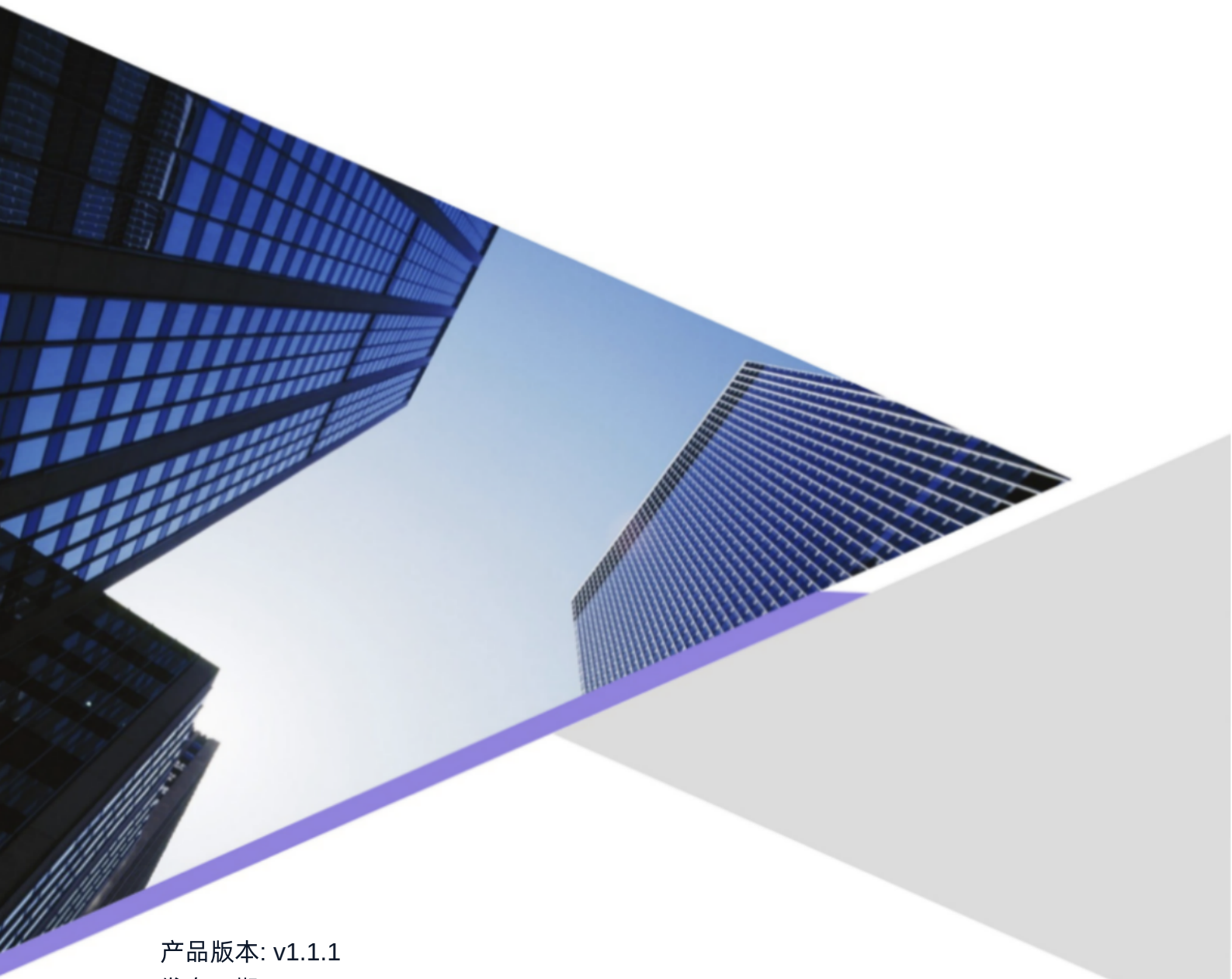
易捷行云
EasyStack

证书与密钥服务

API参考



产品版本: v1.1.1
发布日期: 2023-06-20

目录

1 API参考

1.1 API简介

欢迎使用API文档，如果您熟悉CA以及证书体系和一种以上编程语言，推荐您调用API管理您的资源和开发自己的应用程序。 本文档提供了API的描述、语法、参数说明及示例等内容。在调用API之前，请确保已经充分了解相关术语，详细信息请参见下表。

术语	说明
CA	证书授权中心（Certificate Authority）或称证书授权机构。
证书	证书又称终端实体证书，安装在终端实体上的证书，含客户端证书（应用于客户端）、服务器证书（应用于服务器）等。承担实体的身份验证的作用，不可用于签发证书，属于证书链中的最后一层，是拥有该证书的实体与其它实体进行HTTPS通信的凭证。
证书链	从根CA到终端实体证书之间的完整的证书链路，即各个层级证书按序链在一起的文件，用于进行身份的逐层校验。
HTTPS	HTTPS也就是HTTP+SSL，基于SSL协议的网站加密传输协议，是HTTP的安全版。

1.2 调用方式

请求结构

API支持基于URI发起HTTP/HTTPS GET请求。请求参数需要包含在URI中。本文列举了GET请求中的结构解释，并以云主机的服务接入地址为例进行了说明。

结构示例

以下为一条未编码的URI请求示例： `http://cloud.com/v1/{project_id}/servers` 在本示例中：

- `http` 指定了请求通信协议
- `cloud.com` 指定了服务接入地址
- `/v1/{project_id}/servers` 为资源路径，也即API访问路径

通信协议

支持HTTP或HTTPS协议请求通信。为了获得更高的安全性，推荐您使用HTTPS协议发送请求。涉及敏感数据时，如用户密码和SSH密钥对，推荐使用HTTPS协议。

服务网址

调用本文档所列举的API时均需使用OpenStack身份服务进行身份验证。 他们还需要一个从“compute”类型的标识符提取出来的“service URI”。 这将是根URI，将添加下面的每个调用来构建一个完整的路径。例如，如果“service URI”是 `http://mycompute.pvt/compute/v2.1` ，那么“/servers”的完整API调用是 `http://mycompute.pvt/compute/v2.1/servers` 。 根据部署计算服务网址可能是http或https，自定义端口，自定义路径，并包含您的租户ID。 要知道您的部署网址的唯一方法是通过使用服务目录。计算URI不应该被硬编码在应用程序中，即使他们只希望在单一地点工作。应始终从身份令牌中发现。因此，对于本文件的其余部分，我们将使用短针，其中"GET /servers"的真正含义"GET your_compute_service_URI/servers"。

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。

方法	说明

方法	说明
GET	从服务端读取指定资源的所有信息，包括数据内容和元数据（Metadata）信息，其中元数据在响应头（Response Header）中返回，数据内容在响应体（Response Body）中。
PUT	向指定的资源上传数据内容和元数据信息。如果资源已经存在，那么新上传的数据将覆盖之前的内容。
POST	向指定的资源上传数据内容。与PUT操作相比，POST的主要区别在于POST一般用来向原有的资源添加信息，而不是替换原有的内容：POST所指的资源一般是处理请求的服务，或是能够处理多块数据。
DELETE	请求服务器删除指定资源，如删除对象等。
HEAD	仅从服务端读取指定资源的元数据信息。

字符编码

请求及返回结果都使用UTF-8字符集编码。

公共参数

公共参数是用于标识用户和接口签名的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

公共请求参数

名称	类型	是否必选	描述
Host	String	否（使用AK/SK认证时该字段必选）	请求的服务器信息，从服务API的URI中获取。值为hostname[:port]。端口缺省时使用默认的端口，https的默认端口为443。

名称	类型	是否必选	描述
Content-Type	String	是	消息体的类型（格式）。推荐用户使用默认值application/json，有其他取值时会在具体接口中专门说明。
Content-Length	String	否	请求body长度，单位为Byte。
X-Project-Id	String	否	project id，项目编号。
X-Auth-Token	String	否（使用Token认证时该字段必选）	用户Token。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。请求响应成功后在响应消息头（Headers）中包含的“X-Subject-Token”的值即为Token值。

公共返回参数

参数名称	参数类型	描述
RequestId	String	请求ID。无论调用接口成功与否，都会返回该参数。

签名机制

调用接口的认证方式为Token认证，通过Token认证通用请求。 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": {
        "scope": {
            "project": {
                "domain": {
                    "name": "Default"
```

```
                },
                "name": "admin"
            }
        },
        "identity": {
            "password": {
                "user": {
                    "password": "devstacker",
                    "id": "858634b407e845f14b02bcf369225dcd0"
                }
            },
            "methods": ["password"]
        }
    }
}
```

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“ABCDEFJ....”，则调用接口时将 `X-Auth-Token: ABCDEFJ....` 加到请求消息头即可，如下所示:

```
POST https://iam.cn-north-1.mycloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

返回结果

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。 为了便于查看和美观，API 文档返回示例均有换行和缩进等处理，实际返回结果无换行和缩进处理。

正确返回结果

接口调用成功后会返回接口返回参数和请求 ID，我们称这样的返回为正常返回。HTTP 状态码为 2xx。 以云主机的接口创建云主机 `(POST /v1/{project_id}/servers)` 为例，若调用成功，其可能的返回如下:

```
{
    "error": {
        "OS-DCF:diskConfig": "AUTO",
        "adminPass": "6NpUwoz2QDRN",
```

```
        "id": "f5dc173b-6804-445a-a6d8-c705dad5b5eb",
        "links": [
            {
                "href":
"http://openstack.example.com/v2/6f70656e737461636b20342065766572/servers/f5
dc173b-6804-445a-a6d8-c705dad5b5eb",
                "rel": "self"
            },
            {
                "href":
"http://openstack.example.com/6f70656e737461636b20342065766572/servers/f5dc1
73b-6804-445a-a6d8-c705dad5b5eb",
                "rel": "bookmark"
            }
        ],
        "security_groups": [
            {
                "name": "default"
            }
        ]
    }
}
```


错误返回结果

接口调用出错后，会返回错误码、错误信息和请求 ID，我们称这样的返回为异常返回。HTTP 状态码为 4xx 或者 5xx。


```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "code": 401,
        "title": "Unauthorized"
    }
}
```


公共错误码

http状态码	Error Message	说明
300	multiple choices	被请求的资源存在多个可供选择的响应。
400	Bad Request	服务器未能处理请求。
401	Unauthorized	被请求的页面需要用户名和密码。
403	Forbidden	对被请求页面的访问被禁止。
404	Not Found	服务器无法找到被请求的页面。
405	Method Not Allowed	请求中指定的方法不被允许。
406	Not Acceptable	服务器生成的响应无法被客户端所接受。
407	Proxy Authentication Required	用户必须首先使用代理服务器进行验证，这样请求才会被处理。
408	Request Timeout	请求超出了服务器的等待时间。
409	Conflict	由于冲突，请求无法被完成。
500	Internal Server Error	请求未完成。服务异常。
501	Not Implemented	请求未完成。服务器不支持所请求的功能。
502	Bad Gateway	请求未完成。服务器从上游服务器收到一个无效的响应。
503	Service Unavailable	请求未完成。系统暂时异常。
504	Gateway Timeout	网关超时。

1.3 证书管理

证书管理

列举证书

功能介绍

获取证书列表。

URI

`GET /v1/secrets`

请求消息

参数	参数类型	是否必选	描述
show_all	string	否	值为 `True` 时，返回所有项目下的证书资源；值为 `False` 时，返回当前项目下的证书资源。该参数仅在云管理员身份下有效。
show_expired	string	否	值为 `True` 时，返回的证书列表中将包含已经过期的证书。默认只返回未过期的证书。
show_cert_secrets_only	string	否	值为 `True` 时，仅返回证书类型的Secret资源。默认将返回所有类型的Secret资源。
use_es_deleted	string	否	值为 `True` 时，代表使用 `es_deleted` 字段标记证书是否被删除，防止负载均衡监听器引用已被删除的证书时报错。

参数	参数类型	是否必选	描述
cert_use_type	integer	否	值为 `1` 时，仅返回服务端证书；值为 `2` 时，仅返回客户端证书；默认返回所有类型的证书。
key_algorithm	integer	否	值为 `1` 时，仅返回 `RSA` 密钥算法类型的证书；值为 `2` 时，仅返回 `ECC` 密钥算法类型的证书；值为 `3` 时，仅返回国密SM2算法类型的证书；默认返回所有算法类型的证书。
limit	integer	否	返回的证书列表数据条数，默认返回10条数据，最大支持100条数据。
offset	integer	否	获取证书数据时的起始索引位置，即偏移量。一般结合 `limit` 参数一起使用。

响应消息

参数	参数类型	描述
name	string	Secret 资源名称，在证书服务中代表证书名称。
status	string	Secret 资源状态，证书服务中未使用此字段。
created	string	证书 Secret 创建时间。
updated	string	证书 Secret 更新时间。
secret_type	string	Secret 资源类型，证书服务中未使用此字段。
expiration	string	证书过期时间。
algorithm	string	Secret 资源加密算法类型，证书服务中未使用此字段。
bit_length	integer	Secret 资源加密算法位数，证书服务中未使用此字段。
mode	string	Secret 资源加密模式，证书服务中未使用此字段。

参数	参数类型	描述
creator_id	uuid	创建证书的用户ID。
es_dns	string	证书所绑定的域名信息。
es_cert_type	integer	证书状态， `1` 代表 `已签发` ； `2` 代表 `已托管` ； `3` 代表 `其他` ，用于标记非证书Secret资源； `4` 代表 `已吊销` 。
es_project_id	uuid	当前证书所处的项目ID。
es_domain_id	uuid	当前证书所处的部门ID。
es_issuer_ca_id	uuid	签发证书的私有CA的ID。
es_deleted	boolean	证书是否已删除。
es_cert_use_type	integer	证书类型， `1` 代表服务端证书， `2` 代表客户端证书。
es_key_algorithm	integer	证书密钥算法类型， `1` 代表RSA密钥算法， `2` 代表ECC密钥算法， `3` 代表国密SM2算法。
content_types	object	Secret对应的Payload内容格式类型。
secret_ref	string	证书资源对应的Secret引用，包含Secret ID。

请求示例

```
curl -X GET -H "X-Auth-Token: "
http://barbican.barbican.svc.cluster.local/v1/secrets?
show_all=True&show_cert_secrets_only=True&cert_use_type=1&use_es_deleted=Tru
e&key_algorithm=1
```

正常响应示例

```
{
    "secrets": [
        {
```

```
            "created": "2023-03-27T12:12:40",
            "updated": "2023-03-27T12:12:40",
            "status": "ACTIVE",
            "name": "server-cert-test",
            "secret_type": "opaque",
            "expiration": "2024-03-26T12:12:40",
            "algorithm": null,
            "bit_length": null,
            "mode": null,
            "creator_id": "bc138a94c9644c9da4a3093f20e29890",
            "es_dns": "www.server-cert.com",
            "es_cert_type": 1,
            "es_project_id": "d0599a61793943fba9278165e51e7d52",
            "es_domain_id": "default",
            "es_issuer_ca_id": "65ddc0d1-2793-4bf2-abbb-3eff4e02e26e",
            "es_deleted": false,
            "es_cert_use_type": 1,
            "es_key_algorithm": 1,
            "content_types": {
                "default": "application/octet-stream"
            },
            "secret_ref": "http://barbican-
api.barbican.svc.cluster.local:9311/v1/secrets/5715c3dd-d32c-4edd-9fd1-
5baeb6a8467b"
        }
    ],
    "total": 1
}
```


正常响应代码

200

错误码

400，401，500

注意点

> **独享型负载均衡服务**对接需注意：

- 目前，独享型负载均衡服务创建HTTPS类型的负载均衡监听器时，仅支持 `RSA` 密钥算法类型的服务端证书。因此在创建HTTPS类型的负载均衡监听器获取证书列表时，需要携带以下参数 `show_cert_secrets_only=True&cert_use_type=1&use_es_deleted=True&key_algorithm=1` ；
- 获取证书列表最多只能返回100条数据，如需获取所有证书数据，可通过 `offset` 和 `limit` 参数进行遍历，最后一次遍历返回的数据条数小于 `limit` 参数的值，则证明证书数据已全部取出。

日期	修订内容

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)