

ACL API参考

备注

仅当Barbican用于经过验证的管道（即与Keystone集成）时，此功能才适用。

备注

当前为容器定义的访问控制列表（ACL）并不会向下传播到容器中的机密。

机密 ACL API

GET /v1/secrets/{uuid}/acl

检索给定机密的ACL设置。

如果机密没有设置ACL，则返回默认的ACL。

请求/响应（定义了ACL）

Request:

GET /v1/secrets/{uuid}/acl

Headers:

X-Auth-Token: {token_id}

Response:

HTTP/1.1 200 OK

```
{
  "read": {
    "updated": "2015-05-12T20:08:47.644264",
    "created": "2015-05-12T19:23:44.019168",
    "users": [
      {user_id1},
      {user_id2},
      .....
    ],
    "project-access": {project-access-flag}
  }
}
```

请求/响应（未定义ACL）

Request:

GET /v1/secrets/{uuid}/acl

```

Headers:
  X-Auth-Token: {token_id}

Response:

HTTP/1.1 200 OK
{
  "read":{
    "project-access": true
  }
}

```

HTTP状态码

code	说明
200	成功更
401	缺失或无效的X-Auth-Token。要求认证
403	用户无权访问该资源。
404	Secrets未找到给定的UUID。

PUT /v1/secrets/{uuid}/acl

为指定的机密创建一个新的ACL或替换已有的ACL。

此调用用来为机密添加新的ACL。如果机密已经设置的ACL，此方法将使用请求的ACL进行替换。在创建或替换已有ACL，都会返回200。如果要从一个ACL定义中删除已存在的用户，为用户传空列表即可。

成功返回ACL引用。

属性

此页面中详述的ACL资源允许访问受控的个人机密。通过对这些机密的操作可以配置此访问。当前仅支持‘read’操作（包括 GET REST操作）。

属性名称	类型	说明	默认值
read	parent element	ACL数据读操作	None
users	[string]	(可选项)用户id列表。需要的是Keystone返回的用户id	[]
project-access	boolean	标记机密是否为私有，这样创建者和ALC列表中的用户就只能访问此机密。false标识私有。	true

请求/响应（设置或者替换ACL）

Request:

```
PUT /v1/secrets/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":{
    "users":[
      {user_id1},
      {user_id2},
      .....
    ],
    "project-access":{project-access-flag}
  }
}

Response:

HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/secrets/{uuid}/acl"}
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID
415	不支持的媒体类型

PATCH /v1/secrets/{uuid}/acl

更新给定机密的现有ACL。此方法用来部分更新现有的ACL设置。客户端可以更新~~用户~~列表，启用或者禁用现有ACL的~~项目访问~~。提供的用户列表将替换现有的用户（如果存在的话）。如果从ACL定义中提供用户的现有列表，传[]即可。

成功返回ACL引用。

属性

属性名称	类型	说明	默认值
read	parent element	ACL数据读操作	无

属性名称	类型	说明	默认值
users	[string]	(可选项)用户id列表。需要的是Keystone返回的用户id	无
project-access	boolean	标记机密是否为私有，这样创建者和ALC列表中的用户就只能访问此机密。false标识私有。	无

请求/响应（更新项目访问标识）

```

PATCH /v1/secrets/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":
  {
    "project-access": false
  }
}

Response:
HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/secrets/{uuid}/acl"}

```

请求/响应（从ACL中移除所有用户）

```

PATCH /v1/secrets/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":
  {
    "users": []
  }
}

Response:
HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/secrets/{uuid}/acl"}

```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID
415	不支持的媒体类型

DELETE /v1/secrets/{uuid}/acl

删除给定机密的ACL。如果成功删除，没有内容返回。

请求/响应

```
DELETE /v1/secrets/{uuid}/acl
Headers:
  X-Auth-Token: {token_id}

Response:
HTTP/1.1 200 OK
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID

容器 ACL API

GET /v1/containers/{uuid}/acl

检索给定容器的ACL设置。
如果容器没有设置ACL，则返回默认的ACL。

请求/响应（有ACL定义）

Request:

```
GET /v1/containers/{uuid}/acl
```

Headers:

```
X-Auth-Token: {token_id}
```

Response:

```
HTTP/1.1 200 OK
```

```
{
  "read":{
    "updated":"2015-05-12T20:08:47.644264",
    "created":"2015-05-12T19:23:44.019168",
    "users":[
      {user_id1},
      {user_id2},
      .....
    ],
    "project-access":{project-access-flag}
  }
}
```

请求/响应（未定义ACL）

Request:

```
GET /v1/containers/{uuid}/acl
```

Headers:

```
X-Auth-Token: {token_id}
```

Response:

```
HTTP/1.1 200 OK
```

```
{
  "read":{
    "project-access": true
  }
}
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源

code	说明
404	未找到给定的UUID

PUT /v1/containers/{uuid}/acl

为指定的容器创建一个新的ACL或替换已有的ACL。

此调用用来为容器添加新的ACL。如果容器已经设置的ACL，此方法将使用请求的ACL进行替换。在创建或替换已有ACL，都会返回200。如果要从一个ACL定义中删除已存在的用户，为用户传空列表即可。

成功返回ACL引用。

属性

属性名称	类型	说明	默认值
read	parent element	ACL数据读操作	无
users	[string]	(可选项)用户id列表。需要的是Keystone返回的用户id	[]
project-access	boolean	标记机密是否为私有，这样创建者和ALC列表中的用户就只能访问此机密。false标识私有。	true

请求/响应（设置或更新ACL）

```
PUT /v1/containers/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":{
    "users":[
      {user_id1},
      {user_id2},
      .....
    ],
    "project-access":{project-access-flag}
  }
}

Response:
HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/containers/{uuid}/acl"}
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID
415	不支持的媒体类型

PATCH /v1/containers/{uuid}/acl

更新给定容器的现有ACL。此方法用来部分更新现有的ACL设置。客户端可以更新用户列表，启用或者禁用现有ACL的 **项目访问**。提供的用户列表将替换现有的用户（如果存在的话）。如果从ACL定义中提供用户的现有列表，传[]即可。

成功返回ACL引用。

属性

属性名称	类型	说明	默认值
read	parent element	ACL数据读操作	无
users	[string]	(可选项)用户id列表。需要的是Keystone返回的用户id	无
project-access	boolean	标记机密是否为私有，这样创建者和ALC列表中的用户就只能访问此机密。false标识私有。	无

请求/响应（更新项目访问标识）

```
PATCH /v1/containers/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":
  {
    "project-access": false
  }
}

Response:
HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/containers/{uuid}/acl"}
```


请求/响应（从ACL中移除所有用户）

```
PATCH /v1/containers/{uuid}/acl
Headers:
  Content-Type: application/json
  X-Auth-Token: {token_id}

Body:
{
  "read":
  {
    "users": []
  }
}

Response:
HTTP/1.1 200 OK
{"acl_ref": "https://{barbican_host}/v1/containers/{uuid}/acl"}
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID
415	不支持的媒体类型

DELETE /v1/containers/{uuid}/acl

删除给定容器的ACL。如果成功删除，没有内容返回。

请求/响应

```
DELETE /v1/containers/{uuid}/acl
Headers:
  X-Auth-Token: {token_id}

Response:
HTTP/1.1 200 OK
```

HTTP状态码

code	说明
200	成功创建或者替换
400	错误的请求
401	遗失或者无效的X-Auth-Token。要求认证
403	用户无权访问此资源
404	未找到给定的UUID