云堡垒机

API 参考

文档版本 03

发布日期 2025-10-31

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 使用前必读

概述

欢迎使用云堡垒机（Cloud Bastion Host，CBH），云堡垒机是一款4A统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

调用说明

云堡垒机服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询服务的终端节点。

基本概念

- 账号

  用户注册时的账号，账号对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。由于账号是付费主体，为了确保账号安全，建议您不要直接使用账号进行日常管理工作，而是创建用户并使用他们进行日常管理工作。

- 用户

  由账号在IAM中创建的用户，是云服务的使用人员，具有身份凭证（密码和访问密钥）。

  通常在调用API的鉴权过程中，您需要用到账号、用户和密码等信息。

- 区域（Region）

  从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

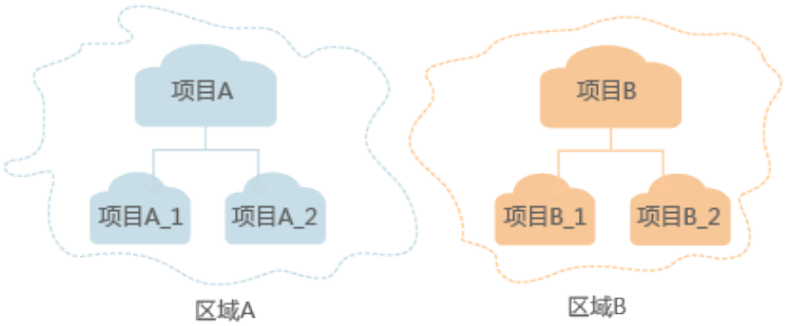
- 可用区（AZ，Availability Zone）

  一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

- 项目

  区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

  图 1-1 项目隔离模型



API 版本选择建议

CBH提供了V1和V2版本的API，供您使用。

建议使用V2版本API，V1版本API不再维护。

2 如何调用 API

2.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的获取用户Token说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

请求 URI

请求URI由如下部分组成。

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

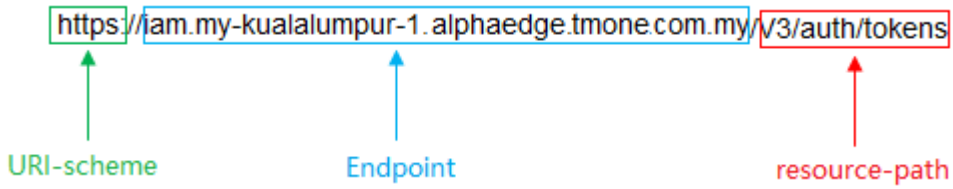
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme**：
  表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：
  指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**获取。
  例如IAM服务在“**my-kualalumpur-1**”区域的Endpoint为“**iam.my-kualalumpur-1.alphaedge.tmone.com.my**”。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **query-string**：
  查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“my-kualalumpur-1”区域的Token，则需使用“my-kualalumpur-1”区域的Endpoint（iam.my-kualalumpur-1.alphaedge.tmone.com.my），并在**地区和终端节点**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

图 2-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在获取用户Token的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用获取用户Token接口的响应值，该接口是唯一不需要认证的接口。

  说明

  API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

  AK/SK认证的详细说明请参见**AK/SK认证**。

对于获取用户Token接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于获取用户Token接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的账号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxxx***为project的名称，您可以从**地区和终端节点**获取。

说明

scope参数定义了Token的作用域，下面示例中获取的Token仅能访问project下的资源。您还可以设置Token作用域为某个账号下所有资源或账号的某个project下的资源，详细定义请参见获取用户Token。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

2.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

Token 认证

说明

Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

Token可通过调用获取用户Token接口获取，调用本服务API需要project级别的Token，即调用获取用户Token接口时，请求body中auth.scope的取值需要选择project，如下所示。

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFG....”，则调用接口时将“X-Auth-Token: ABCDEFG....”加到请求消息头即可，如下所示。

```
GET https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

AK/SK 认证

说明

AK/SK签名认证方式仅支持消息体大小12MB以内，12MB以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见**API签名指南**。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

2.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于获取用户Token接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于获取用户Token接口，返回如**图2-2**所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 2-2 获取用户 Token 响应消息头

响应消息体（可选）

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于获取用户Token接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
```

```
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
.....
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

3 API 说明

3.1 云堡垒机信息查询

3.1.1 获取 CBH 实例列表

功能介绍

获取当前租户下的云堡垒机实例列表。

URI

GET /v1/{project_id}/cbs/instance/list

表 3-1 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID。

请求参数

无

响应参数

状态码： 200

表 3-2 响应 Body 参数

参数	参数类型	描述
total	Integer	云堡垒机实例总数。

参数	参数类型	描述
quotaDetail	**QuotaDetail** object	当前用户云堡垒机的配额信息。返回默认值null。
instance	Array of **InstanceDetail** objects	云堡垒机实例列表信息。

表 3-3 QuotaDetail

参数	参数类型	描述
zh_cn	String	中文配额描述。
en_us	String	英文配额描述。
remaining	Integer	租户剩余配额数量。

表 3-4 InstanceDetail

参数	参数类型	描述
publicip	String	云堡垒机实例弹性公网IP，返回默认值null
expTime	String	云堡垒机实例过期时间。
startTime	String	云堡垒机实例开始时间，使用时间戳格式表示。
endTime	String	云堡垒机实例结束时间，使用时间戳格式表示。
releaseTime	String	云堡垒机释放时间，使用时间戳格式表示。
name	String	云堡垒机实例名称。
instanceId	String	云堡垒机实例ID，UUID格式。
privateIp	String	云堡垒机实例私有ip。

参数	参数类型	描述
taskStatus	String	云堡垒机实例当前的任务状态。 ● powering-on 开启 ● powering-off 关闭 ● rebooting 重启 ● delete_wait 删除 ● frozen 冻结 ● NO_TASK 运行 ● unfrozen 解冻 ● alter 变更 ● updating 升级中 ● configuring-ha 配置HA
status	String	云堡垒机实例状态。 ● SHUTOFF 已关闭 ● ACTIVE 运行中 ● DELETING 删除中 ● BUILD 创建中 ● DELETED 已删除 ● ERROR 故障 ● HAWAIT 等待备机创建成功 ● FROZEN 已冻结 ● UPGRADING 升级中 ● UNPAID 待支付 ● RESIZE 规格变更中 ● DILATATION 扩容中 ● HA 配置HA中
created	String	云堡垒机实例创建时间，使用UTC时间表示。
region	String	云堡垒机实例所在局点。
zone	String	云堡垒机实例所在可用区。
availability_zone_display	String	云堡垒机实例所在可用区中文名称。
vpcId	String	云堡垒机实例所在虚拟私有云的VPC ID。
subnetId	String	云堡垒机实例所在子网的ID。
securityGroupId	String	云堡垒机实例所属的安全组的ID。

参数	参数类型	描述
specification	String	云堡垒机实例规格。
update	String	云堡垒机实例是否可以升级。 ● NEW，可以升级 ● OLD，不能升级
createinstanceStatus	String	云堡垒机实例在创建实例过程中的过程状态信息。 ● Waiting for payment，等待支付 ● creating-network，创建网络 ● creating-server，创建服务 ● tranfering-horizontal-network，网络打通 ● adding-policy-route，添加路由策略 ● configing-dns，配置DNS ● starting-cbs-service，服务运行中 ● setting-init-conf，初始化 ● buying-EIP，购买弹性公网IP
failReason	String	云堡垒机实例创建实例失败原因。
instanceKey	String	云堡垒机实例key。
orderId	String	订单ID。
periodNum	String	云堡垒机实例订购周期数。
resourceId	String	云堡垒机实例的资源id,UUID格式显示。
bastion_type	String	云堡垒机实例堡垒机类型。 ● OEM
alterPermit	String	云堡垒机实例是否可以扩容。 ● 1 开启扩容 ● 0 关闭扩容
publicId	String	云堡垒机实例绑定公网的弹性IP的ID，UUID格式表示。
bastionVersion	String	云堡垒机实例当前版本。
newBastionVersion	String	云堡垒机实例可以升级的版本。

参数	参数类型	描述
instanceStatus	String	云堡垒机实例状态。 ● building 创建中 ● deleting 删除中 ● deleted 删除了 ● unpaid 未支付 ● upgrading 升级中 ● resizing 扩容中 ● abnormal 异常 ● error 故障 ● ok 正常
instanceDescription	String	云堡垒机实例状态描述。
slaveZone	String	备可用分区，默认返回null。
enterpriseProjectId	String	云堡垒机实例所属企业项目ID。
instanceType	String	云堡垒机实例类型。 ● null 单机默认返回null ● master HA时返回主机 ● slave HA时返回备机
haId	String	云堡垒机实例主备ID。 ● 单机堡垒机实例默认返回null ● HA堡垒机实例返回主机HAID
slaveZoneDisplay	String	云堡垒机实例备机可用分区名称。 单机堡垒机实例和备机堡垒机实例返回null，HA堡垒机实例主机返回备机所在可用区名称。
webPort	String	云堡垒机实例WEB界面访问的端口号。
vip	String	云堡垒机实例浮动ip。返回默认值null

状态码： 400

表 3-5 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_description	String	请求参数错误。

状态码： 401

表 3-6 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_description	String	校验TOKEN失败。

状态码： 403

表 3-7 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_description	String	租户无权限操作。

状态码： 404

表 3-8 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_description	String	没有找到CBH资源。

请求示例

无

响应示例

状态码： 200

查询云堡垒机实例列表信息成功。


```
{
  "total" : 1,
  "quotaDetail" : "null",
  "instance" : [ {
    "publicip" : "null",
    "expTime" : "14",
    "startTime" : "1669911490000",
    "endTime" : "1672675199000",
    "releaseTime" : "1675267199000",
```

```
    "name" : "CBH-8a80",
    "instanceId" : "f7854c8d-9bbc-4970-8b7d-6ed8280f6bfe",
    "privateIp" : "192.168.0.67",
    "status" : "SHUTOFF",
    "taskStatus" : "NO_TASK",
    "created" : "2022-12-02 00:04:42.0",
    "region" : "cn-north-4",
    "zone" : "cn-north-4c",
    "availability_zone_display" : "可用区3",
    "vpcId" : "279e8217-4a8a-4d83-8fd9-b8f14d47170b",
    "subnetId" : "a86217e6-a96d-4803-ae5c-b57da6811249",
    "securityGroupId" : "c5564ac2-bdcf-4e45-b892-92c2ae79ecd9",
    "specification" : "cbh.basic.50",
    "update" : "OLD",
    "createinstanceStatus" : "starting-cbs-service",
    "failReason" : "No FailReason Now",
    "instanceKey" : "6771",
    "orderId" : "CS22120200031TOLA",
    "periodNum" : "1,2",
    "resourceId" : "01903dfb-11fc-4ae4-8bff-bca51d11ad92",
    "bastion_type" : "OEM",
    "publicId" : "",
    "alterPermit" : "1",
    "bastionVersion" : "3.3.41.0",
    "newBastionVersion" : "3.3.40.1",
    "instanceStatus" : "error",
    "instanceDescription" : "LoadBalance service error!,2022-12-19 17:14:30,{\"d_usage\":\"0.80\",\"m_usage
\":\"30.04\",\"c_usage\":\"0.62\",\"session_count\":\"0\"",
    "webPort" : "443",
    "enterpriseProjectId" : "0",
    "vip" : null,
    "slaveZone" : null,
    "slaveZoneDisplay" : null,
    "haId" : null,
    "instanceType" : null
  } ]
}
```


状态码

状态码	描述
200	查询云堡垒机实例列表信息成功。
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found

错误码

请参见**错误码**。

A 附录

A.1 状态码

状态码	编码	状态说明
200	OK	请求成功。
400	Bad Request	请求失败。 建议直接修改该请求，不要重试该请求。
401	Unauthorized	请求认证失败。 表明服务端指出客户端所提供的认证信息不正确或非法。
403	Forbidden	请求被拒绝访问。 返回该状态码，表明请求能够到达服务端，且服务端能够理解用户请求，但是拒绝做更多的事情，因为该请求被设置为拒绝访问，建议直接修改该请求，不要重试该请求。
404	NotFound	所请求的资源不存在。 建议直接修改该请求，不要重试该请求。
500	InternalServerError	表明服务端能被请求访问到，但是不能理解用户的请求。

A.2 错误码

状态码	错误码	错误信息	描述	处理措施
400	CBH.10020009	请求消息格式非法	请求消息格式非法	请求消息格式非法

状态码	错误码	错误信息	描述	处理措施
400	CBH.10020010	Request message param error.	请求消息体参数错误！	请核对您的请求参数。
400	CBH.10020011	serverId错误	serverId错误	serverId错误
401	CBH.10020100	The IAM token is invalid.	无法通过IAM校验！	请核对您的token是否正确。
403	CBH.10020002	Tenant has no authority.	租户无权限！	该租户无权限，请去IAM确认用户权限。
500	CBH.10020000	Unknown error！	未知错误！	未知错误，请联系技术人员处理。

A.3 获取项目 ID

操作场景

在调用接口的时候，部分URL中需要填入项目ID，所以需要获取到项目ID。有如下两种获取方式：

- **调用API获取项目ID**
- **从控制台获取项目ID**

调用 API 获取项目 ID

项目ID可以通过调用IAM服务的“查询指定条件下的项目信息”API获取。

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从**地区和终端节点**获取。接口的认证鉴权请参见**认证鉴权**。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
```

```
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目ID，所以需要获取到项目ID。项目ID获取步骤如下：

1. 登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的凭证”。

   在“我的凭证”页面的项目列表中查看项目ID。

B 修订记录

发布日期	修改说明
2025-10-31	第三次正式发布。 优化使用前必读章节。
2025-01-26	第二次正式发布。 修改获取CBH实例列表接口的URI信息。
2023-10-30	第一次正式发布。