSubnetForDescribeVpcAndSubnetInternal

Complex type: VpcOssSubnetForDescribeVpcAndSubnetInternal.

Referenced by the following interfaces: DescribeVpcAndSubnetInternal

name	required	NULL allowed	type	description
Subnet	no	no	String	Subnet address. Example: 172.16.0.0
Name	no	no	String	Name Example: Default-Subnet
ZoneId	no	no	Int64	Name of the original VPC OSS API (v2): GetVpcAndSubnet.zoneId. Example: 100002
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-dbrazzr0
IntMask	no	no	Int64	Integer mask. Example: 20
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetVpcAndSubnet.createTime. Example: 2021-03-22 20:59:55
DefaultFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetVpcAndSubnet.bDefault. Example: 1
SubnetId	no	no	Int64	Integer subnetId. Example: 1990867
DhcpFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetVpcAndSubnet.dhcpFlag. Example: 0

AclRuleIdType

Local IP Translation ACL Rule ID Complex Type

Referenced by the following interfaces: DeleteLocalSourceIpPortTranslationAclRule

name	required	NULL allowed	type	description
AclRuleId	yes	no	Int64	Rule ID Example: 5

LocalSourceIpPortTranslationAclRule

Local Source IP Port Translation ACL Mapping Rules

Referenced by the following interfaces: CreateLocalSourceIpPortTranslationAclRule, DescribeLocalSourceIpPortTranslationAclRules

name	required	NULL allowed	type	description
Protocol	yes	no	String	Protocol Example: tcp
SourceCidr	yes	no	String	Source Address Example: 1.1.1.0/16
SourcePort	yes	no	String	Source Port Example: 80
DestinationCidr	yes	no	String	Destination address Example: 2.2.2.0/16
DestinationPort	yes	no	String	Destination port Example: 80
Action	no	no	Int64	Action. 0: Allow, 1: Reject. Example: 0
AclRuleId	no	no	Int64	ACL Rule ID Example: 26

HaVip

Description of HAVIP Information

Referenced by the following interfaces: CreateHaVip, DescribeHaVips

name	required	NULL allowed	type	description
Vip	yes	no	String	Virtual IP address. Example: 10.0.0.10
VpcId	yes	no	String	VPC ID of HAVIP. Example: vpc-hj3tw929
Visible	no	no	Bool	Whether the HAVIP is visible to the tenant. Example: True
CdcId	no	no	String	CDC instance ID. Example: cluster-gbo27yc4
HaVipId	yes	no	String	ID of HAVIP, which is the unique identifier of HAVIP. Example: havip-nsiwq8wkq
CreatedTime	yes	no	Datetime	Creation time. Example: 2018-10-10 17:03:09
TagSet	no	no	Array of Tag	Tag key-value pairs. Example:View
HaVipName	yes	no	String	HAVIP name. Example: demo
SubnetId	yes	no	String	Subnet ID of HAVIP. Example: subnet-4t7fr3fi
NetworkInterfaceId	yes	no	String	Associated ENI ID of HAVIP. Example: eni-pnpcf5il
InstanceId	yes	no	String	Bound instance ID. Example: ins-kmjyjbol
State	yes	no	String	Status: • AVAILABLE : Running. • UNBIND : Not bound. Example: AVAILABLE
HaVipAssociationSet	no	no	Array of HaVipAssociation	HAVIP switch scope. Example:View
CheckAssociate	no	no	Bool	Whether HAVIP switch scope verification is enabled. Example: True
AddressIp	yes	no	String	Bound EIP. Example: 100.10.123.131
Business	yes	no	String	Business identifier using havip. Example: SCF
FlushedTime	no	no	String	HAVIP refresh time. This parameter is used only as an output parameter. The refresh of FlushTime will be triggered by the following scenarios: (1) The instance sends a gratuitous ARP to trigger HAVIP drift. (2) Manually unbind the HAVIP from the ENI. The default value is 0000-00-00 00:00:00 when there is no update. Example: 2024-06-06 22:24:45
Ipv6Vip	no	no	String	Virtual IPv6 address. Example: 240d:c000:f030:900:0:9d0b:92a5:af00
IfnName	no	no	String	ENI interface name. Example: veth_21CF5180
IsCdc	no	no	Uint64	Whether it is a CDC type HAVIP. Example:

RouteTable

Route Table Object

Referenced by the following interfaces: CreateIpv6Routes, CreateRouteTable, CreateRoutes, DescribeRouteTables

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-m0c2kcun
RouteTableId	yes	no	String	Route table instance ID, e.g., rtb-aad4df1c. Example: rtb-324bqgtm
RouteTableName	yes	no	String	Route table name. Example: ruby
AssociationSet	yes	no	Array of RouteTableAssociation	Route Table Association. Example:View
RouteSet	yes	no	Array of Route	Route table policy set. Example:View
Main	yes	no	Bool	Whether it is a default route table. Example: True
CreatedTime	no	no	String	Creation time. Example: 2010-11-21
TagSet	no	no	Array of Tag	Tag key-value pairs. Example:View
SubnetNum	no	yes	Uint64	Subnet Count Example: 4
Region	no	no	String	Region. Example: sz
LocalCidrBlocks	no	no	String	Local routing. Example: 10.0.0.0/16

AclRuleId

Local IP Translation ACL Rule ID Complex Type

Referenced by the following interfaces: DeleteLocalIpTranslationAclRule

name	required	NULL allowed	type	description
RuleId	yes	no	Int64	Rule ID Example: 5
AclRuleId	no	no	Int64	ACL Rule ID Example: 6

Address

Describe EIP Information

Referenced by the following interfaces: DescribeAddresses, DescribeIp6Addresses

name	required	NULL allowed	type	description
AddressId	no	yes	String	ID of EIP, which is the unique identifier of EIP. Example: eip-ip9ongec
AddressName	no	yes	String	EIP name. Example: demoName
AddressStatus	no	yes	String	EIP status. 'CREATING': creating; 'BINDING': binding; 'BIND': bound; 'UNBINDING': unbinding; 'UNBIND': unbound; 'OFFLINING': releasing; 'BIND_ENI': bound to idle ENIs; 'PRIVATE': IPv6 address with public network access disabled. Example: UNBIND
AddressIp	no	yes	String	Public Network IP Address Example: 100.10.1.1
InstanceId	no	yes	String	ID of the bound resource instance, which may be a CVM, NAT, or BMS instance. Example: ins-qwz3er13
CreatedTime	no	yes	Datetime_iso	Creation time. It is expressed by a UTC time according to the ISO8601 standard. The format is YYYY-MM-DDThh:mm:ssZ. Example: 2021-05-19T08:37:53Z
NetworkInterfaceId	no	yes	String	Bound ENI ID Example: eni-37xao8t
PrivateAddressIp	no	yes	String	Private IP of Resource Bound Example: 10.2.3.4
IsArrears	no	yes	Bool	Resource isolation status. TRUE indicates that the EIP is isolated. FALSE indicates that the EIP is not isolated. Example: false
IsBlocked	no	yes	Bool	Resource blocking status. TRUE indicates that the EIP is blocked. FALSE indicates that the EIP is not blocked. Example: false
IsEipDirectConnection	no	yes	Bool	Whether EIP supports the Direct Connect mode. TRUE indicates Yes, and FALSE indicates No. Example: false
AddressType	no	yes	String	EIP resource types, including "CalcIP", "WanIP", "EIP", and "AnycastEIP". Where, "CalcIP" indicates device IP; "WanIP" indicates general public network IP; "EIP" indicates elastic public IP; and "AnycastEip" indicates accelerated EIP. Example: EIP
CascadeRelease	no	yes	Bool	Whether the EIP is automatically released after unbinding. True indicates that the EIP will be automatically released after unbinding. False indicates that the EIP will not be automatically released after unbinding. Example: false
EipAlgType	no	yes	AlgType	EIP ALG enabled protocol type. Example:View
InternetServiceProvider	no	yes	String	EIP ISP information. The current possible returned values include CMCC, CTCC, CUCC, and BGP. Example: BGP
TagSet	no	yes	Array of Tag	List of Tags Bound to EIP Example:View
CompliianceStatus	no	yes	String	EIP compliance status: BANNING and FREEZING. Others indicate normal. Example: BANNING
ApplicableForCLB	no	yes	Bool	Whether it is used for CLB. Example: True
IsNewGeneration	no	yes	Bool	Whether it is the next-generation EIP. Example: True
IsActiveAccessEip	no	yes	Bool	Whether to initiate active outbound connections. Example: True

name	required	NULL allowed	type	description
NetworkGroup	no	yes	String	EIP region information. Example: ap-region
PayMode	no	yes	String	Billing method. Example: BANDWIDTH_POSTPAID_BY_MONTH
DeadlineDate	no	yes	Date	Expiration time. Example: 2024-10-17 22:45:47
IsEip	no	yes	Bool	Whether it is EIP. Example: True
Bandwidth	no	yes	Uint64	Bandwidth value of EIP. Note: EIPs of traditional accounts do not have a bandwidth attribute, so the value is empty. Example: 1
UpdatedTime	no	yes	String	Update time. Example: 2024-10-17 22:45:47
InternetChargeType	no	yes	String	Network billing mode of the EIP. Note: EIPs under traditional account types do not have a billing mode attribute, and its value is empty. Example: TRAFFIC_POSTPAID_BY_HOUR
BindResourceType	no	yes	String	Bound resource type. Example: BIND_LB
LocalBgp	no	yes	Bool	Whether it is a local bandwidth EIP. Example: false
IsFromWanIP	no	yes	Bool	Whether to convert from WANIP. Example: true
UniVpcId	no	yes	String	VPC ID. Example: vpc-ig8xpno8
DedicatedClusterId	no	yes	String	Unique CDC ID. Example: cluster-gbo27yc4
OnlyActiveAccess	no	yes	Bool	Whether to allow only active outbound access. Example: true

CidrDetailSet

Non-standard IP Range Type

Referenced by the following interfaces: DescribeNmsCidrs

name	required	NULL allowed	type	description
AddrSegment	no	no	String	Non-standard IP Range Address Example: 10.0.0.0/8
AddressType	no	no	String	Network Type Example: Overlay
CreateTime	no	no	Datetime	Creation Time Example: 2024-05-22 11:58:26
IsReserved	no	no	Uint64	Whether it is a reserved address. Example: 0
Ver	no	no	String	Address type Example: IPv4

NetworkAclEntrySet

Network ACL Rule Collection

Referenced by the following interfaces: ModifyNetworkAclEntries

name	required	NULL allowed	type	description
Ingress	no	no	Array of NetworkAclEntry	Inbound rules. Example:View
Egress	no	no	Array of NetworkAclEntry	Outbound rules. Example:View

ReferredSecurityGroup

Security Group Referenced Information

Referenced by the following interfaces: DescribeSecurityGroupReferences

name	required	NULL allowed	type	description
SecurityGroupId	yes	no	String	Security group instance ID. Example: sg-pnpcf8l
ReferredSecurityGroupIds	yes	no	Array of String	All security group instance IDs with reference to security group instance ID (SecurityGroupId). Example: ["sg-nseejlbeby"]

VpcOssSubnet

Complex type: VpcOssSubnet.

Referenced by the following interfaces: DescribeRoutingTableListDetailInternal

name	required	NULL allowed	type	description
CdcFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.bCdc. Example: 0
DefaultFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.bDefault. Example: 1
UniqueCdcId	no	no	String	Name of the original VPC OSS API (v2): GetRtbListDetail.uniqCdcId. Example: cdc-asdqasd
UniqueSubnetId	no	no	String	The externally unique SubnetId. Example: subnet-sbrazer0
DhcpFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.dhcpFlag. Example: 0
Subnet	no	no	String	Subnet address Example: 172.16.0.0
Name	no	no	String	Name Example: Default-Subnet
Mask	no	no	String	Mask Example: 255.255.240.0
ZoneId	no	no	Int64	Name of the original VPC OSS API (v2): GetRtbListDetail.zoneId. Example: 100002
IntMask	no	no	Int64	Integer mask. Example: 20
SubnetId	no	no	Int64	Integer subnetId. Example: 1990867

DfwOssVMPolicy

Complex type: DfwOssVMPolicy.

Referenced by the following interfaces: DescribeVmPolicyInternal

name	required	NULL allowed	type	description
Policy	no	no	Array of DfwOssPolicies	Name of the original DFW API (v2): getVMPolicy.policy. Example:View
IsolateLevel	no	no	Int64	Name of the original DFW API (v2): getVMPolicy.isolateLevel. Example: 0
Uuid	no	no	String	Name of the original DFW API (v2): getVMPolicy.uuid. Example: 84ff9a2ad-6659-4864-808c-bd17f3c2acea
ErrorCode	no	no	Int64	Name of the original DFW API (v2): getVMPolicy.errorCode. Example: 0

NetDetectState

Network probe verification result.

Referenced by the following interfaces: DescribeNetDetectStates

name	required	NULL allowed	type	description
NetDetectId	yes	no	String	The network detection instance ID, such as netd-demoaq78. Example: netd-7v4wt576
NetDetectIpStateSet	yes	no	Array of NetDetectIpState	Validation result object array of the destination IP in network probe. Example:View

ServiceTemplateSpecification

Protocol Port Template

Referenced by the following interfaces: CreateSecurityGroupPolicies, CreateSecurityGroupWithPolicies, DeleteSecurityGroupPolicies, DescribeSecurityGroupPolicies, DescribeSecurityGroupPolicyTemplates, ModifySecurityGroupPolicies, ReplaceSecurityGroupPolicy

name	required	NULL allowed	type	description
ServiceId	yes	no	String	Protocol port ID, e.g., ppm-f5n1f8da. Example: ppm-f5n1f8da
ServiceGroupId	yes	no	String	Protocol port group ID, e.g, ppmg-f5n1f8da. Example: ppmg-f5n1f8da

UsedDetailDownload

Generation History of Traffic Package Usage Detail File

Referenced by the following interfaces: DescribeDownloadSpecificTrafficPackageUsedDetails

name	required	NULL allowed	type	description
Id	yes	no	Int64	Unique ID of Generation History Example: 5
TrafficPackageId	yes	no	String	Unique ID of Traffic Package Example: tfp-f7a3qh6x
StartTime	yes	no	Datetime	Start Time Example: 2021-10-10 10:00:00
EndTime	yes	no	Datetime	End time Example: 2021-10-10 10:00:00
DownloadUrl	yes	yes	String	Download link Example: https://ip-address-repo.cos.ap-region.mycloud.com
Filename	yes	no	String	File name Example: cos
Status	yes	no	String	Task status: RUNNING, SUCCESS, or FAIL. Example: RUNNING
ErrorMsg	yes	yes	String	Error Message Example: time out
ExpiredAt	yes	yes	Datetime	Download Link Expiration Time Example: 2021-10-10 10:00:00
CreatedAt	yes	no	Datetime	File Generation Time Example: 2021-10-10 10:00:00
IsExpired	yes	yes	Bool	Whether the download link has expired. Example: True

VpcOssService

Complex type: VpcOssService.

Referenced by the following interfaces: DescribeServiceByRealServerInternal

name	required	NULL allowed	type	description
Protocol	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.proto. Example: tcp
ResetFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.rstFlag. Example: 0
StickyTimeout	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.stickyTimeout. Example: 0
GroupId	no	no	Array of Int64	Original VPC OSS APIv2 name: GetServiceByRs.groupId. Example: [0]
RemoteVpcId	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.remoteVpcId. Example: 0
SetId	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.setId. Example: 0
VpcId	no	no	Int64	Integer VPCID. Example: 2598864
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-rpufyveg
Vip	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.vip. Example: 169.254.0.30
StickyFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.stickyFlag. Example: 0
UniqueVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.uniqVpcgwId. Example: vpcgw-7hk70tq8
ToaHostIpFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.toaHostIpFlag. Example: 0
NoSnatFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.noSnatFlag. Example: 0
HealthFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.healthFlag. Example: 1
Business	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.business. Example: dockerMaster
RouteSet	no	no	Array of VpcOssRoute	Original VPC OSS APIv2 name: GetServiceByRs.route. Example:View
StickyMaxCount	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.stickyMaxCount. Example: 0
VipVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.uniqVpcGwbrVpcgwId. Example: vpcgw-7hk7255d
VirtualPort	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.vport. Example: 443
BypassFlag	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.bypassFlag. Example: 0
Type	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.type. Example: 1
SubnetRouteAlgorithm	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.subnetRouteAlgorithm. Example: 0
VipSetId	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.vipSetId. Example: 0
UniqueClassicVpcGatewayId	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.uniqClassicVpcgwId. Example: vpcgw-7hk70tq8
VpcGatewayIp	no	no	String	Original VPC OSS APIv2 name: GetServiceByRs.vpcGwIp. Example: 9.105.119.10
LbType	no	no	Int64	Original VPC OSS APIv2 name: GetServiceByRs.lbType. Example:
RouteType	no	no	String	Service routing type. 0: The RS is in the current VPC; 1: The RS is in a physical network; 3: The RS is in another VPC. Example:

VpcIpv6Address

VPC private IPv6 object.

Referenced by the following interfaces: DescribeVpcIpv6Addresses

name	required	NULL allowed	type	description
Ipv6Address	yes	no	String	IPv6 address within VPC . Example: CVM/ENI
CidrBlock	yes	no	String	Subnet IPv6 CIDR . Example: 192.241.0.0/24
Ipv6AddressType	yes	no	String	IPv6 type. Example: CVM/ENI
CreatedTime	yes	no	String	IPv6 application time. Example: 2019-03-11T17:58:07

SSLVpnClient

SSLVpnClient

Referenced by the following interfaces: DescribeVpnGatewaySSLClients

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPCID Example: vpc-jaif7k23
VpnSslServerId	yes	no	String	VpnSslServerId Example: vpns-cjkt5c
CertStatus	yes	no	Int64	Certificate Status Example: 6
VpnSslClientId	yes	no	String	VpnSslClientId Example: vpnc-awe1254
CertBeginTime	yes	no	Datetime	Certificate Creation Time Example: 2021-02-03 00:00:00
CertEndTime	yes	no	Datetime	Certificate expiration time Example: 2021-02-04 00:00:00
State	yes	no	Int64	Client Creation Status Example: 6
Name	no	no	String	SSL VPN client name Example: vpn-client

VpcPrivateIpAddress

VPC private IP object.

Referenced by the following interfaces: DescribeVpcPrivateIpAddresses

name	required	NULL allowed	type	description
PrivateIpAddress	yes	no	String	Private IP of VPC . Example: 192.168.12.3
CidrBlock	yes	no	String	Subnet CIDR . Example: 192.241.0.0/24
PrivateIpAddressType	yes	no	String	Private IP type. Example: CVM/ENI
CreatedTime	yes	no	Datetime	IP application time. Example: 2020-06-06 10:00:00

DfwOssDeleteUSGRequest

Complex type: DfwOssDeleteUSGRequest.

Referenced by the following interfaces: DeleteUSGInternal

name	required	NULL allowed	type	description
UsgId	no	no	String	Name of the original DFW API (v2): deleteUSG.usgId. Example: 123123
ProjectId	no	no	String	Name of the original DFW API (v2): deleteUSG.projectId. Example: 123

DfwOssCreateUSGRequest

Complex type: DfwOssCreateUSGRequest.

Referenced by the following interfaces: CreateUSGInternal

name	required	NULL allowed	type	description
Sys	no	no	Int64	Name of the original DFW API (v2): createUSG.sys. Example: 1
SgId	no	no	String	Name of the original DFW API (v2): createUSG.sgId. Example: 123123
UsgName	no	no	String	Name of the original DFW API (v2): createUSG.usgName. Example: test
UsgRemark	no	no	String	Name of the original DFW API (v2): createUSG.usgRemark. Example: remark
ProjectId	no	no	String	Name of the original DFW API (v2): createUSG.projectId. Example: 123
Os	no	no	Int64	Name of the original DFW API (v2): createUSG.os. Example: 1

ItemPrice

Unidirectional Billing Price Information

Referenced by the following interfaces: InquiryPriceCreateVpcPeerConnection, InquiryPriceCreateVpnGateway, InquiryPriceNatGateway, InquiryPriceResetVpnGatewayInternetMaxBandwidth, InquiryPriceUpdateCcnBandwidth

name	required	NULL allowed	type	description
UnitPrice	no	no	Float	Unit price of Pay-as-you-go (postpaid) billing mode, with the unit being USD. Example: 1.0
ChargeUnit	no	no	String	Pay-as-you-go (postpaid) billing unit. The value range is as follows. HOUR: Indicates the billing unit is hour. Scenarios involving this billing unit include instance postpaid by hour (POSTPAID_BY_HOUR), and bandwidth postpaid by hour (BANDWIDTH_POSTPAID_BY_HOUR). GB: Indicates the billing unit is GB. Scenarios involving this billing unit include traffic postpaid by hour (TRAFFIC_POSTPAID_BY_HOUR). Example: HOUR
OriginalPrice	no	no	Float	Original price of prepaid product, with the unit being USD. Example: 1.0
DiscountPrice	no	no	Float	Discounted price for prepaid products, with the unit being USD. Example: 0.5

BandwidthLimitForCcnAlarmOnly

CCN Regional Outbound Bandwidth Limit

Referenced by the following interfaces: BandwidthLimitForCcnAlarmOnly

name	required	NULL allowed	type	description
Region	yes	no	String	Region. For example, ap-region. Example: region
BandwidthLimit	yes	no	Uint64	Outbound bandwidth cap, in Mbps. Example: 100
VpcId	yes	no	Uint64	Integer ID. Example: 65535
CcnId	yes	no	String	Instance ID. Example: ccn-245ecr35

CvmInstance

CVM instance information.

Referenced by the following interfaces: DescribeVpcInstances

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID. Example: vpc-67wlq16v
SubnetId	yes	no	String	Subnet instance ID. Example: subnet-hj3her929
InstanceId	yes	no	String	CVM Instance ID Example: ins-nswq8wkq
InstanceName	yes	no	String	CVM name. Example: demo
InstanceState	yes	no	String	CVM status. Example: RUNNING
CPU	yes	no	Uint64	The CPU core count of the instance, in cores. Example: 8
Memory	yes	no	Uint64	Instance memory capacity, in GB. Example: 32
CreatedTime	yes	no	String	Creation time. Example: 2020-06-08 10:00:00
InstanceType	yes	no	String	Instance model. Example: SA3.2XLARGE32
EniLimit	yes	no	Uint64	Instance ENI quota (including the primary network interface). Example: 6
EniIpLimit	yes	no	Uint64	Instance ENI private IP quota (including the primary network interface). Example: 20
InstanceEniCount	yes	no	Uint64	Number of ENIs bound to the instance (including the primary ENI). Example: 1

NetworkInterfaceAttachment

ENI Binding Relationship

Referenced by the following interfaces: CreateAndAttachNetworkInterface, CreateNetworkInterface, DescribeNetworkInterfaces, DescribeNetworkInterfacesEx, DescribeNetworkInterfacesExtra

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Cloud host instance ID. Example: ins-89k2kjt4
DeviceIndex	yes	no	Uint64	Sequence number of the ENI inside the CVM instance. Example: 0
InstanceAccountId	yes	no	String	Account information of CVM owner. Example: jkt4567
AttachTime	yes	no	String	Binding time. Example: 2021-06-17 11:24:24

NatGatewayAddress

Elastic IP Bound to NAT Gateway

Referenced by the following interfaces: CreateNatGateway, DescribeNatGateways

name	required	NULL allowed	type	description
AddressId	no	no	String	The unique ID of the EIP, such as eip-jrkzpvgt . Example: eip-jrkzpvgt
PublicIpAddress	no	no	String	Public IP address, e.g., 123.121.34.33. Example: 123.121.34.3
IsBlocked	no	no	Bool	Resource blocking status. TRUE indicates that the EIP is blocked. FALSE indicates that the EIP is not blocked. Example: true

BandwidthAttribute

Bandwidth Attributes

Referenced by the following interfaces: DescribeBandwidthAttribute

name	required	NULL allowed	type	description
NetworkPayMode	yes	yes	Array of String	Network billing mode list. Values include BANDWIDTH_POSTPAID_BY_MONTH, BANDWIDTH_PREPAID_BY_MONTH, TRAFFIC_POSTPAID_BY_HOUR, BANDWIDTH_POSTPAID_BY_HOUR, BANDWIDTH_PACKAGE. Example: TRAFFIC_POSTPAID_BY_HOUR
networkPayMode	no	yes	Array of Int64	Network billing mode list. Example: TRAFFIC_POSTPAID_BY_HOUR
CvmPayMode	yes	yes	Array of String	CVM instance billing mode list. Values include "PREPAID", "POSTPAID_BY_HOUR", and "CDHPAID". Example: POSTPAID_BY_HOUR
cvmPayMode	no	yes	Array of Int64	List of CVM instance billing modes. Example: POSTPAID_BY_HOUR
Cpu	yes	yes	Array of Int64	CPU core range, a front-off rear-off range, e.g., [9,23], which indicates 9 <= CPU core count <= 23. An empty range indicates support for any CPU core count. Example: 1
cpu	no	yes	Array of Int64	CPU core range, a front-off rear-off range, e.g., [9,23], which indicates 9 <= CPU core count <= 23. An empty range indicates support for any CPU core count. Example: 1
ZoneId	yes	yes	Array of Int64	Availability zone ID list. An empty list indicates support for any availability zone ID. Example: 21
zoneId	no	yes	Array of Int64	Availability zone ID list. An empty list indicates support for any availability zone ID. Example: 21
BandwidthUpper	yes	no	Int64	Maximum Bandwidth Example: 200
bandwidthUpper	no	yes	Int64	Maximum Bandwidth Example: 200
BandwidthLimit	yes	yes	Int64	Whether the bandwidth must have a cap. 1 indicates Yes, and 0 indicates No. Example: 0
bandwidthLimit	no	yes	Int64	Whether the bandwidth must have a cap. 1 indicates Yes, and 0 indicates No. Example: 0
ResourceIds	no	no	String	List of unique IDs of resources, which can be CVM Instance ID, or unique ID of EIP. Example: eip-d97psd1o

VpcOssIp

Complex type: VpcOssIp.

Referenced by the following interfaces: DescribeIpInternal

name	required	NULL allowed	type	description
DirtyFlag	no	no	Int64	Name of the original VPC OSS API (v2): GetIp.bDirty. Example: 0
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmayw9z
Ip	no	no	String	Name of the original VPC OSS API (v2): GetIp.ip. Example: 169.254.128.2
Mask	no	no	String	Mask Example: 255.255.128.0
UniqueInstanceId	no	no	String	Name of the original VPC OSS API (v2): GetIp.uniqInstanceId. Example: instance-asdaq1
IpType	no	no	Int64	Name of the original VPC OSS API (v2): GetIp.ipType. Example: 0
CreateTime	no	no	String	Name of the original VPC OSS API (v2): GetIp.createTime. Example: 2021-03-22 21:35:59
Subnet	no	no	String	Subnet address Example: 169.254.128.0
VpcId	no	no	Int64	Integer VPCID. Example: 78257
IntSubnet	no	no	Int64	Name of the original VPC OSS API (v2): GetIp.intSubnet. Example: 2852028416
Gateway	no	no	String	Name of the original VPC OSS API (v2): GetIp.gateway. Example: 169.254.128.1
Flag	no	no	Int64	Name of the original VPC OSS API (v2): GetIp.flag. Example: 0

InstanceChargePrepaid

Prepaid (Monthly Subscription) billing object.

Referenced by the following interfaces: CreateVpnGateway, InquiryPriceCreateVpnGateway

name	required	NULL allowed	type	description
Period	yes	no	Uint64	Purchased instance duration, in months. Value range: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, 36. Example: 5
RenewFlag	no	no	String	Auto-renewal flag. Value range: NOTIFY_AND_AUTO_RENEW: notify and auto-renew on expiration, NOTIFY_AND_MANUAL_RENEW: notify and do not auto-renew on expiration. Default: NOTIFY_AND_MANUAL_REVIEW. Example: NOTIFY_AND_AUTO_RENEW

DestinationIpPortTranslationNatRule

Port Forwarding Rules of NAT Gateway

Referenced by the following interfaces: CreateNatGateway, CreateNatGatewayDestinationIpPortTranslationNatRule, DeleteNatGatewayDestinationIpPortTranslationNatRule, DescribeNatGateways, ModifyNatGatewayDestinationIpPortTranslationNatRule

name	required	NULL allowed	type	description
IpProtocol	yes	no	String	IP options: TCP and UDP . Example: TCP
PublicIpAddress	yes	no	String	Elastic IP. Example: 20.20.20.20
PublicPort	yes	no	Uint64	Public network port. Example: 80

name	required	NULL allowed	type	description
PrivateIpAddress	yes	no	String	Private network address. Example: 10.10.10.10
PrivatePort	yes	no	Uint64	VPC port. Example: 80
Description	yes	no	String	Description of NAT gateway forwarding rules. Example: for_demo

DfwOssCreateUSGResult

Complex type: DfwOssCreateUSGResult.

Referenced by the following interfaces: CreateUSGInternal

name	required	NULL allowed	type	description
SgId	no	no	String	Name of the original DFW API (v2): createUSG.sgId. Example: 251197522
UsgId	no	no	String	Name of the original DFW API (v2): createUSG.usgId. Example: sg-ispsj3ah
UsgName	no	no	String	Name of the original DFW API (v2): createUSG.usgName. Example: test_sdk

InstanceStatistic

For Description of the Statistical Information of Instance

Referenced by the following interfaces: DescribeSecurityGroupAssociationStatistics

name	required	NULL allowed	type	description
InstanceType	yes	no	String	Instance Type Example: CVM
InstanceCount	yes	no	Uint64	Number of Instances Example: 10

DfwOssInsertUSGRuleRequest

Complex type: DfwOssInsertUSGRuleRequest.

Referenced by the following interfaces: CreateUSGRuleInternal

name	required	NULL allowed	type	description
UsgId	no	no	String	Name of the original DFW API (v2): insertUSGRule.usgId. Example: 123123
Index	no	no	Int64	Name of the original DFW API (v2): insertUSGRule.index. Example: 1
Direction	no	no	String	Name of the original DFW API (v2): insertUSGRule.direction. Example: inbound
Version	no	no	Int64	Name of the original DFW API (v2): insertUSGRule.version. Example: 12
Policies	no	no	Array of DfwOssUSGPolicyItem	Name of the original DFW API (v2): insertUSGRule.policies. Example:View

AssistantCidr

VPC's auxiliary CIDR information.

Referenced by the following interfaces: CreateAssistantCidr, CreateVpc, DescribeAssistantCidr, DescribeVpcInternal, DescribeVpcs, ModifyAssistantCidr

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC instance ID , e.g., vpc-6v2ht8q5 . Example: vpc-napxigxr5
CidrBlock	yes	no	String	Auxiliary CIDR, e.g., 172.16.0.0/16 . Example: 192.241.0.0/24
AssistantType	yes	no	Int64	Auxiliary CIDR type (0: Normal auxiliary CIDR, 1: Container auxiliary CIDR), The default is 0. Example: 0: 'NORMAL', 1: 'DOCKER'
SubnetSet	yes	yes	Array of Subnet	Subnets split by auxiliary CIDR. Example:View
Region	no	no	String	Region information. Example: sz

CcnLimit

CCN Quota

Referenced by the following interfaces: DescribeCcnLimits

name	required	NULL allowed	type	description
Type	yes	no	String	CCN Quota Type Example: 1
Value	yes	no	Uint64	CCN Quota Value Example: 10

VpcOssRouteForUpdateRouteWeightInternal

Complex type: VpcOssRouteForUpdateRouteWeightInternal.

Referenced by the following interfaces: UpdateRouteWeightInternal

name	required	NULL allowed	type	description
PrivateIp	no	no	String	Original VPC OSS APIv2 name: UpdateRouteWeight.pip. Example: 10.19.0.121
ProtocolPort	no	no	Int64	Original VPC OSS APIv2 name: UpdateRouteWeight.pport. Example: 8080
Weight	no	no	Int64	Original VPC OSS APIv2 name: UpdateRouteWeight.weight. Example: 10

Ipv6SubnetCidrBlock

IPv6 subnet IP range object.

Referenced by the following interfaces: AssignIpv6SubnetCidrBlock, UnassignIpv6SubnetCidrBlock

name	required	NULL allowed	type	description
SubnetId	yes	no	String	Subnet instance ID , e.g., subnet-pxir56ns . Example: subnet-8qywqc4y
Ipv6CidrBlock	no	no	String	IPv6 subnet IP range, e.g., 3402:4e00:20:1000::/64 . Example: 3402:4e00:20:1200::/56
AddressType	no	no	String	IPv6 address type. Example: GUA
ISPType	no	no	String	ISP type of the IPv6 CIDR block. Valid values: 'BGP' (default type), 'CMCC', 'CTCC', and 'CUCC'. Example: BGP

Service

Service Information

Referenced by the following interfaces: DescribeServiceInternal

name	required	NULL allowed	type	description
VpcId	no	no	String	vpc id Example: vpc-m0c2kcun
RouteSet	no	no	Array of ServiceRoute	Routing information set. Example:View
GroupId	no	no	Array of Uint64	Group ID Example: 5
SetId	no	no	Uint64	Set id Example: 0
StickyTimeout	no	no	Uint64	Session persistence timeout duration. Example: 0
VipSetId	no	no	Uint64	VIP set ID. Example: 1
VpcGatewayIp	no	no	String	The vpcgwip accessed via Direct Connect. Example: 10.112.98.185
VirtualPort	no	no	Uint64	Vport port number. Example: 23
HealthFlag	no	no	Uint64	Health identifier. Example: 0
SubnetRouteAlgorithm	no	no	Uint64	Hash algorithm. Example: 0
BypassFlag	no	no	Uint64	Bypass identifier. Example: 0
ResetFlag	no	no	Uint64	RST message identifier. Example: 0
Type	no	no	Uint64	Type Example: 1
Protocol	no	no	String	Protocol Example: udp
IpType	no	no	Uint64	IP Type Example: 29
ClassicVpcGatewayId	no	no	String	The vpcgw cluster that accesses the VIP via ClassicLink. Example: vpcgw-7hk7255d
VpcNumId	no	no	Int64	The numeric ID of the VPC. Example: 122211
VpcGatewayAttrFlag	no	no	Uint64	When the vpcgw cluster type is 3 (vpcgw logical cluster selected based on the RS availability zone), the marker indicates whether forwarding is based on the VPCID + vip granularity of the cluster ID attribute. Example: 0
SnatFlag	no	no	Uint64	SNAT identifier. Example: 0
StickyMaxCount	no	no	Uint64	Maximum value for session persistence entries. Example: 1
RemoteVpcId	no	no	Uint64	Remote VPC ID. Example: 0
VpcGatewayId	no	no	String	The vpcgw cluster ID accessed via CVM. Example: vpcgw-7hk7255d
Business	no	no	String	Business type identifier. Example: dockerMaster
VpcGatewayZoneId	no	no	Uint64	When the vpcgw cluster type is 3 (vpcgw logical cluster selected based on the RS availability zone), it is used to return the availability zone of the RS. Example: 0
FakeToaIp	no	yes	String	fakeToaIp is used to populate a fake client IP. Example: 192.168.0.1

name	required	NULL allowed	type	description
ToaHostIpFlag	no	no	Uint64	Whether the TOA includes the client's host IP identifier. Example: 0
LbType	no	no	Uint64	Whether it is an L8 rule. Example: 0
VipVpcGatewayId	no	no	String	Switch vpcGwIp. Select the vpcgwid corresponding to the vpcGwIp in the zone of the subnet where the VIP is located, choosing the nearest option. Example: vpcgw-7hk7255d
Vip	no	no	String	VIP information Example: 172.16.48.216
StickyFlag	no	no	Uint64	Session persistence identifier. Example: 0
RsZoneVpcGatewayId	no	no	Uint64	When the vpcgw cluster type is 3 (vpcgw logical cluster selected based on the RS availability zone), the marker indicates whether the cluster ID is forwarded based on the vpcid + vip granularity. If bVpcgwAttrFlag=1, the cluster ID is returned; otherwise, 0 is returned, indicating that forwarding based on the cluster ID is disabled. Example: 0
DelPipRouteFlag	no	no	Int64	Original VPC OSS APIv2 name: AddService.bDelPipRoute. Example: 0

AddressLibInfo

IP Address Library Information

Referenced by the following interfaces: DescribeIpLocation, DescribeIpOnline

name	required	NULL allowed	type	description
Country	yes	no	String	Country Information Example: UK
Province	yes	no	String	Information of Administrative Zone at Province, State, or County Level Example: ap-region
City	yes	no	String	Municipal Administrative Region Information Example: ap-region
Region	yes	no	String	Urban Region Information Example: ap-region
Isp	yes	no	String	Access ISP Information Example: BGP
Addressip	yes	no	String	Query IP Address Example: 10.21.3.2
AsName	yes	no	String	Backbone ISP Information Example: CTCC
AsId	yes	no	String	ISP AS Number Example: CTCC
Comment	yes	no	String	Comment information. The currently filled value is the APN value of mobile access users. If there is no APN attribute, it will be empty. Example: demo
InternetServiceProvider	yes	no	String	Same ISP, deprecated. Example: BGP

IpField

Field Information for IP Online Query

Referenced by the following interfaces: DescribeIpLocation, DescribeIpOnline

name	required	NULL allowed	type	description
Country	no	no	Bool	National Field Information Example: true
Province	no	no	Bool	Administrative zone information at province, state, or county level. Example: true
City	no	no	Bool	Field Information on Municipal Administrative Region Example: true
Region	no	no	Bool	Urban zone field information Example: true
Isp	no	no	Bool	Access ISP Field Information Example: true
AsName	no	no	Bool	Backbone ISP Field Information Example: true
AsId	no	no	Bool	Backbone AS Number Example: true
Comment	yes	no	Bool	Comment Field Example: true

VpcOssNatServiceRequestForCreateNatGatewayServiceInternal

Complex type: VpcOssNatServiceRequestForCreateNatGatewayServiceInternal.

Referenced by the following interfaces: CreateNatGatewayServiceInternal

name	required	NULL allowed	type	description
Business	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.business. Example: xxx
BusinessOwner	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.businessOwner. Example: xxx
VpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.vgwIndex. Example: xxx
Count	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.count. Example: 10
VirtualPort	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.vport. Example: 111
SkipCheckPrivateIpDatabaseFlag	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.bSkipCheckPipDb. Example: 0
GwType	no	no	Int64	JNSGW type. Valid values: 0 and 1. Example: 0
ProtocolPort	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.pport. Example: 554
GatewayIp	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.gwIp. Example: 1.1.1.1
IpType	no	no	Uint64	ipType value applied for by the service from VPC OSS. Example: 10
Protocol	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.proto. Example: tcp
PrivateIp	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.pip. Example: 172.16.0.18
Bandwidth	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.bandwidth. Example: 10
VpcId	no	no	Int64	Integer VPCID. Example: 123
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywfbr
Owner	yes	no	String	User app ID Example: 251198225
VirtualGatewayType	no	no	Int64	Name of the original VPC OSS API (v2): AddNatgwService.vgwType Example: 0
UniqueVpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): AddNatgwService.uniqVgwIndex. Example: xxx
SubnetId	no	no	Int64	Integer subnetId. Example: 123

DfwOssVMOperateResult

Complex type: DfwOssVMOperateResult.

Referenced by the following interfaces: AttachPolicyToVMInternal, DeletePolicyFromVmInternal

name	required	NULL allowed	type	description
Uuid	no	no	String	Name of the original DFW API (v2): addPolicyToVM.uuid. Example: 84f9a2ad-6659-4864-808c-bd1793c2acea
ErrorCode	no	no	Int64	Name of the original DFW API (v2): addPolicyToVM.errorCode. Example: 0
ErrorInfo	no	no	String	Name of the original DFW API (v2): addPolicyToVM.errodInfo. Example: success

VpcOssNatServiceRequest

Complex type: VpcOssNatServiceRequest.

Referenced by the following interfaces: DeleteNatGatewayServiceInternal

name	required	NULL allowed	type	description
UniqueVpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.uniqVgwIndex. Example: xxx
Business	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.business. Example: xxx
SubnetId	no	no	Uint64	Integer subnetId. Example: 123
VpcId	no	no	Int64	Integer VPCID. Example: 123
Owner	yes	no	String	User app ID Example: 251198225
Protocol	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.proto Example: tcp
Vip	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.vip. Example: 1.1.1.1
VirtualPort	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.vport. Example: 111
PrivateIp	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.pip. Example: 172.16.0.18
ProtocolPort	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.pport. Example: 554
VpcGatewayIndex	no	no	String	Name of the original VPC OSS API (v2): DelNatgwService.vgwIndex. Example: xxx
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-jmaywfbr
VirtualGatewayType	no	no	Int64	Name of the original VPC OSS API (v2): DelNatgwService.vgwType. Example: 0

AddressBase

EIP Basic Information

Referenced by the following interfaces: DescribeAddressSet

name	required	NULL allowed	type	description
InternetServiceProvider	yes	no	String	ISP, including Mobile, Unicom, Telecom, and cloud platform CAP. Example: BGP
SetName	yes	no	String	EIP Cluster Name Example: demo
SetId	yes	no	Int64	Unique ID of EIP Cluster Example: 24523
AddressIp	yes	no	String	EIP Address Example: 10.23.32.2
IsDpdk	yes	no	Bool	Whether EIP supports DPDK. Example: True
Status	yes	no	String	Whether the EIP is available. Example: Used

NetDetect

Network probe object.

Referenced by the following interfaces: CreateNetDetect, DescribeNetDetects

name	required	NULL allowed	type	description
VpcId	yes	no	String	The VPC instance ID , such as vpc-demoag78 . Example: vpc-67wlqf6v
VpcName	yes	no	String	VPC instance name. Example: demo
SubnetId	yes	no	String	The subnet instance ID, such as subnet-demoag78. Example: subnet-8qywqc4y
SubnetName	yes	no	String	Subnet instance name. Example: demo
NetDetectId	yes	no	String	The network detection instance ID, such as netd-demoag78. Example: netd-7v4wt576
NetDetectName	yes	no	String	Network probe name, up to 60 bytes in length. Example: demo
DetectDestinationIp	yes	no	Array of String	Probe destination IPv4 address array. The maximum number is two. Example: ["1.1.1.3", "1.1.1.8"]
DetectSourceIp	yes	no	Array of String	IPv4 array of probe sources automatically allocated by the system. The length is 2. Example: ["1.1.1.3", "1.1.1.8"]
NextHopType	yes	no	String	Next hop type, currently supporting: VPN: VPN gateway; DIRECTCONNECT: Direct Connect gateway; PEERCONNECTION: Peer connection; NAT: NAT gateway; NORMAL_CVM: Normal CVM. Example: CVM
NextHopDestination	yes	no	String	The next hop target gateway, with valid values depending on the next hop type: When the next hop type is VPN, the value should be the VPN gateway ID, such as vpngw-demoag78. When the next hop type is DIRECTCONNECT, the value should be the Direct Connect gateway ID, such as dcg-demoag78. When the next hop type is PEERCONNECTION, the value should be the peering connection ID, such as pcx-demoag78. When the next hop type is NAT, the value should be the NAT gateway, such as nat-demoag78. When the next hop type is NORMAL_CVM, the value should be the CVM IPv4 address, such as 10.0.0.12. Example: 10.0.0.198
NextHopName	yes	yes	String	Next hop gateway name. Example: demo
NetDetectDescription	yes	yes	String	Network probe description. Example: demo
CreateTime	yes	yes	Datetime	Creation time. Example: 2018-06-21 11:32:29
Status	no	no	String	NFV network detection status. Example: RUNNING

SecurityGroupPolicyTemplate

Security Group Rule Template

Referenced by the following interfaces: DescribeSecurityGroupPolicyTemplates

name	required	NULL allowed	type	description
TemplateName	yes	no	String	Template name. Example: demo
TemplateRemark	yes	no	String	Template description. Example: demo
Ingress	yes	no	Array of SecurityGroupPolicy	Inbound rules. Example:View
Egress	yes	no	Array of SecurityGroupPolicy	Outbound rules. Example:View

VpcOssVpcCidr

Complex type: VpcOssVpcCidr.

Referenced by the following interfaces: UpdateVpcAssistCidrInternal

name	required	NULL allowed	type	description
Owner	no	no	String	User app ID Example: 251198225
Subnet	no	no	String	Subnet address Example: 172.16.0.0
IntMask	no	no	Int64	Integer mask. Example: 20
OperationRouteToVbcFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcAssistCidrbOpRouteToVbc. Example: 1
PublishVpgFlag	no	no	Int64	Name of the original VPC OSS API (v2): bPublishVpg. Example: 1
VpcId	no	no	Int64	Integer VPCID. Example: 78257
UniqueVpcId	no	no	String	The externally unique VPCID. Example: vpc-fjknxwrj

LocalIpTranslationNatRule

Local IP Translation Complex Type

Referenced by the following interfaces: CreateLocalIpTranslationNatRule, CreatePeerIpTranslationNatRule, DeleteLocalIpTranslationNatRule, DeletePeerIpTranslationNatRule, DescribeLocalIpTranslationNatRules, DescribePeerIpTranslationNatRules

name	required	NULL allowed	type	description
OriginalIp	yes	no	String	Original IP Example: 10.0.0.5
TranslationIp	yes	no	String	Mapping IP Example: 2.2.2.2
Description	yes	yes	String	Description Example: for_demo

SSLVpnServer

SSLVpnServer

Referenced by the following interfaces: DescribeVpnGatewaySSLServers

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC ID Example: vpc-jaif7kz3
VpnSslServerId	yes	no	String	VpnSslServerId Example: vpns-adws41c
VpnGatewayId	yes	no	String	VpnGatewayId Example: vpngw-1u2xtmbz
SSLVpnServerName	yes	no	String	SSLVpnServerName Example: server-name
LocalAddress	yes	no	String	Local Segmentation Address Example: 10.0.0.0/16
RemoteAddress	yes	no	String	Customer Address Example: 172.0.0.0/23
MaxConnection	yes	no	Array of Int64	Connections Example: 23
WanIp	yes	no	String	Public IP Example: jkt.14.51.3
State	yes	no	Int64	Server Creation Status Example: 6
SSLVpnProtocol	no	no	String	The listening protocol of the SSL VPN server. Example: UDP
SSLVpnPort	no	no	String	The listening protocol port of the SSL VPN server. Example: 1194
EncryptAlgorithm	no	no	String	Encryption algorithm. Example: AES-128-CBC
IntegrityAlgorithm	no	no	String	Authentication algorithm. Example: SHA1
CreateTime	no	no	String	Creation Time Example: 2021-03-24 15:31:56

Price

Price

Referenced by the following interfaces: InquiryPriceCreateVpcPeerConnection, InquiryPriceCreateVpnGateway, InquiryPriceNatGateway, InquiryPriceResetVpnGatewayInternetMaxBandwidth

name	required	NULL allowed	type	description
InstancePrice	no	no	ItemPrice	Instance price. Example:View
BandwidthPrice	no	no	ItemPrice	Network price. Example:View

VpnGatewayQuota

VPN Gateway Quota Object

Referenced by the following interfaces: CreateVpnGateway, DescribeVpnGatewayQuota, DescribeVpnGateways

name	required	NULL allowed	type	description
Bandwidth	yes	no	Uint64	Bandwidth Quota Example: 100
Cname	yes	no	String	Name of Quota Example: Large

name	required	NULL allowed	type	description
Name	yes	no	String	Quota's English Name Example: newlarge

VpnGateway

VPN gateway object.

Referenced by the following interfaces: CreateVpnGateway, DescribeVpnGateways

name	required	NULL allowed	type	description
VpnGatewayId	yes	no	String	Gateway instance ID. Example: vpngw-az2nuzp5
VpcId	yes	no	String	VPC instance ID. Example: vpc-qqa5md5
VpnGatewayName	yes	no	String	Gateway instance name. Example: demo-gateway
Type	yes	no	String	Gateway instance type: IPSEC, SSL, CCN. Example: IPSEC
State	yes	no	String	Gateway instance status: 'PENDING' - pending production, 'DELETING' - Deleting, and 'AVAILABLE' - in operation. Example: AVAILABLE
PublicIpAddress	yes	no	String	Public IP of gateway. Example: 139.124.3.2
RenewFlag	yes	no	String	Gateway renewal type: 'NOTIFY_AND_MANUAL_RENEW' - manually renew, 'NOTIFY_AND_AUTO_RENEW' - automatically renew, 'NOT_NOTIFY_AND_NOT_RENEW' - not to renew upon expiration. Example: NOTIFY_AND_MANUAL_RENEW
InstanceChargeType	yes	no	String	Gateway payment types: POSTPAID_BY_HOUR: postpaid by hour; PREPAID: prepaid by year/month. Example: POSTPAID_BY_HOUR
InternetMaxBandwidthOut	yes	no	Uint64	Outbound bandwidth of the gateway. Example: 5
CreatedTime	yes	no	Datetime	Creation time. Example: 2021-04-25 17:14:34
ExpiredTime	yes	no	Datetime	Expiration time of prepaid gateway. Example: 2021-04-25 17:14:34
IsAddressBlocked	yes	no	Bool	Whether the public IP is blocked. Example: false
NewPurchasePlan	yes	no	String	Billing mode change. PREPAID_TO_POSTPAID: prepaid by year/month to postpaid by hour. Example: PREPAID_TO_POSTPAID
RestrictState	yes	no	String	Gateway billing state. PROTECTIVELY_ISOLATED: Instance that is securely isolated, NORMAL: Normal. Example: PROTECTIVELY_ISOLATED
Zone	yes	no	String	Availability zone. For example, ap-region-2. Example: ap-region-2
VpnGatewayQuotaSet	yes	no	Array of VpnGatewayQuota	Gateway Bandwidth Quota Information Example:View
Version	yes	no	String	Gateway Instance Version Information Example: 1.0
NetworkInstanceId	yes	no	String	When the value of Type is CCN, this value indicates CCN Instance ID. Example: ccn-gree226l
IspType	yes	no	String	Public IP ISP Example: 5
ProtocolType	no	no	String	Protocol type IPSEC/SSL. Example: IPSEC
NetworkType	no	no	String	Network type. Currently, only VPC is supported. Example: VPC
MaxConnection	no	no	Uint64	The maximum connections. Example: 5
CreateSSLServer	no	no	Bool	Whether the SSL server has been created. Example: true
CdcId	no	yes	String	CDC instance ID. Example: cluster-gbo27yc4

NatGatewayDestinationIpPortTranslationNatRule

Port Forwarding Rules of NAT Gateway

Referenced by the following interfaces: DescribeNatGatewayDestinationIpPortTranslationNatRules

name	required	NULL allowed	type	description
IpProtocol	no	no	String	IP options: `TCP` and `UDP`. Example: TCP
PublicIpAddress	yes	no	String	Elastic IP. Example: jkt.jkt.jkt.jkt
PublicPort	yes	no	Uint64	Public network port. Example: 443
PrivateIpAddress	yes	no	String	Private network address. Example: 192.168.1.2
PrivatePort	yes	no	Uint64	VPC port. Example: 443
Description	no	no	String	Description of NAT gateway forwarding rules. Example: Port forwarding example
NatGatewayId	yes	yes	String	ID of NAT gateway. Example: nat-3iinf9tr0
VpcId	yes	yes	String	VPC ID. Example: vpc-rkzpefgh
CreatedTime	yes	yes	String	Creation time of NAT gateway forwarding rule. Example: "2021-05-24 19:28:31"

VpcOssUpdatePeer

Complex type: VpcOssUpdatePeer.

Referenced by the following interfaces: UpdateVpcPeerInternal

name	required	NULL allowed	type	description
SrcVpcSubnet	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.sVpcSubnet. Example: 172.16.0.0
OldName	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldName. Example: DDDD
SrcVpcId	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.sVpcId. Example: 78257
LocalBandwidth	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.localBandwidth. Example: 0
OldDestVpcIntMask	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldDVpcIntMask. Example: 16
OldSrcExpireTime	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldSExpireTime. Example: 2021-12-31 19:41:49
VirtualSafeGroupIp	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.vsgIp. Example: 0.0.0.0
DestViewFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.dViewFlag. Example: 1
OldState	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldState. Example: 1
OwedFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.owedFlag. Example: 0
NewAfcFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bNewAfc. Example: 0
OldWanOutLimit	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldWanOutLimit. Example: 0
Type	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.type. Example: 0
OldLastState	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldLastState. Example: 0
OldVirtualSafeGroupIp	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldVsgIp. Example: 0.0.0.0
UniqueDestVpcId	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.uniqDVpcId. Example: vpc-n05sx3vl
SrcOwner	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.sOwner. Example: 251198225
State	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.state. Example: 1
OldSrcVpcIntMask	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldSVpcIntMask. Example: 16
UniqueSrcVpcId	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.uniqSVpcId. Example: vpc-jmaywl6r
DestVpcId	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.dVpcId. Example: 76644
OldNewAfcFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldBNewAfc. Example: 0
DestVpcIntMask	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.dVpcIntMask. Example: 16
OldSrcVpcSubnet	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldSVpcSubnet. Example: 172.16.0.0
DestRegion	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.dRegion. Example: 0
OldDestViewFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldDViewFlag. Example: 1
SrcRegion	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.sRegion. Example: 0
Bandwidth	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bandwidth. Example: 0
OldZoneVpcPeerFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldBZoneVpcPeer. Example: 0
OldOwedFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldOwedFlag. Example: 0
PublishDockerCidrFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bPublishDockerCidr. Example: 0
OldDestVpcSubnet	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldDVpcSubnet. Example: 10.0.0.0
LastState	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.lastState. Example: 0
SrcViewFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.sViewFlag. Example: 1
DestVpcSubnet	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.dVpcSubnet. Example: 10.0.0.0

name	required	NULL allowed	type	description
CreateTime	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.createTime. Example: 2021-12-31 19:41:49
OldDestExpireTime	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldDExpireTime. Example: 2021-12-31 19:41:49
SrcExpireTime	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.sExpireTime. Example: 2021-12-31 19:41:49
VpcPeerId	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.vpcPeerId. Example: 26574
Name	no	no	String	Name Example: DDDD
UniqueVpcPeerId	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.uniqVpcPeerId. Example: pcx-fh7xs34s
SrcVpcIntMask	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.sVpcIntMask. Example: 16
OldSrcViewFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldSViewFlag. Example: 1
DestExpireTime	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.dExpireTime. Example: 2021-12-31 19:41:49
DestOwner	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.dOwner. Example: 2511198225
Owner	no	no	String	User app ID Example: 2511198225
OldLocalBandwidth	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldLocalBandwidth. Example: 0
WanOutLimit	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.wanOutLimit. Example: 0
ZoneVpcPeerFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bZoneVpcPeer. Example: 0
NfvFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.bNfv. Example: 0
OldPublishDockerCidrFlag	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldBPublishDockerCidr. Example: 0
OldBandwidth	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.oldBandwidth. Example: 0
ImageId	no	no	String	Name of the original VPC OSS API (v2): UpdateVpcPeer.imageId. Example: xx
AfcVpcPeerGlobalId	no	no	Int64	Name of the original VPC OSS API (v2): UpdateVpcPeer.afcVpcPeerGlobalId. Example: 0

AddressTemplate

IP address template

Referenced by the following interfaces: CreateAddressTemplate, DescribeAddressTemplates

name	required	NULL allowed	type	description
AddressTemplateName	yes	no	String	IP address template name. Example: name
AddressTemplateId	yes	no	String	Unique ID of IP address template instance. Example: ipm-3x46d0c
AddressSet	yes	no	Array of String	IP address information. Example: ["2.2.2.2"]
CreatedTime	no	no	String	Creation time. Example: 2021-03-02 14:41:15

VpcOssGlobalRoute

Complex type: VpcOssGlobalRoute.

Referenced by the following interfaces: DescribeGlobalRouteInternal

name	required	NULL allowed	type	description
Subnet	no	no	String	Subnet address Example: 100.64.0.0
IntMask	no	no	Int64	Integer mask. Example: 24
Remote	no	no	String	Name of the original VPC OSS API (v2): GetGlobalRoute.remote. Example: 172.16.0.2
Master	no	no	String	Name of the original VPC OSS API (v2): GetGlobalRoute.master. Example: 16.5.3.6
VpcId	no	no	Int64	Integer VPCID. Example: 22

SellingModelTag

Available VPN Model Tags and Corresponding CPU Architecture List

Referenced by the following interfaces: DescribeVpnSellingModelTaglist

name	required	NULL allowed	type	description
CpuType	no	no	String	CPU Architecture Example: X86
VsModelTag	no	no	String	VS Model Tag Example: vs_vpn_intel

VpcOssRouteForDeleteRouteInternal

Complex type: VpcOssRouteForDeleteRouteInternal.

Referenced by the following interfaces: CreateRouteInternal, CreateServiceInternal, DeleteRouteInternal

name	required	NULL allowed	type	description
PrivateIp	no	no	String	Original VPC OSS APIv2 name: DelRoute.pip. Example: 10.19.0.121
ProtocolPort	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.pport. Example: 8080
Weight	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.weight. Example: 10
ZoneId	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.zoneId. Example: 50001
UdpOption	no	no	Int64	Original VPC OSS APIv2 name: DelRoute.udpOption. Example: 1
HostIp	no	no	String	Original VPC OSS APIv2 name: DelRoute.hostIp. Example: 1.1.1.1

LocalGateway

Local gateway information.

Referenced by the following interfaces: CreateLocalGateway, DescribeLocalGateway

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Local gateway creation time Example: 2021-03-24 15:31:56
CdcId	yes	no	String	CDC instance ID Example: cluster-gbo27yc4
VpcId	yes	no	String	VPC Instance ID Example: vpc-m0c2kcun
UniqLocalGwId	yes	no	String	Local gateway instance ID Example: lgw-jkt4wr1y
LocalGatewayName	yes	no	String	Local gateway name Example: demo
LocalGwIp	yes	no	String	Local gateway IP address Example: 192.168.15.55

DirectConnectGateway

Direct Connect gateway object.

Referenced by the following interfaces: CreateDirectConnectGateway, DescribeDirectConnectGateways

name	required	NULL allowed	type	description
DirectConnectGatewayId	yes	no	String	Direct Connect gateway ID . Example: dcg-e6mxyyvj
DirectConnectGatewayName	yes	no	String	Direct Connect gateway name. Example: demo
VpcId	yes	no	String	Direct Connect gateway association with VPC instance ID . Example: vpc-hm2okght
NetworkType	yes	no	String	Associated network type: • VPC - Virtual Private Cloud • CCN - Cloud Connect Network. Example: CCN
NetworkInstanceId	yes	no	String	Associated network instance ID : • When NetworkType is VPC , this is the VPC instance ID . • When NetworkType is CCN , this is the CCN instance ID . Example: ccn-4rukgymd
GatewayType	yes	no	String	Gateway type: • NORMAL - Standard type, note: CCN supports only the Standard type • NAT - NAT type NAT type supports network address translation configuration. Once the type is set, it cannot be changed. A VPC can create 1 NAT type Direct Connect gateway and 1 non-NAT type Direct Connect gateway. Example: NORMAL
CreateTime	yes	no	Datetime	Creation time. Example: 2020-02-01 12:00:00
DirectConnectGatewayIp	yes	no	String	Direct Connect gateway IP. Example: 10.212.253.59
CcnId	yes	no	String	Associated CCN instance ID of Direct Connect gateway. Example: ccn-4rukgymd
CcnRouteType	yes	no	String	CCN route learning type: • BGP - Automatic learning. • STATIC - Static, i.e., user configured. Example: BGP
EnableBGP	yes	no	Bool	Whether to enable BGP. Example: true
EnableBGPCommunity	no	no	Bool	Attribute of Community enabling and disabling the BGP. Example: false
Bandwidth	no	no	Int64	Direct Connect gateway bandwidth speed limit value. Example: 100

name	required	NULL allowed	type	description
ModeType	no	no	String	Whether it supports releasing to CCN. Example: standard
BGPCommunitySupport	no	no	Bool	Whether it supports BGP community attribute. Example: true
VXLANSupport	no	yes	Bool	Whether VXLAN is supported. Example: true
LocalZone	no	no	Bool	Whether it is a local region. Example: false
BGPSupport	no	no	Bool	Whether BGP is supported. Example: true
TagSet	no	no	Array of Tag	Tag Information Example:View
AliasType	no	yes	String	Alias type. Example: NORMAL
Ipv6Mode	no	no	Bool	Whether it is an IPv6 gateway. Example: true
FlowDetailsUpdateTime	no	yes	String	Update time for streaming log information. Example: 2021-07-08 14:47:49
AccessNetworkType	no	no	String	Backbone network type. Example: MPLS
FlowLogId	no	yes	String	Unique ID of Flow Log Example: fl-7zvyvr8d
DirectConnectGatewayVersion	no	yes	String	Direct Connect (DC) gateway version number. Example: V1
AliasInstanceId	no	yes	String	Alias instance ID of the DC gateway, which is used in conjunction with AliasType. Example: Sgcg-12345678
EnableFlowDetails	no	no	Int64	Whether to enable traffic statistics. Example: 0
NewAfc	no	no	Int64	Marks whether the new AFC architecture is used for the DC gateway. Example: 0

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
InvalidProjectId.NotFound	The project ID is invalid.

Error codes	Description
UnsupportedOperation.CIDRUnSupportedClassicLink	The specified VPC CIDR range does not support interconnection between the VPC and basic network devices.
UnsupportedOperation.VpcPeerInvalidStateChange	The peering connection status is abnormal.
UnsupportedOperation.RecordNotExists	
InvalidInstanceId.NotFound	Invalid instance ID. The specified instance ID does not exist.
InvalidParameterValue.VpnConnCidrConflict	The destination IP range conflicts with the CIDR of current VPN tunnel.
InternalServerError	Internal operation error.
UnsupportedOperation.LocalGatewayAlreadyExists	The specified CDC instance already has a local gateway.
InvalidParameter.InvalidPortType	Port Type Error
LimitExceeded.CidrBlock	The number of IP ranges allocated to the VPC has reached the upper limit.
UnsupportedOperation.UnableCrossFinance	The current CCN cannot be associated with Finance Cloud instances.
UnsupportedOperation.AttachmentAlreadyExists	
InternalError.ModuleError	
UnsupportedOperation.VersionMismatch	The specified security group rule version number is inconsistent with the latest version.
InvalidParameterValue.IpNotExists	It does not exist within the rules.
ResourceUnavailable	Resource unavailable

Error codes	Description
InvalidParameterValue.NatRuleNotExists	The Direct Connect gateway NAT rule does not exist.
UnsupportedOperation.MutexOperationTaskRunning	Exclusive operation task of resources is in progress.
InvalidParameterValue.SubnetRange	Invalid subnet CIDR.
UnsupportedOperation.NotMatchTargetService	
InvalidNetworkInterfaceId.NotFound	The specified NetworkInterfaceId does not exist or the specified PrivateIpAddress is not on the NetworkInterfaceId.
LimitExceeded.ActionLimited	
LimitExceeded.SubnetCidrBlock	The number of sub-IP range allocated to the sub-net has reached the upper limit.
InvalidParameterValue.ObjectUseInTrafficMirror	The traffic mirror collection object has already been used.
InvalidParameter.FilterValuesNotList	
UnsupportedOperation.AttachmentNotFound	The binding relationship does not exist.
UnsupportedOperation.UnassignCidrBlock	The IPv6 IP range is not allocated.
UnsupportedOperation.UinNotFound	The account ID does not exist.
UnsupportedOperation.InvalidState	The resource status is invalid.
InvalidVpnGatewayId.NotFound	Invalid VPN gateway. The VPN instance does not exist. Verify whether the resource information you entered is correct.
ResourceInsufficient.CidrBlock	The IP range resources are insufficient.

Error codes	Description
LimitExceeded.Address	The number of IP addresses allocated has reached the upper limit.
InvalidParameter.NextHopMismatch	The next hop type does not match it's gateway.
InvalidAccount.NotSupported	This account is not supported.
InvalidParameterValue.NetDetectSameIp	The probe destination IP is the same as that of another network probe within the same VPC and subnet.
InvalidParameterValue.CidrNotInPeerVpc	The destination IP range is not within the CIDR range of the peer VPC.
InvalidParameterValue.IpExists	It already exists in the rules.
MissingParameter	Missing parameters. The request did not carry the required parameter.
FailedOperation.NetDetectTimeOut	
InvalidParameterConflict	The specified two parameters conflict with each other and can not coexist. An EIP can only be bound to an instance or a specified private network IP of a designated network interface.
InvalidVpnGatewayId.Malformed	Invalid VPN gateway. VPN instance ID is invalid.
UnsupportedOperation.Ecmp	ECMP is not supported.
InvalidParameterValue.CcnAttachBmvpcLimitExceeded	The number of BM VPCs associated with the specified CCN has reached the upper limit.
InvalidSecurityGroupID.NotFound	Invalid security group. The security group instance ID does not exist.

Error codes	Description
LimitExceeded.PublicIpAddressPerNatGatewayLimitExceeded	The number of elastic IPs bound to the NAT gateway has exceeded the upper limit.
InvalidParameterValue.SubnetOverlapAssistCidr	
UnsupportedOperation.SubnetNotExists	
UnsupportedOperation.ResourceMismatch	
UnsupportedOperation.DirectConnectGatewayIsUpdatingCommunity	The Direct Connect gateway is updating the BGP Community attribute.
InvalidParameterValue.InVpcCidr	It cannot be within the VPC CIDR range.
InternalError	
LimitExceeded.JNSRulesExceeded	
UnsupportedOperation.PublicIpAddressIsNotBGPIp	The elastic IP address bound to NAT gateway is not an IP of BGP attribute.
UnsupportedOperation	Operation unsupported.
InvalidParameterValue.MirrorLackTargetResource	The private network bandwidth for the traffic mirror target is insufficient.
UnsupportedOperation.EcmpWithUserRoute	An ECMP is formed with the user-defined route.
UnauthorizedOperation.PrimaryIp	The primary IP does not support the specified operation.
InvalidParameterValue.Range	The parameter value is not within the specified range.
UnsupportedOperation.BindEIP	An EIP is already bound.
InvalidParameterValue.Malformed	Invalid input format.
InvalidParameterValue.Duplicate	Input Parameters are repetitive.

Error codes	Description
ResourceInsufficient	Insufficient resources
UnsupportedOperation.ClassicInstanceIdAlreadyExists	The instance is already bound to the VPC.
UnsupportedOperation.VpcPeerAlreadyExist	The peering connection already exists.
InvalidParameterValue.LimitExceeded	The parameter value exceeds the limit.
UnsupportedOperation.UnsupportedInstanceFamily	
InvalidParameterValue	The parameter value is invalid.
InvalidParameterValue.Empty	Missing parameter
InvalidParameterValue.NotInVpcCidr	It must be within the VPC CIDR range.
UnsupportedOperation.PublicIpAddressNotBilledByTraffic	The elastic IP bound to the NAT gateway is not charged by traffic.
LimitExceeded.NatGatewayPerVpcLimitExceeded	The number of NAT gateways created by VPC has exceeded the upper limit.
UnknownParameter	Unknown parameter error
UnsupportedOperation.ActionNotFound	The API does not exist.
InvalidParameterValue.NatRuleExists	Existed
UnsupportedOperation.CcnAttached	The instance is already associated with a CCN.
InvalidParameterValue.Reserved	The parameter value is a reserved object of the system.
UnsupportedOperation.SystemRoute	System route. The operation is prohibited.
InvalidParameterValue.SubnetConflict	There's a subnet CIDR conflict.
ResourceInUse.Address	The specified IP address is already in use.

Error codes	Description
InvalidAddressIdState.InArrears	The specified EIP is in arrears state.
InvalidParameter.Coexist	The parameters must not be specified simultaneously.
InvalidAddressId.Blocked	The designated EIP is in a blocked state. Binding operation cannot be performed while the EIP is blocked. Unbinding is required first.
InvalidParameterValue.ParameterMismatch	
InvalidParameterValue.NotNatVpg	It's not a NAT type Direct Connect gateway.
MissingResourceId	Missing bound entity. Either InstanceId, NetworkInterfaceId, or PrivateIpAddress must be specified.
UnsupportedOperation.ZoneMismatch	
VpcLimitExceeded	The application number of VPC resources in the specified region has reached the upper limit.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnauthorizedOperation.AttachmentNotFound	The binding relationship does not exist.
UnsupportedOperation.EcmpWithCcnRoute	An ECMP is formed with the route to CCN.
LimitExceeded	Exceeded the limit
UnsupportedOperation.EniHasSubEni	
InvalidAddressId.NotFound	The specified EIP does not exist.

Error codes	Description
UnsupportedOperation.UnableCrossBorder	Cross-border is not supported.
InvalidParameterValue.AclRuleExists	The Direct Connect gateway ACL rule already exists.
InvalidParameterValue.ObjectVpcNotCurrentVpc	The VPC collected by the traffic mirror is not the current VPCID.
UnauthorizedOperation	Unauthorized operation
UnsupportedOperation.DuplicatePolicy	Duplicate security group rules.
UnsupportedOperation.UnbindEIP	No EIP is bound.
InvalidParameterValue.VpgVpcNotMatch	The Direct Connect gateway does not exist or is not associated with the VPC.
InvalidInstanceId.AlreadyBindEip	The specified instance has already been bound with an EIP. The current EIP must be unbound before another binding operation can be performed.
InvalidAddressState	The current status of the specified EIP does not allow this operation.
UnsupportedOperation.VpcMismatch	The resources do not belong to the same VPC.
UnsupportedOperation.CcnNotAttached	The instance is not associated with a CCN.
UnknownParameter.WithGuess	This parameter cannot be recognized. Similar parameters can be used for replacement.
InvalidVpcId.Malformed	Invalid VPC. The VPC instance ID is invalid.

Error codes	Description
InvalidParameterValue.VpcCidrConflict	The destination IP range conflicts with the current VPC's CIDR.
ResourceInUse	Resources occupied
UnsupportedOperation.PublicIpAddressIsNotExisted	The elastic IP bound to the NAT gateway does not exist.
InvalidVpcId.NotFound	Invalid VPC. The VPC resource does not exist.
InvalidParameterValue.AclRuleNotExists	The Direct Connect gateway ACL rule does not exist.
InvalidSecurityGroupID.Malformed	Invalid security group. Invalid security group instance ID.
InvalidParameter.FilterInvalidKey	
UnsupportedOperation.AppIdMismatch	
UnsupportedOperation.InsufficientFunds	Insufficient account balance
AddressQuotaLimitExceeded	Insufficient account quota. Each account can create up to 20 EIPs in each region.
ResourceNotFound	The resource does not exist
InvalidPrivateIpAddress.AlreadyBindEip	The specified private IP of the specified ENI has already been bound to an EIP. It cannot be bound again.
UnsupportedOperation.ConflictWithDockerRoute	Overlaps with the IP range of a TKE container under this VPC.
InvalidInstance.NotSupported	The instance is not supported.
InvalidAddressIdStatus.NotPermit	The current status of the designated EIP does not allow for binding operation. Binding operation can only be performed when the EIP's status is UNBIND.

Error codes	Description
UnsupportedOperation.PublicIpAddressDisassociate	A NAT gateway must have at least one elastic IP, which cannot be unbound.
InvalidParameter	Invalid input parameters.
AddressQuotaLimitExceeded.DailyAllocate	Insufficient purchase attempts. The number of daily subscriptions for each account in each region is twice the quota.