## Test case EG-TST-SEC-CP-1-1

#### 测试说明：

所有用于跨网络传输的机器对机器和人对机器接口都必须具有访问认证机制，并且认证过程必须在服务器上执行。 **注意**：跨网络接口必须支持身份验证，以防止欺骗

### Mecm:

#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

直接curl， 需要认证，没有认证会请求失败

##### 测试结果：通过

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)

未加认证， 接口调用返回未认证错误。

##### 测试结果：通过

## Test case EG-TST-SEC-CP-1-3

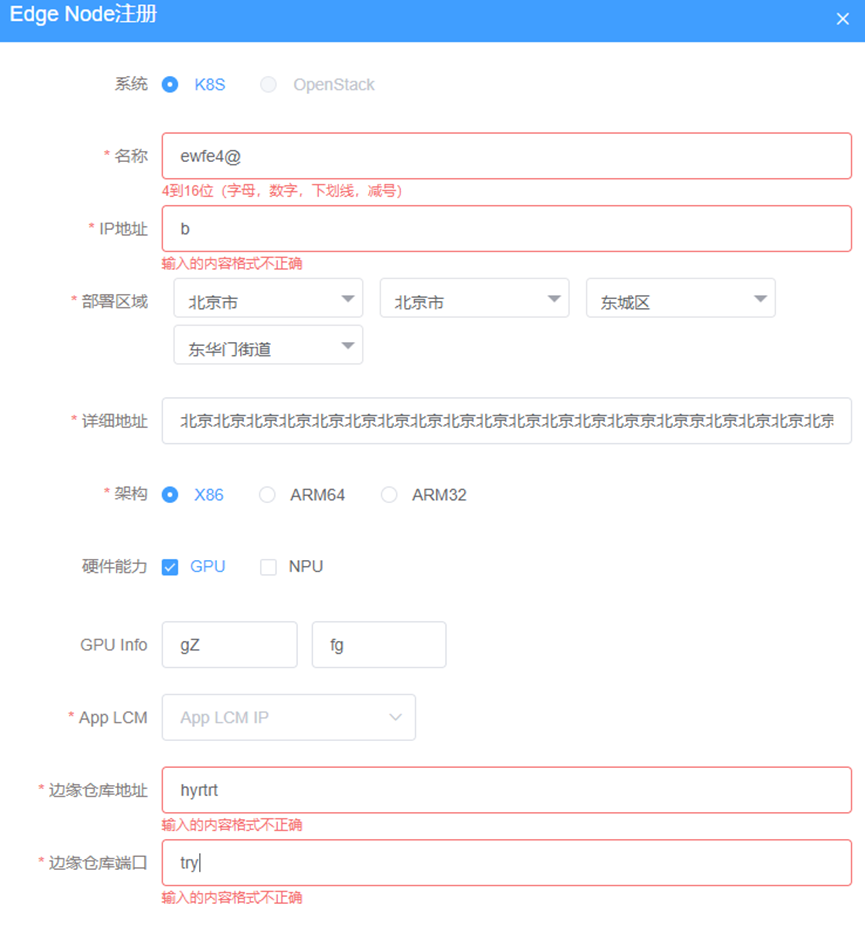
#### 测试说明：

服务器必须验证所有不受信任的数据源的大小，类型，长度和特殊字符，并拒绝所有未通过验证的数据

### Mecm:

#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)





##### 测试结果：通过

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

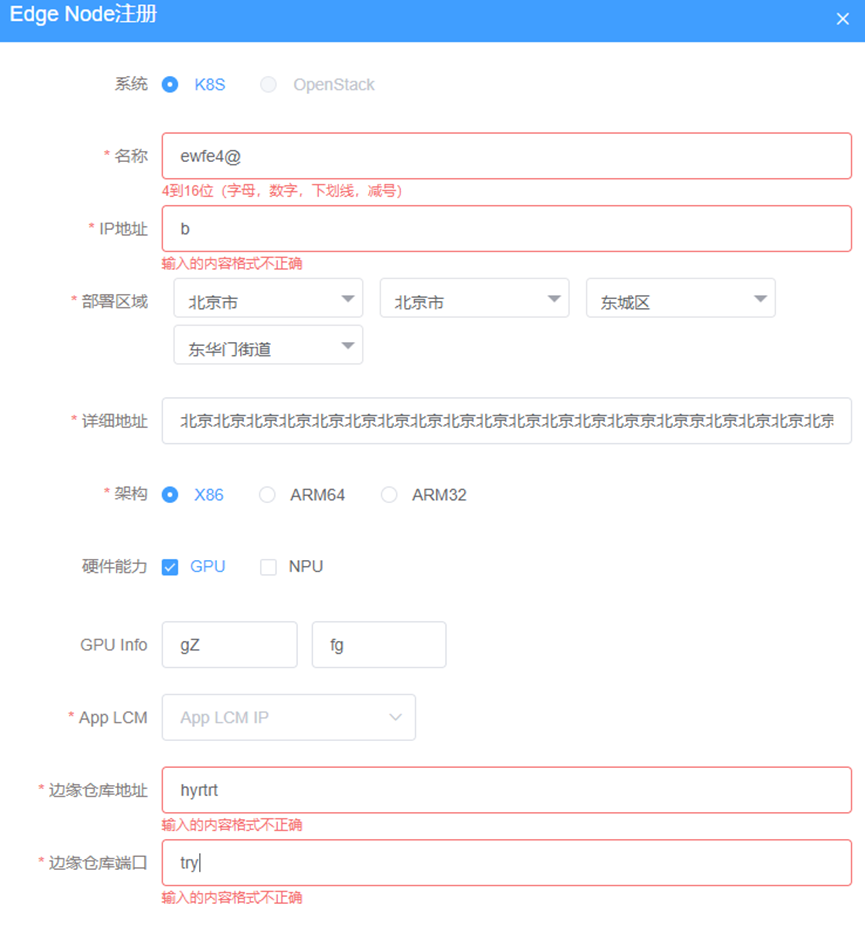
无效的token，长度不符合规定的token 认证失败。

输入不存在的hostIp, 依然可以查询到capability.

##### 测试结果：不通过

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)





##### 测试结果：通过

## Test case EG-TST-SEC-CP-2-1

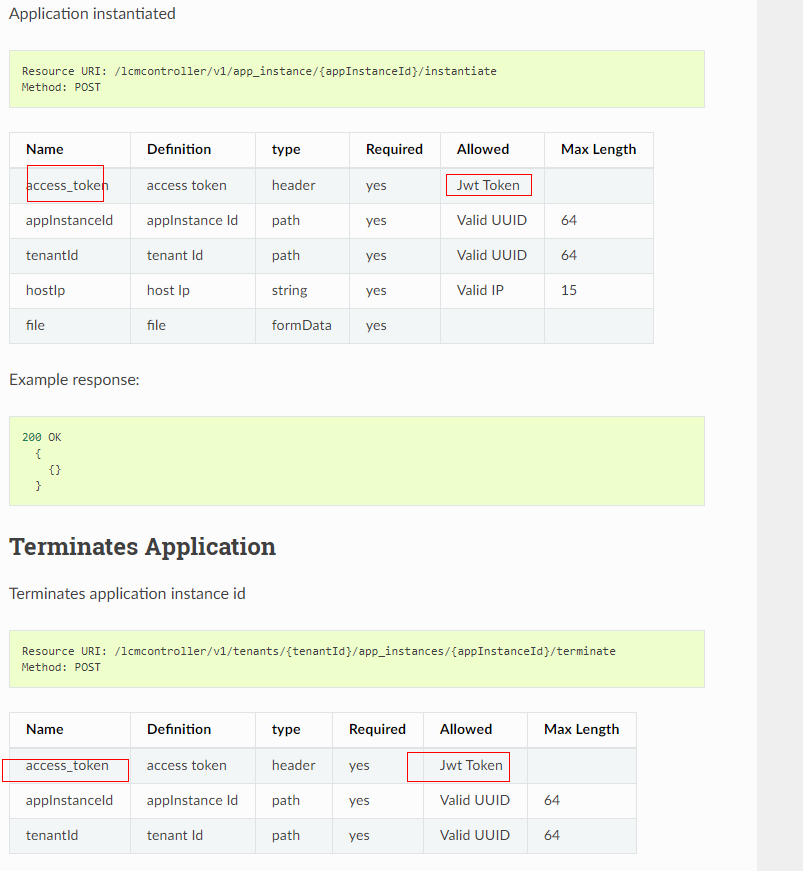
#### 测试说明：

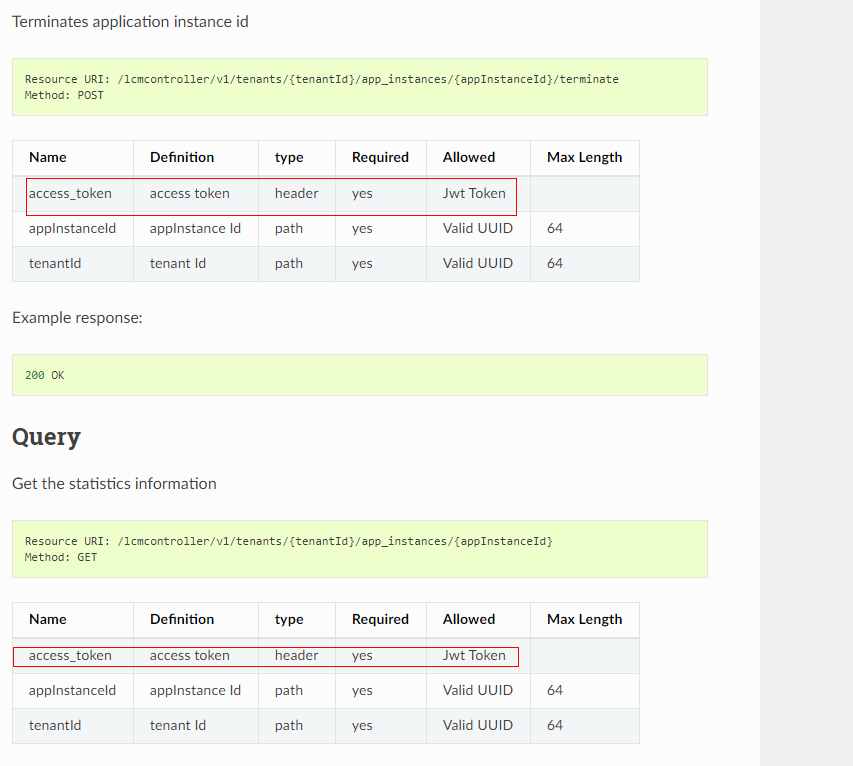
### 敏感数据（包括密码）或关键服务数据（网络结构，模型参数）必须使用安全传输协议在网络上传输，或者在传输之前进行加密。 注意：跨网络传输数据时，容易受到攻击者的窃取或篡改。因此，必须保护重要数据

### Mecm:

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

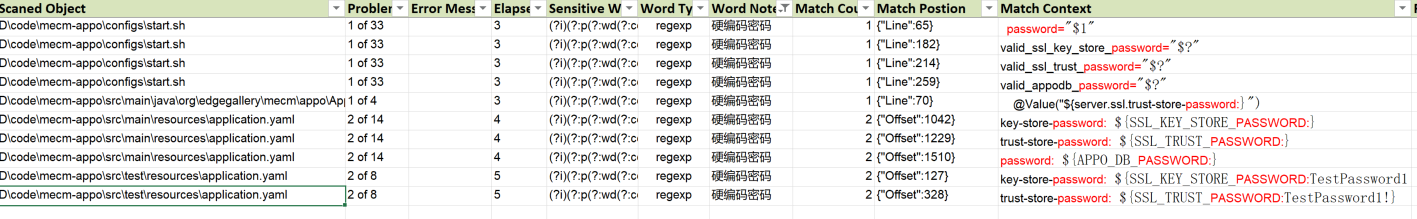
**检查加密方案：有认证方案**

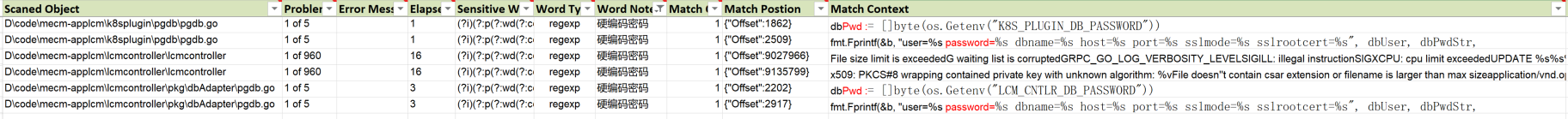




扫描硬编码：

无硬编码



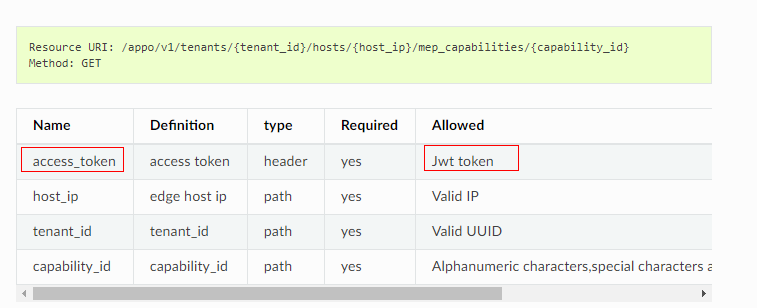


#### 测试结果：通过

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

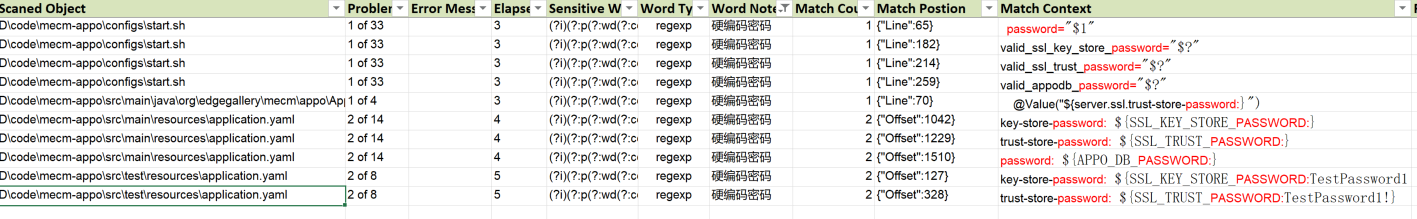
**检查加密方案：有认证方案**

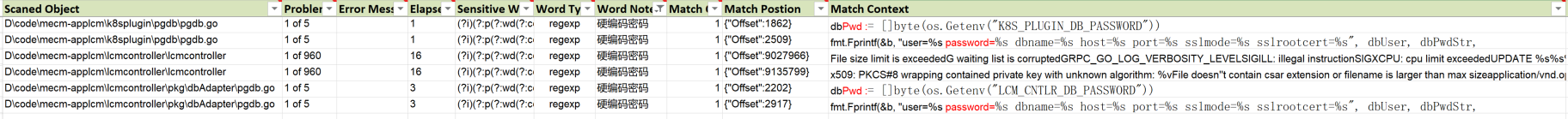




扫描硬编码：

无硬编码



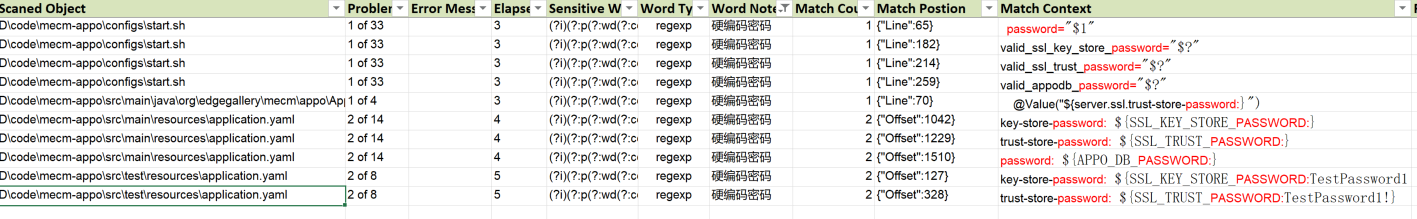


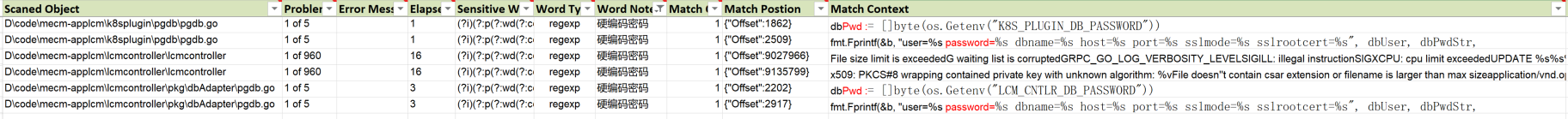
#### 测试结果：通过

#### ：

扫描硬编码：

无硬编码





#### 测试结果：通过

## Test case EG-TST-SEC-CP-2-2

#### 测试说明：

### 请勿使用SSL2.0，SSL3.0，TLS1.0或TLS1.1进行安全传输。建议使用TLS1.2和TLS1.3

### Mecm:

#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

##### 测试结果：通过

## Test case EG-TST-SEC-CP-3-3

#### 测试说明：

所有敏感数据都通过HTTP消息正文发送到服务器

### Mecm:

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)

注册applcm：

https://x.x.x.x:x/inventory/v1/tenants/{{tenant\_id}}/applcms

注册边缘节点

https://x.x.x.x:x/inventory/v1/tenants/{{tenant\_id}}/mechosts

分发app

https://119.8.36.45:30202/apm/v1/tenants/{{tenant\_id}}/packages

部署app：

https://119.8.36.45:30201/appo/v1/tenants/{{tenant\_id}}/app\_instances

##### 测试结果：通过

## Test case EG-TST-SEC-CP-3-8

#### 测试说明：

使用安全的随机数生成器生成密钥, 如果密钥是由随机数生成器生成的，则随机数生成器必须是安全的

进行横向越权测试。 ，用户访问另一个同级别权限用户，获取信息,不能获取到。

进行纵向越权测试，用户(访客)访问另一个更高级别权限用户(租户)，获取信息，不能获取.

##### 测试结果：通过

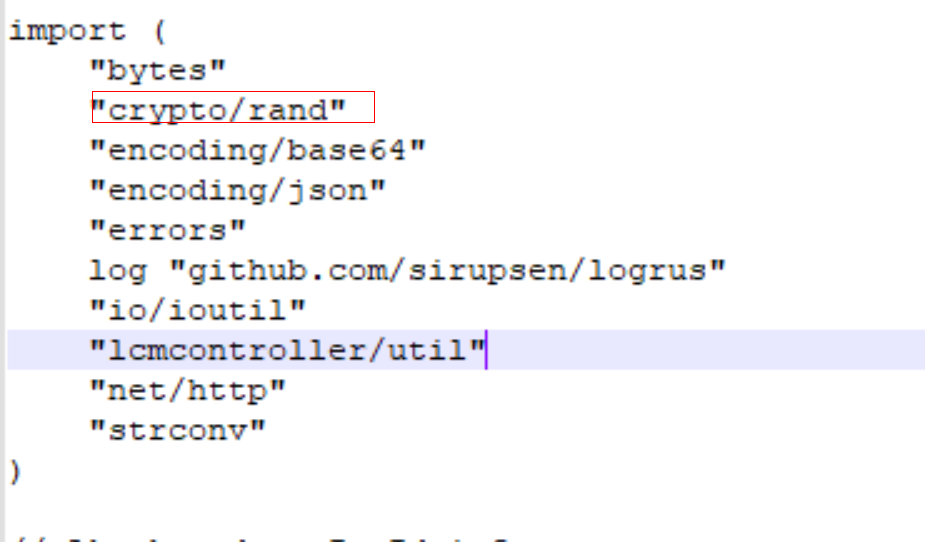
## Test case EG-TST-SEC-CP-4-5

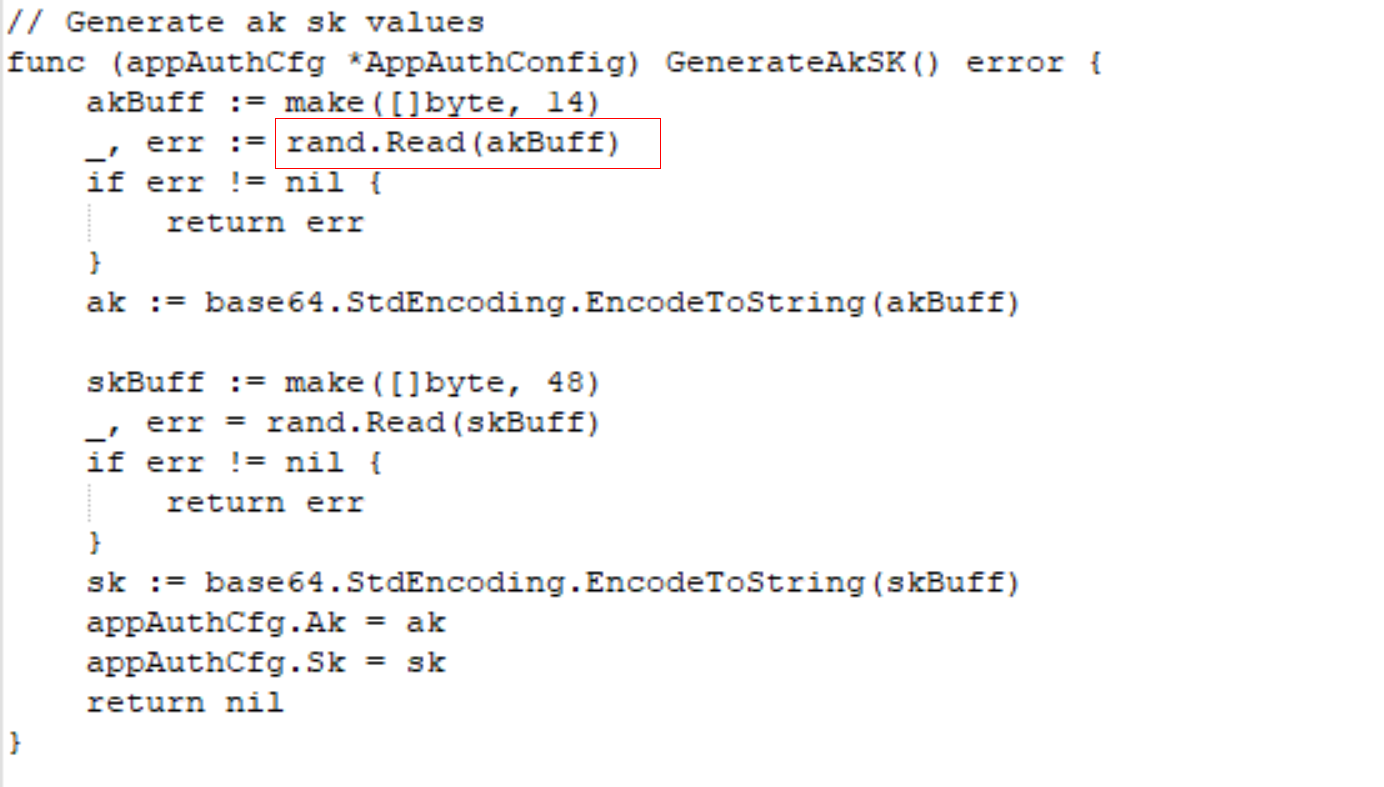
#### 测试说明：

使用安全的随机数生成器生成密钥, 如果密钥是由随机数生成器生成的，则随机数生成器必须是安全的

### Mecm:

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)





##### 测试结果：通过

## Test case EG-TST-SEC-CP-5-3

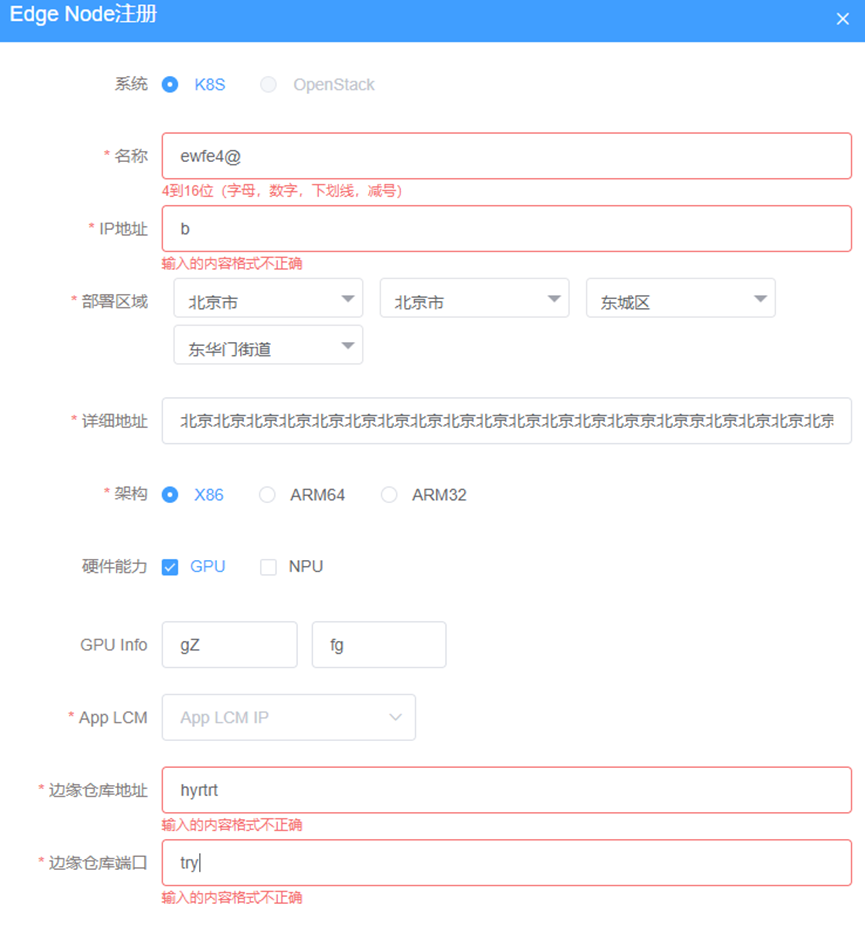
#### 测试说明：

### 所有输入必须限制在适当的大小限制内

### Mecm:

#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)

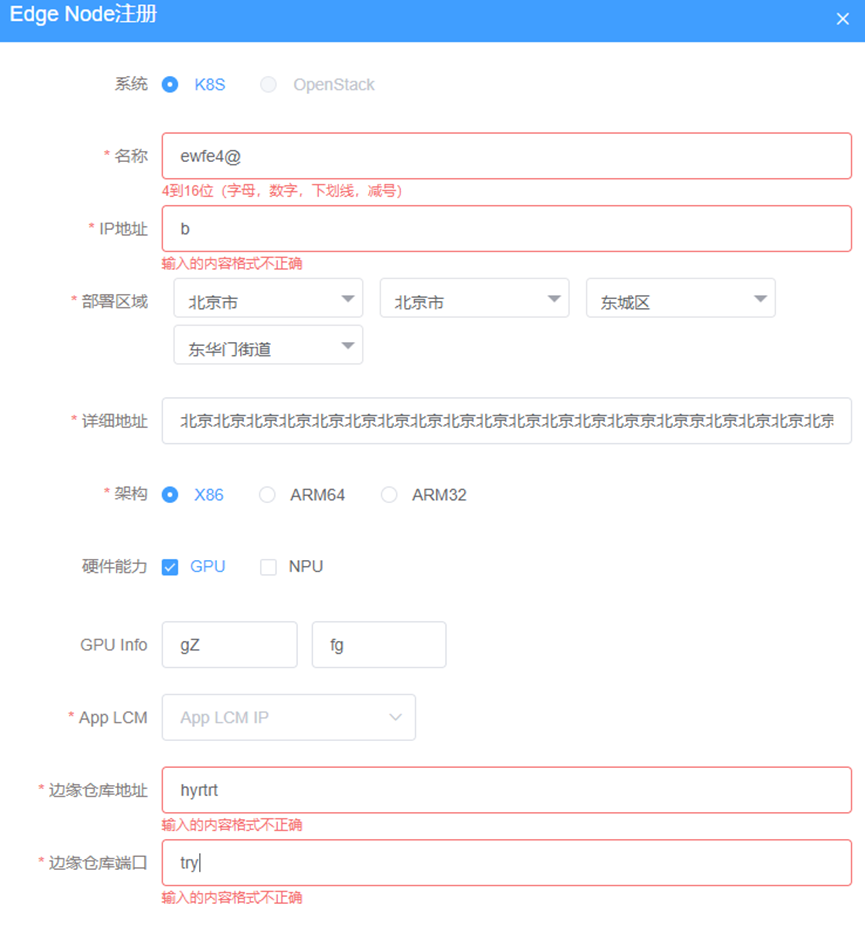




##### 测试结果：通过

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)





##### 测试结果：通过

## Test case EG-TST-SEC-CP-6-2

#### 测试说明：

将会话/凭证设置为有效的到期日期

### MECM

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)

Session半个小时后过期，继续操作需要重新登录。

##### 测试结果：通过

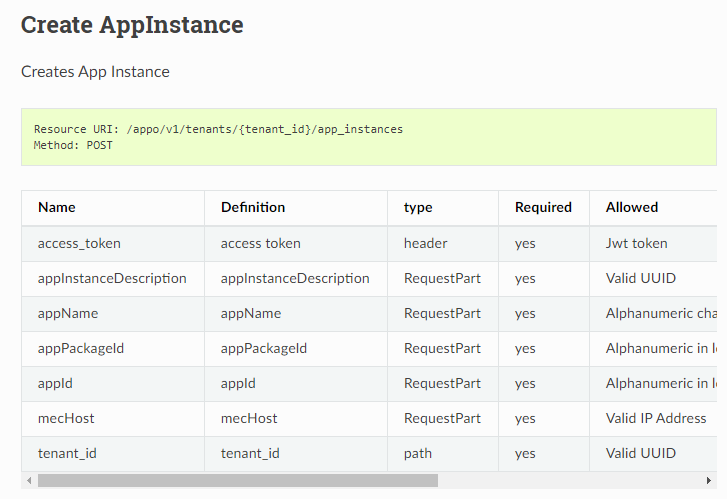
## Test case EG-TST-SEC-CP-8-1

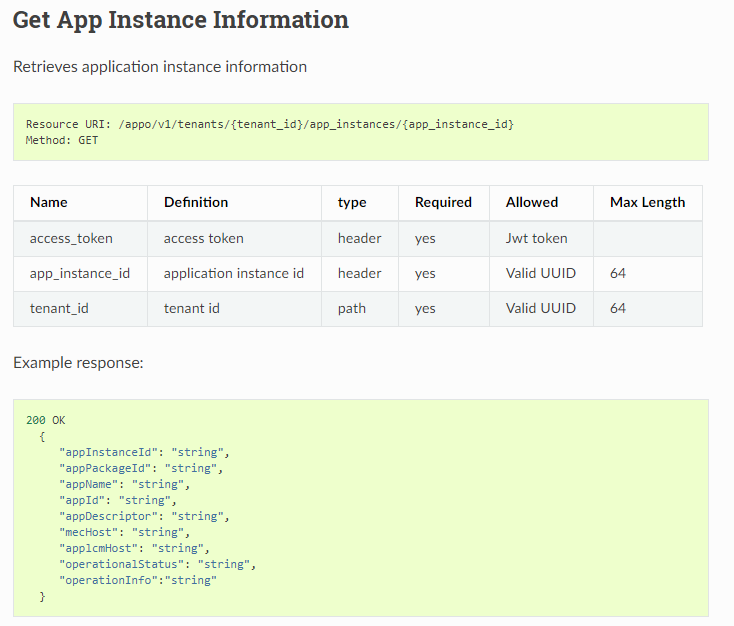
#### 测试说明：

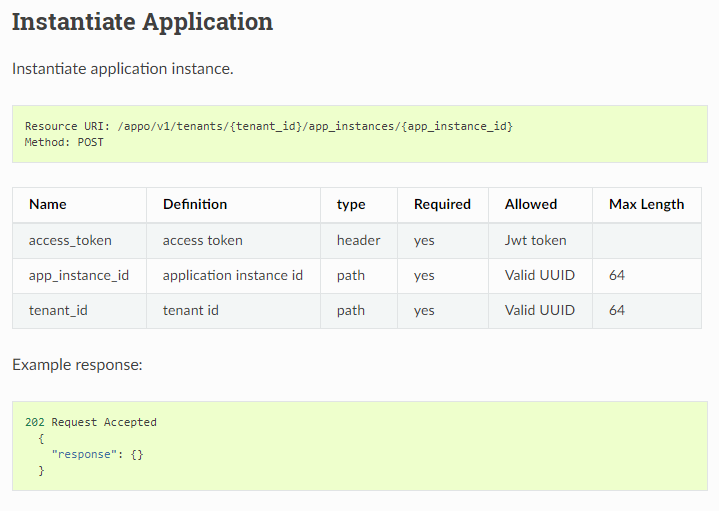
所有公共功能接口，RESTful接口，本地功能接口，命令行接口以及用于身份验证的默认用户名和密码都必须在产品或应用程序文档中进行描述。 **注意**：必须在应用文档中描述所有前面的新接口，以帮助用户更好地理解相应的模块

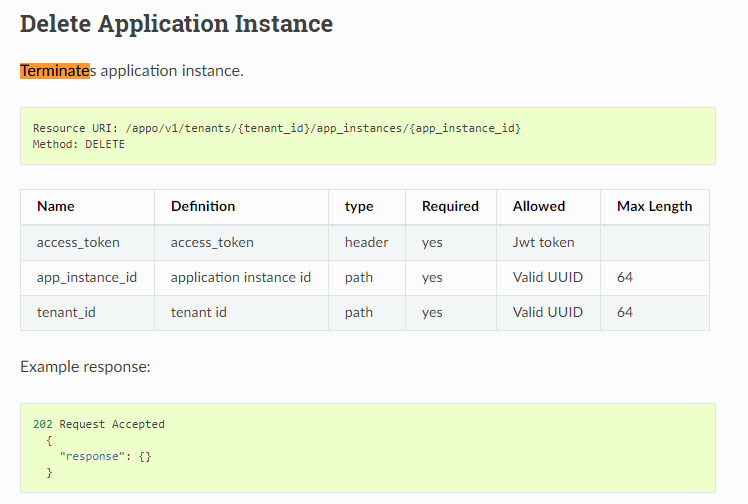
### Mecm:

#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)



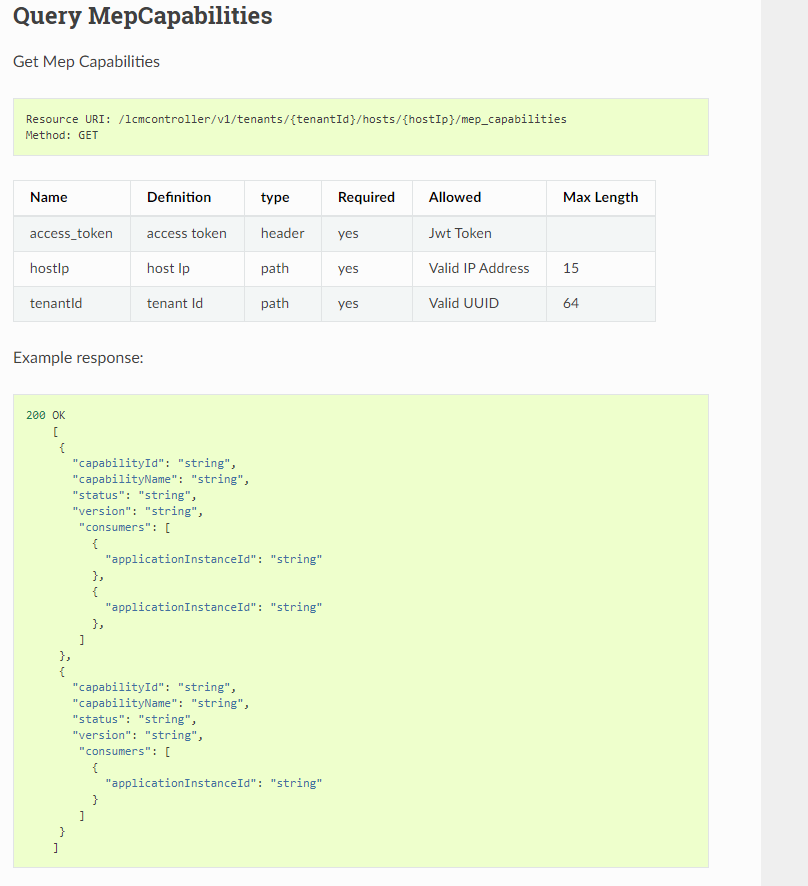


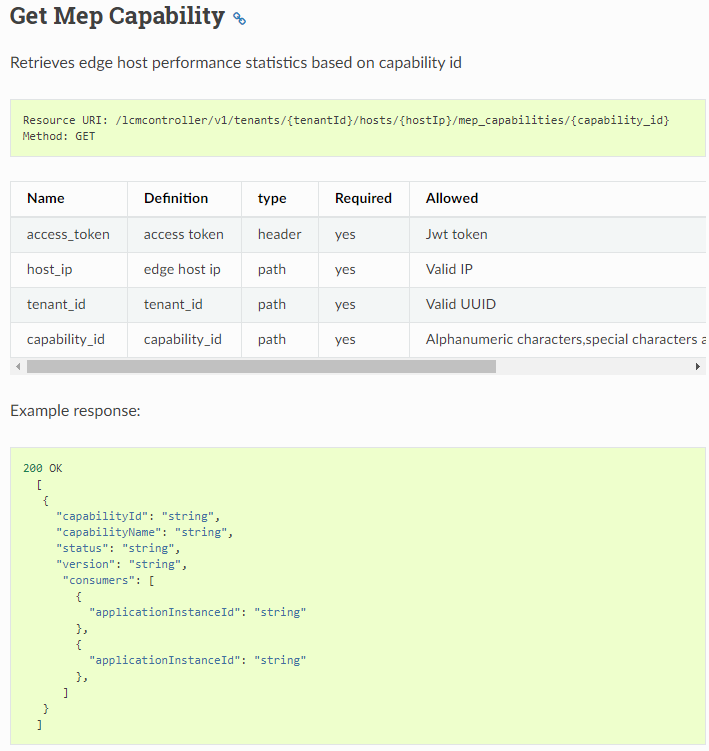




##### 测试结果：通过

#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

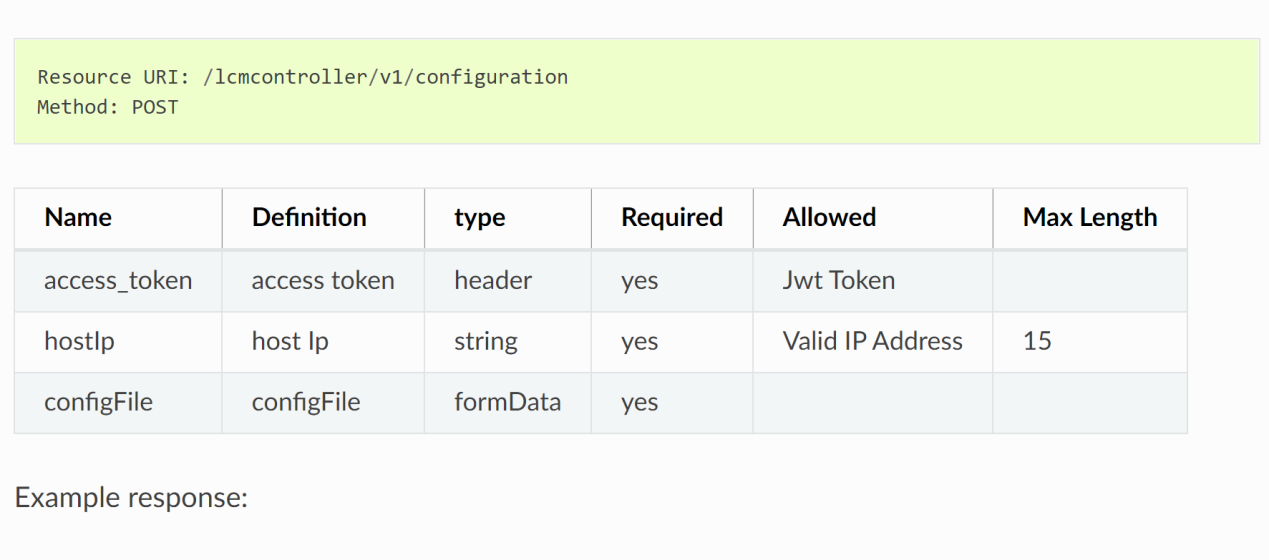


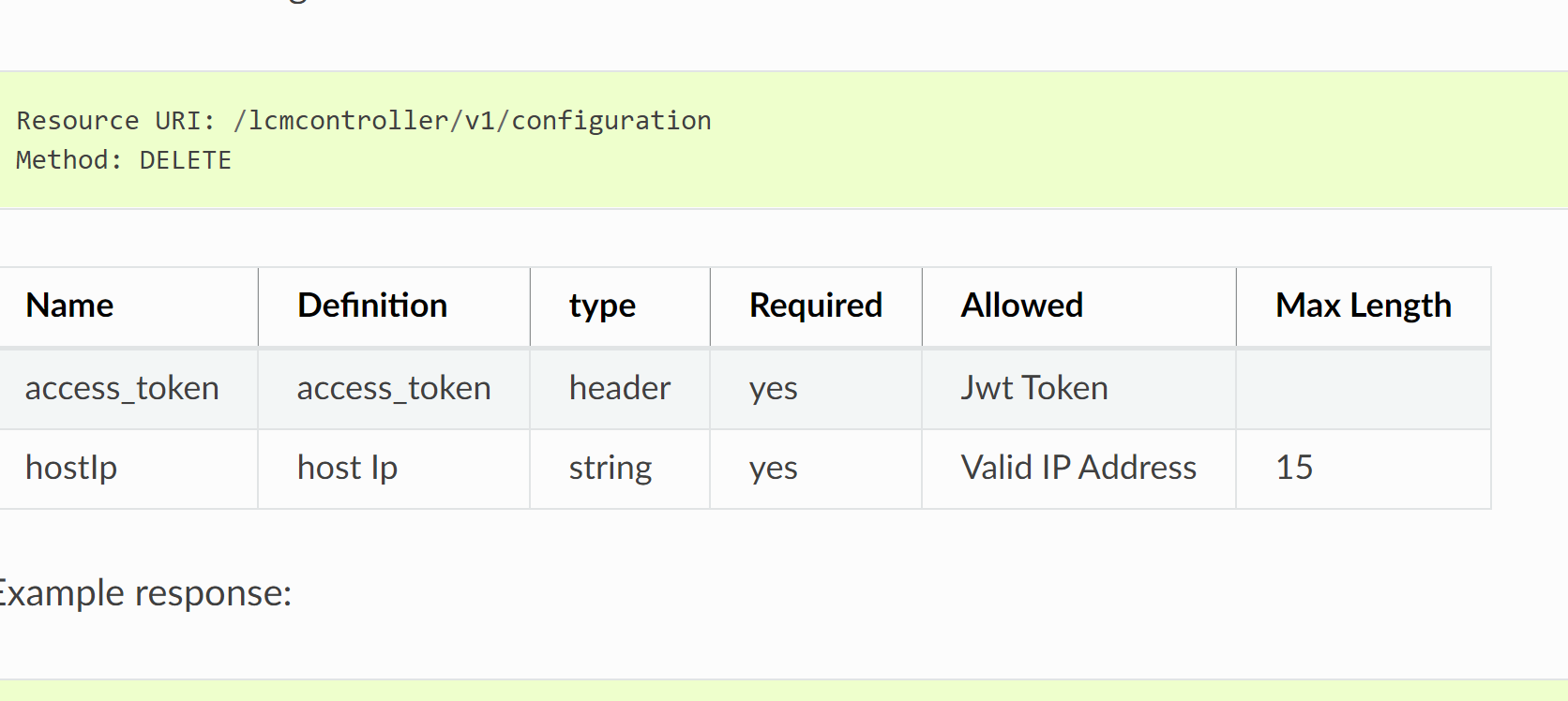


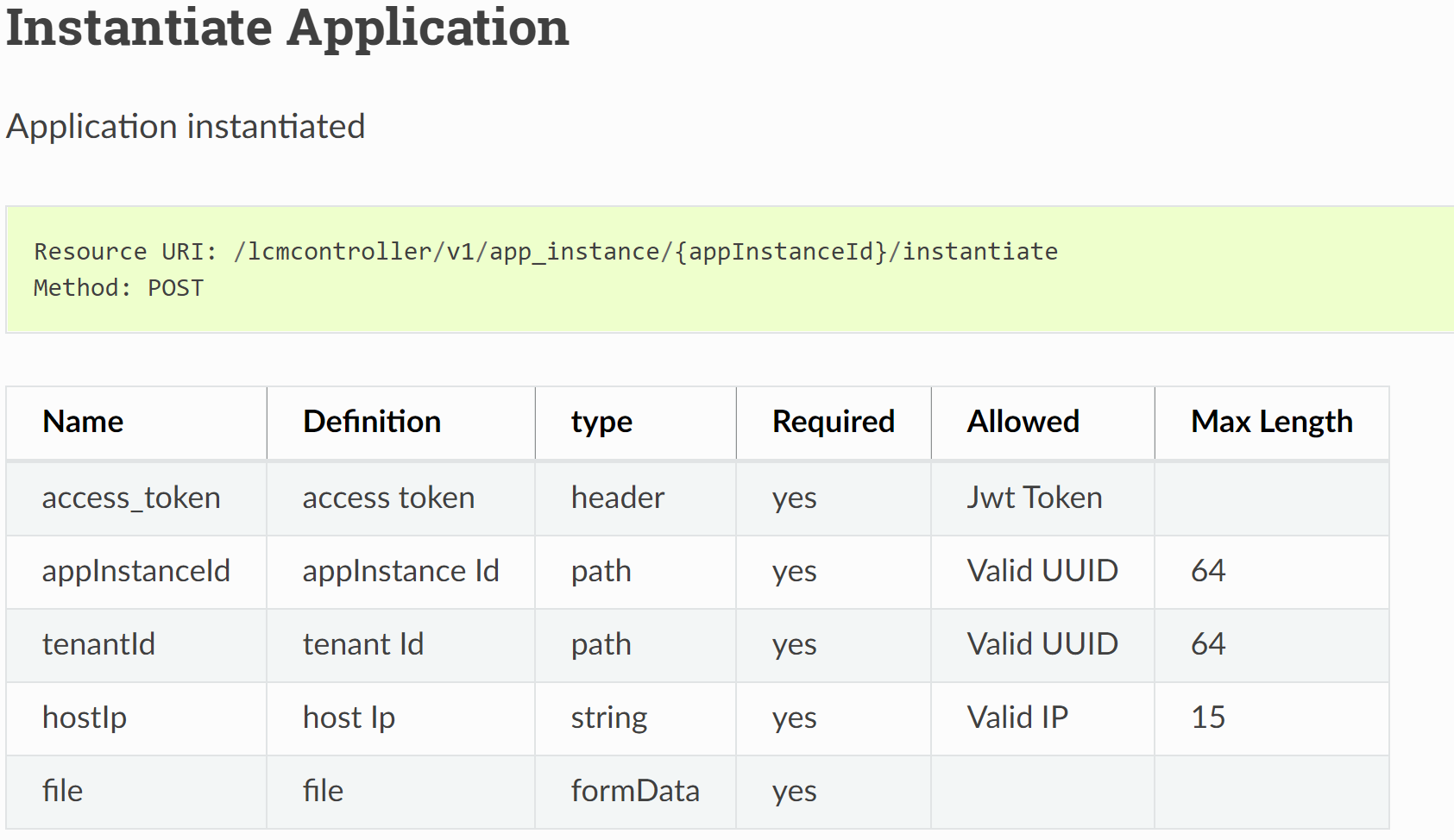
##### 测试结果：通过

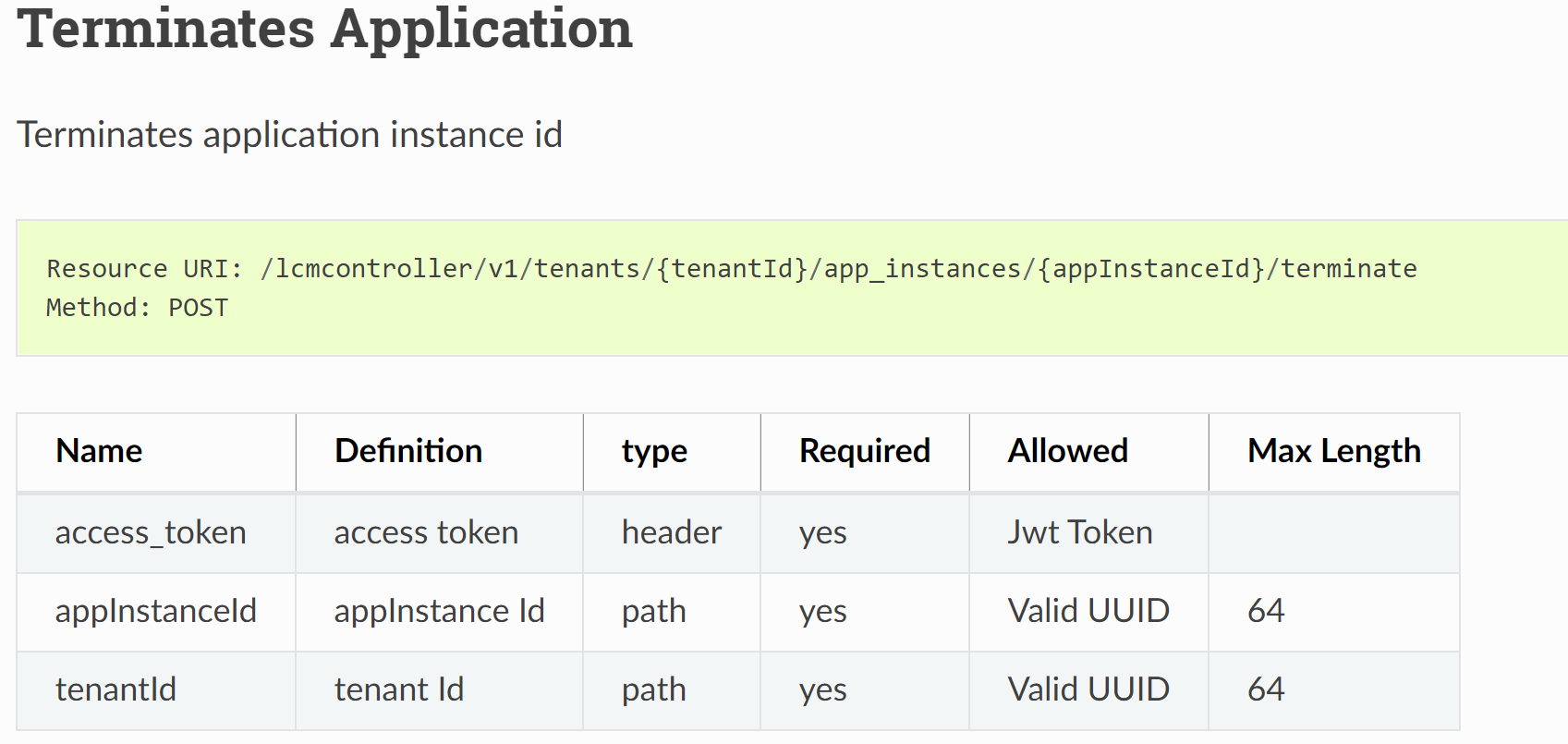
#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)

所有公共功能接口，都在文档中进行描述。









##### 测试结果：通过

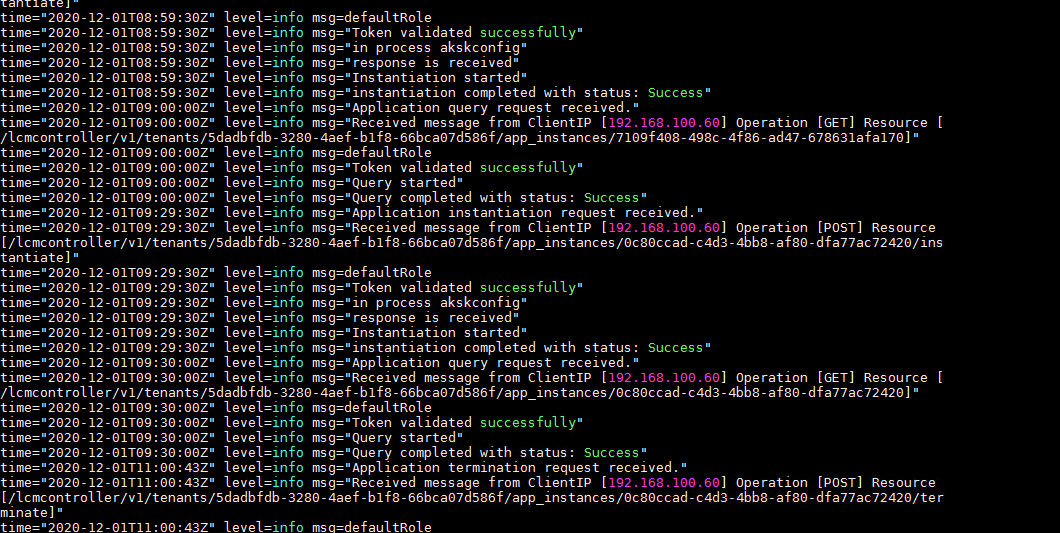
## Test case EG-TST-SEC-CP-9-2

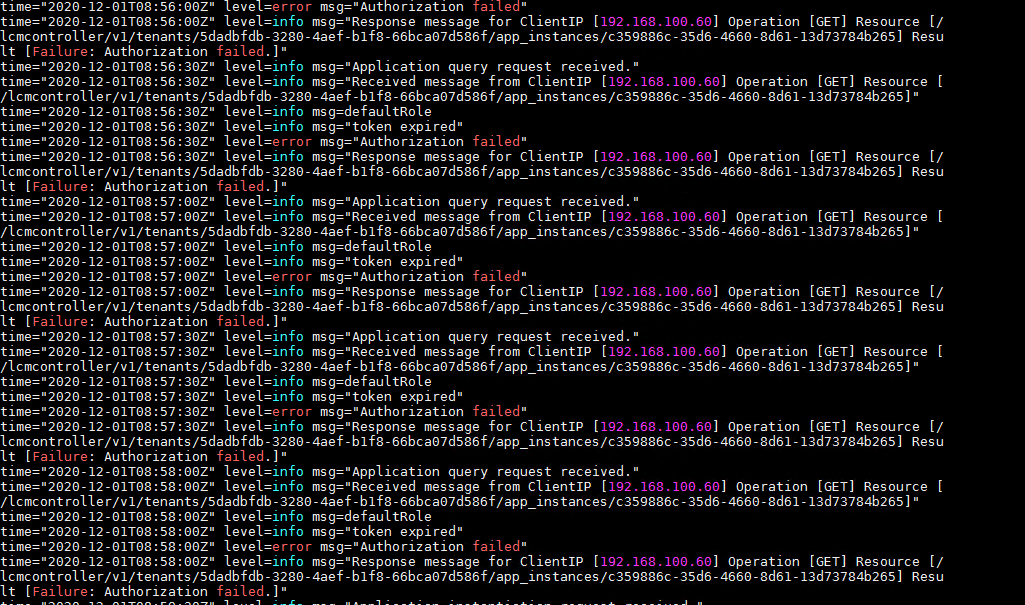
#### 测试说明：

足够的日志记录。 **注意**：确保记录所有与安全相关的成功和失败。如果没有正确记录安全性至关重要的事件（例如登录尝试失败），这将使恶意行为更难以检测，并且可能会阻止攻击成功后的取证分析

### Mecm:

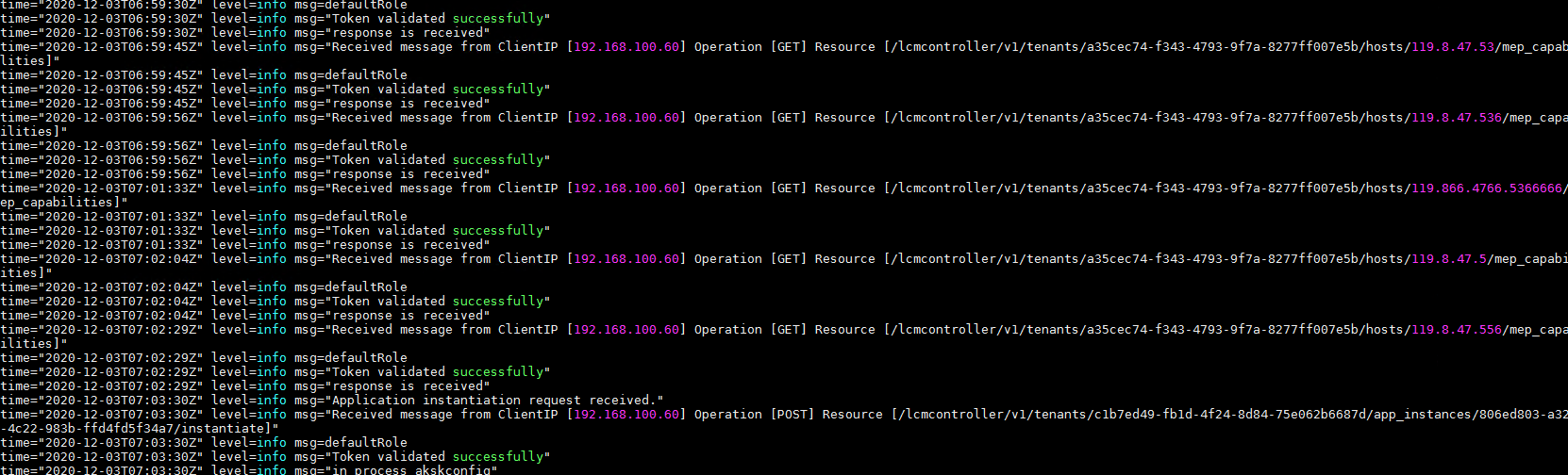
#### [MECM Support Batch Distribution and Batch Deployment](https://gitee.com/OSDT/dashboard?issue_id=I249AF)

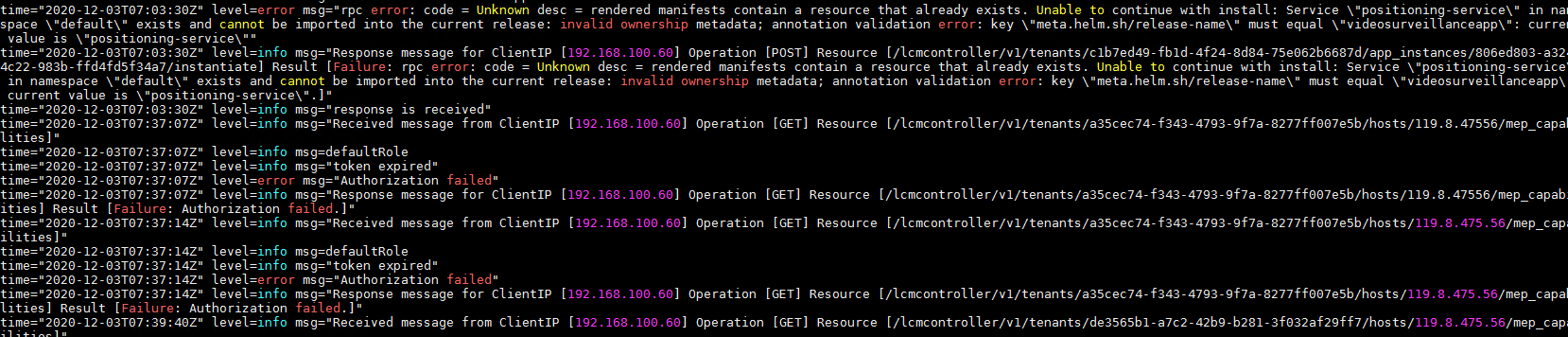




##### 测试结果：通过

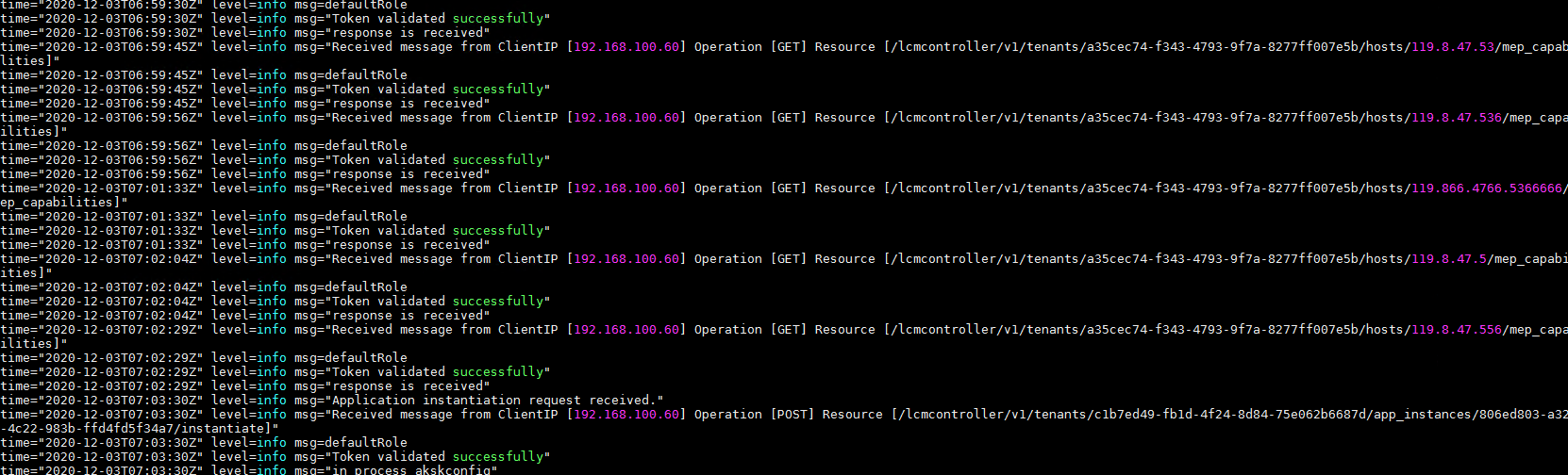
#### [【MECM 】MECM Support to query the capabilities](https://gitee.com/OSDT/dashboard?issue_id=I1Z3CN)

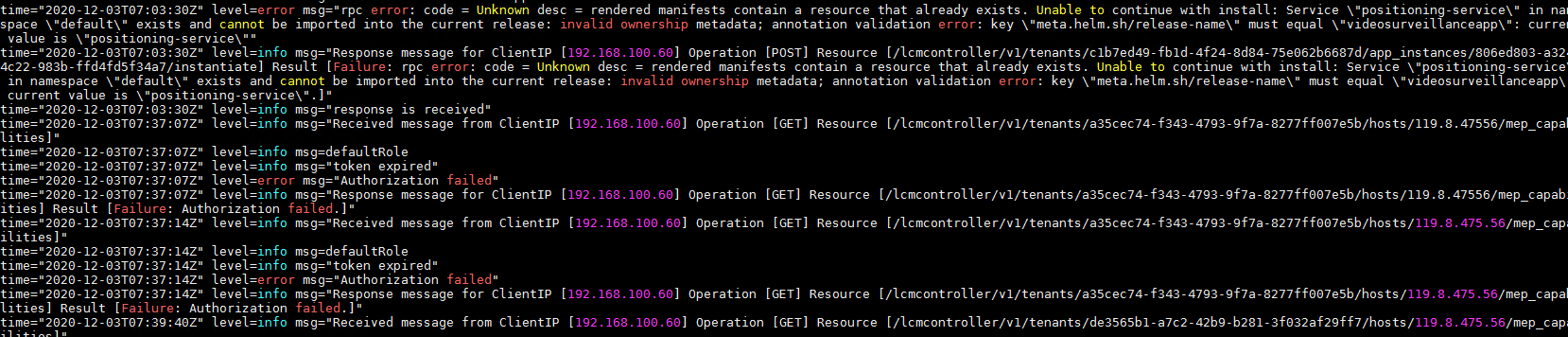




##### 测试结果：通过

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)





##### 测试结果：通过

## Test case EG-TST-SEC-CP-9-3

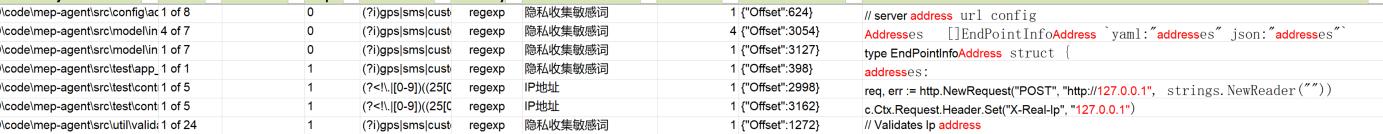
#### 测试说明：

请勿将敏感信息添加到日志或日志文件中

### MEP-Agent:

#### [【MEP-Agent】添加ak/sk配置接口](https://gitee.com/OSDT/dashboard?issue_id=I1QT48)

没有收集敏感信息存入日志



##### 测试结果：通过

## Test case EG-TST-SEC-CP-9-4

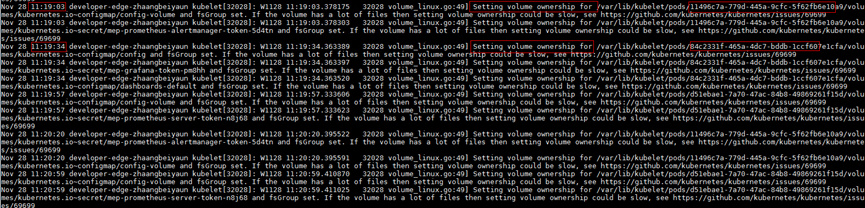
#### 测试说明：

避免记录过多的数据。 **注意**：禁止大量重复的日志消息，并用定期摘要替换它们

### Mecm:

#### 【MECM】[提供ak/sk分配功能](https://gitee.com/OSDT/dashboard?issue_id=I1R5LY)





##### 测试结果：通过