## R1.0迭代3合规测试报告

## R1.0 Sprint3 Compliance Test Report

## 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 APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

尝试删除access\_token直接访问App Rule MGR相关接口。

**测试结论**：**PASS**

[【MEP-Agent】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)

尝试在无身份验证的前提下直接调用。由于直接调用时无法获取Authorization参数，调用失败。Ok

**测试结论**：**PASS**

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

#### 测试说明：

对于每个需要授权的访问请求，服务器必须验证用户是否有权执行此操作。

Story：[【MECM】MECM支持权限处理，避免横向越权](https://gitee.com/OSDT/dashboard?issue_id=I1TH3T)

对Mecm各接口进行抓包，修改userID参数，查看能否得到正确响应。

均报401权限错误，ok

**测试结论**：**PASS**

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

#### 测试说明：

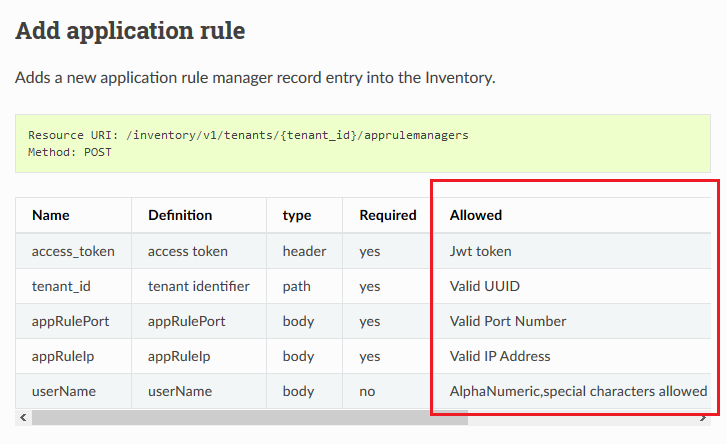
服务器必须验证所有不受信任的数据源的大小，类型，长度和特殊字符，并拒绝所有未通过验证的数据

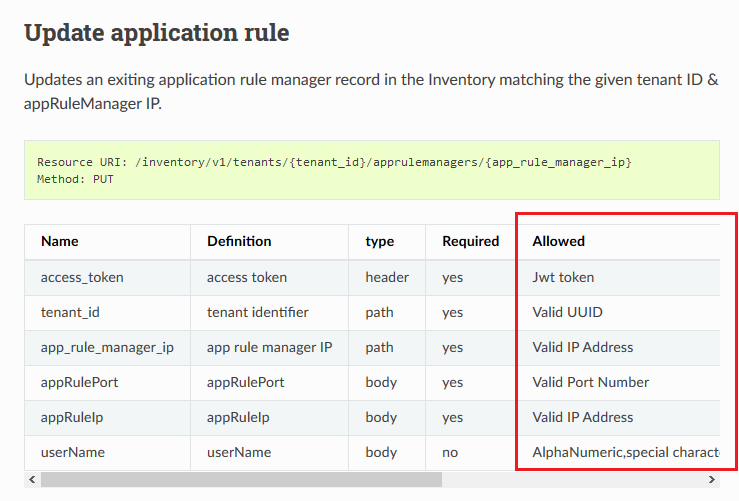
Story：[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

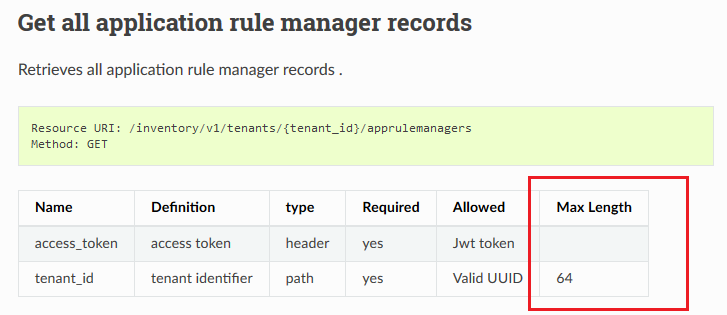
Story：[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

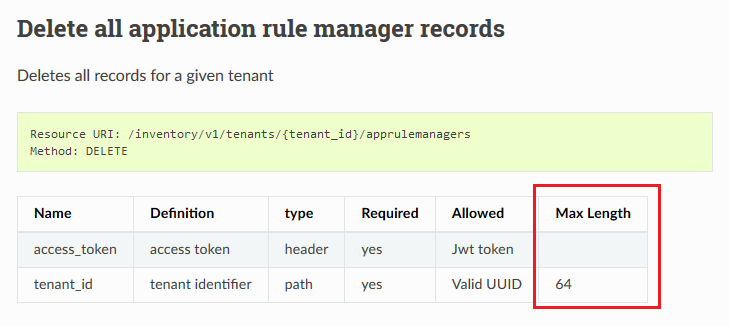
1. 输入不正确的数据，判断应用是否对用户输入数据进行了限制。
2. 查看接口文档，可以看到接口文档中，对各个接口所传入的参数进行了正确限制。











**测试结论**：**PASS**

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

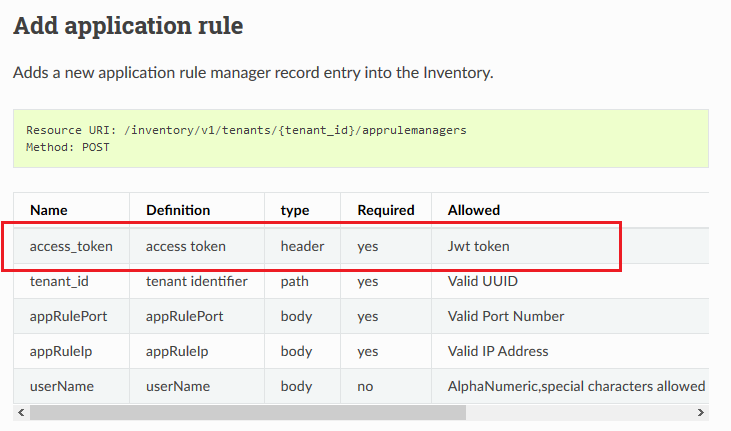
#### 测试说明：

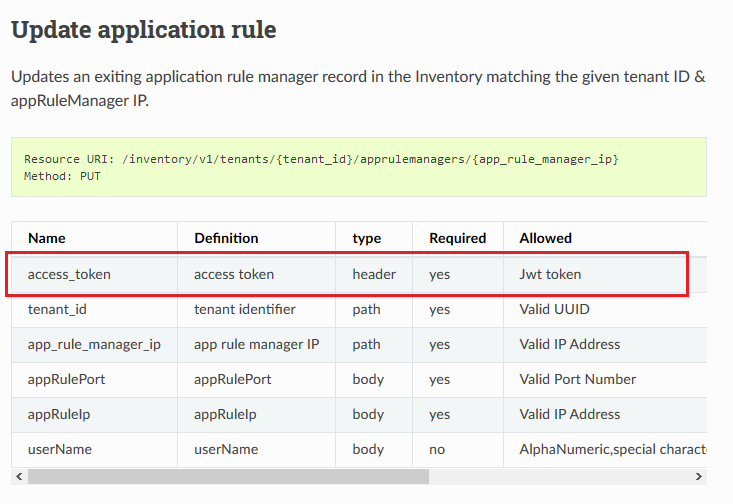
### 敏感数据（包括密码）或关键服务数据（网络结构，模型参数）必须使用安全传输协议在网络上传输，或者在传输之前进行加密。 注意：跨网络传输数据时，容易受到攻击者的窃取或篡改。因此，必须保护重要数据

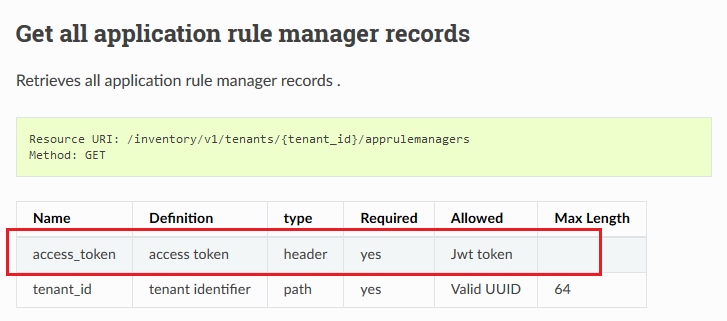
[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

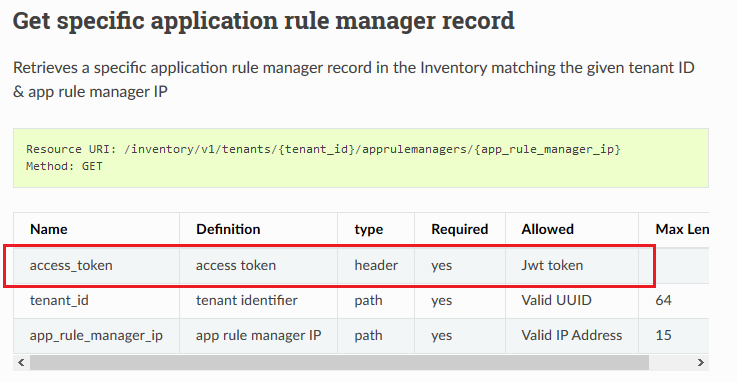
[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

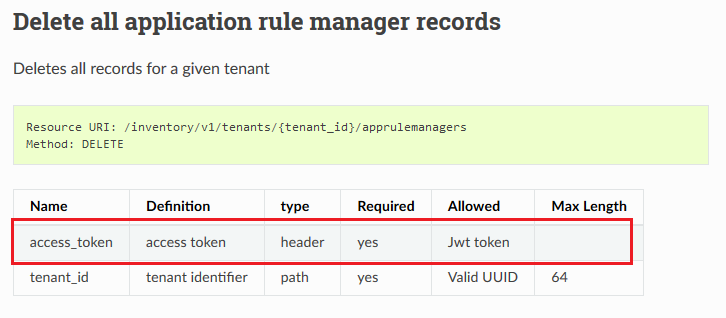
信息均通过https进行传输，并使用token来进行身份验证，防止信息被篡改。











**测试结论**：**PASS**

[【MEP-Agent】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)



**测试结论**：**PASS**

## 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 APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

使用sslscan进行测试，看到支持TLS 1.2

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-5-2

#### 测试说明：

应用程序必须限制活动的并发会话数。

**Story：**[【MECM】MECM支持限制活动的并发会话数](https://gitee.com/OSDT/dashboard?issue_id=I1TH8K)

**使用slowhttptest建立200个以上的活动连接，查看活动连接数是否存在上限。**

**测试过程**：

命令：slowhttptest -u “https://https://x.x.x.x:x” -B -c 500

可以看到，连接数增加到200时，应用拒绝服务，说明应用限制的活动的并发连接数。

**测试结论**：**PASS**

## 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 APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)



**测试结论**：**PASS**

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

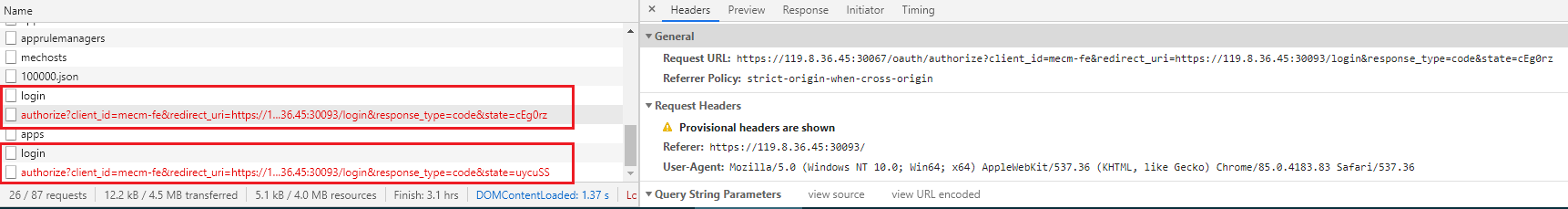
#### 测试说明：

将会话/凭证设置为有效的到期日期

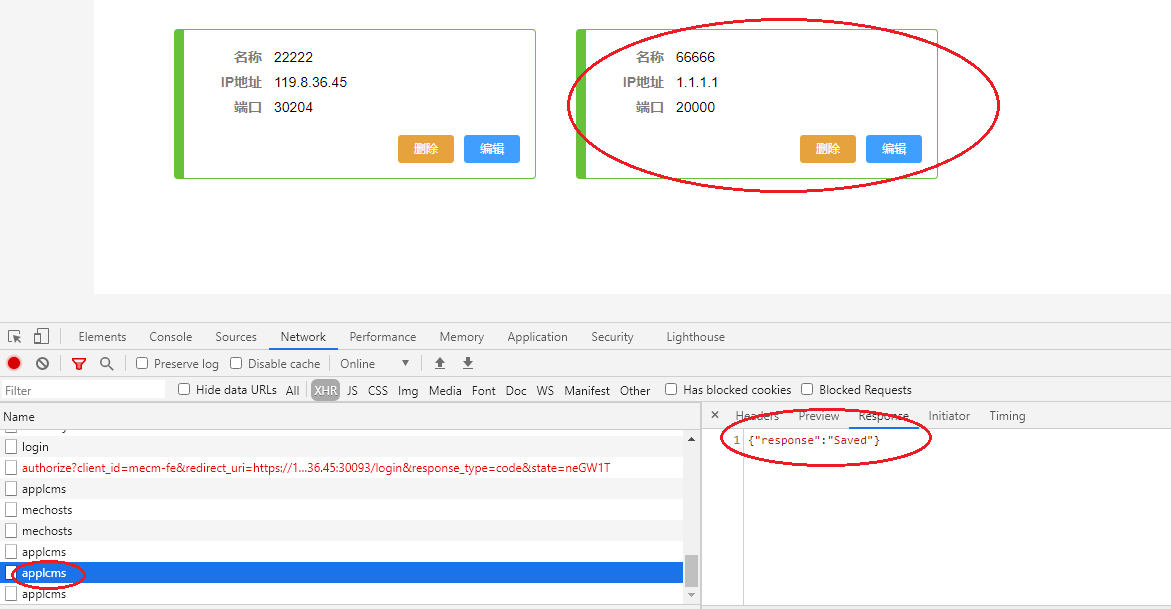
[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

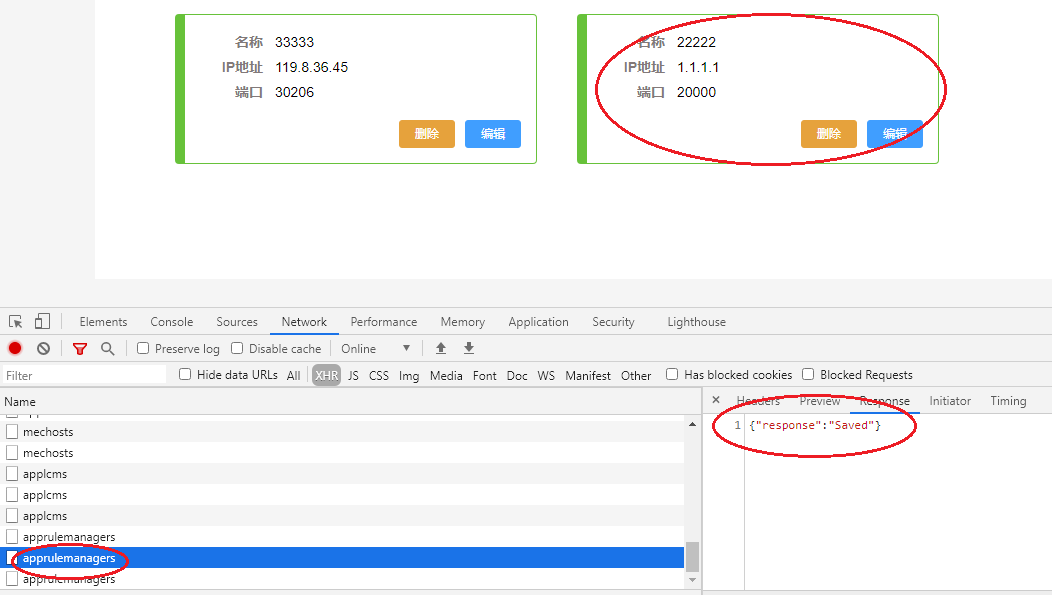
###问题描述  
Mecm会话超时后，AppLCM、AppRuleMGR、边缘节点注册等接口依然可以成功调用  
###重现步骤  
①登录mecm，并等待会话超时。（本次测试等待约2小时）  
②点击“应用包管理”，无法正确返回数据，并返回302状态，说明会话已超时



③点击“APP LCM注册系统”、“APP Rule MGR注册系统”、“边缘节点注册系统”等功能，发现相关接口依然可以成功调用。  
尝试注册AppLCM，成功



尝试注册AppRuleMGR，成功



尝试注册边缘节点，成功

###期望结果  
会话超时后，以上接口均无法调用  
###实际结果  
会话超时后，以上接口均可以调用。建议检查token自动失效机制是否正常。

**测试结论**：**Not PASS**

**不通过原因：token超时后，接口依然可以正常调用。**

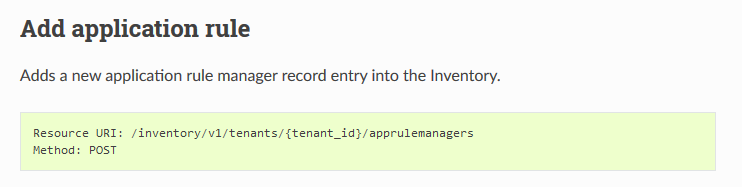
## Test case EG-TST-SEC-CP-8-1

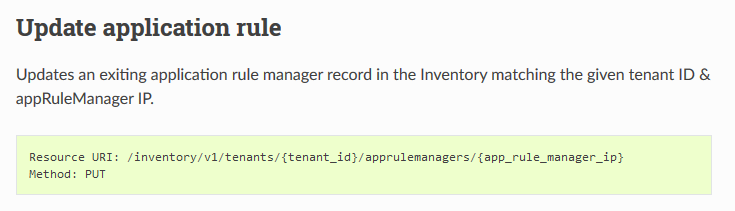
#### 测试说明：

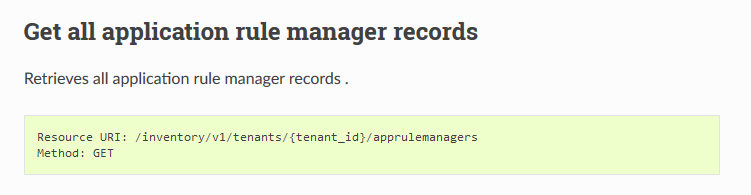
所有公共功能接口，RESTful接口，本地功能接口，命令行接口以及用于身份验证的默认用户名和密码都必须在产品或应用程序文档中进行描述。 **注意**：必须在应用文档中描述所有前面的新接口，以帮助用户更好地理解相应的模块

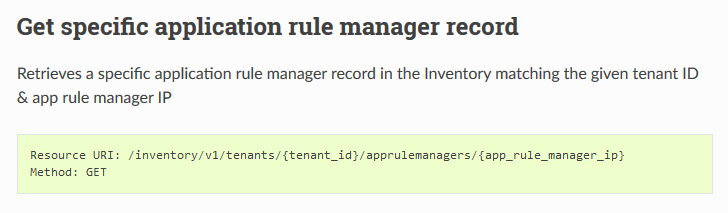
[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

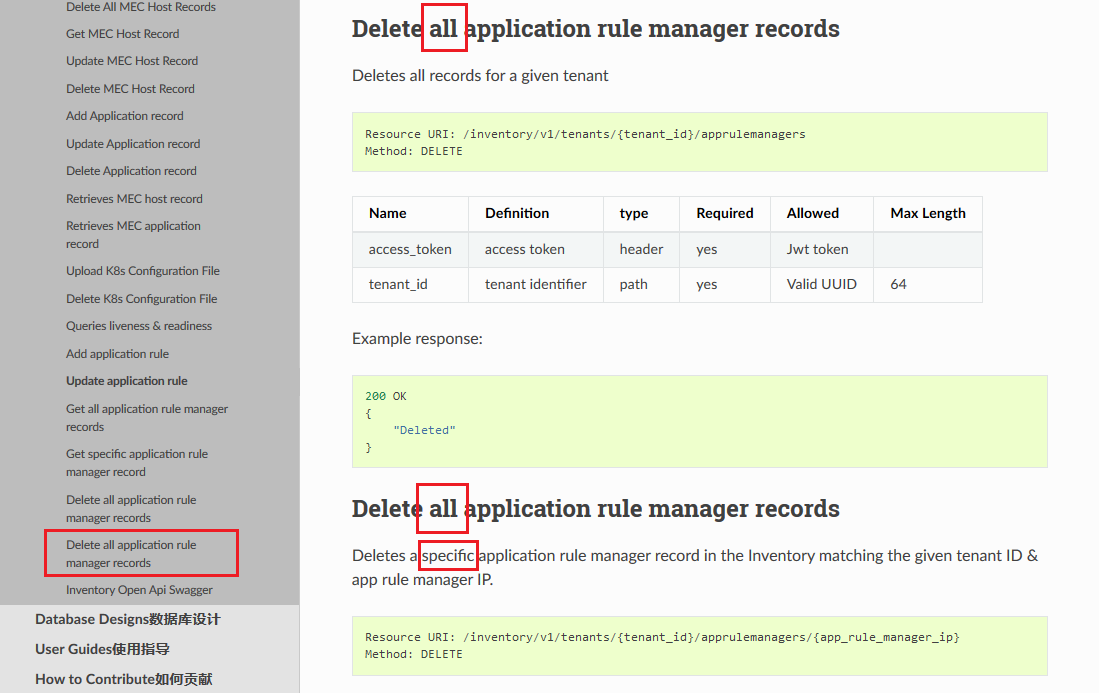








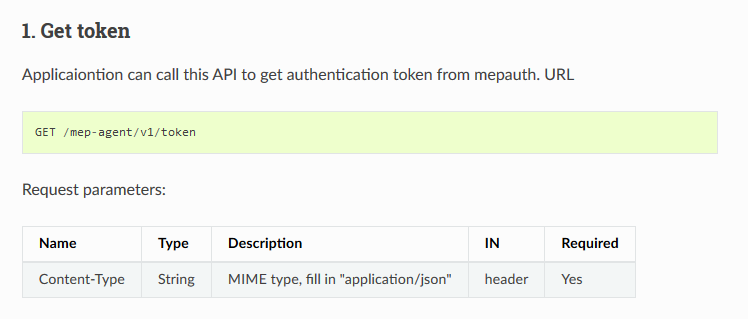




2个标签重复，第二个“Delete all”应改为“Delete a specific”

**测试结论**：**Not PASS**

[【MEP-Agent】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)



**测试结论**：**PASS**

## 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

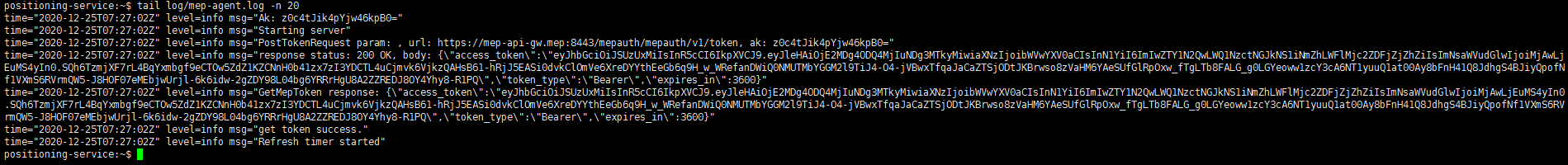
[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

登录mecm，进行AppRuleMGR相关新建、删除、修改、获取等操作，查看日志是否都进行记录。

**测试结论**：**PASS**

[【MEP-Agent】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)



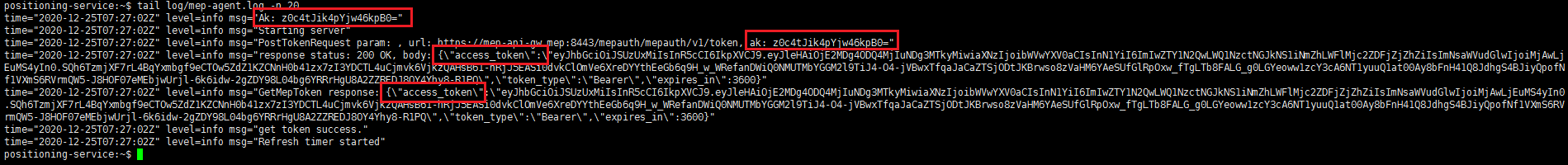
**测试结论**：**PASS**

## 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】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)



Mep-agent日志中看到access\_token等敏感信息，不通过。

**测试结论**：**Not PASS**

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

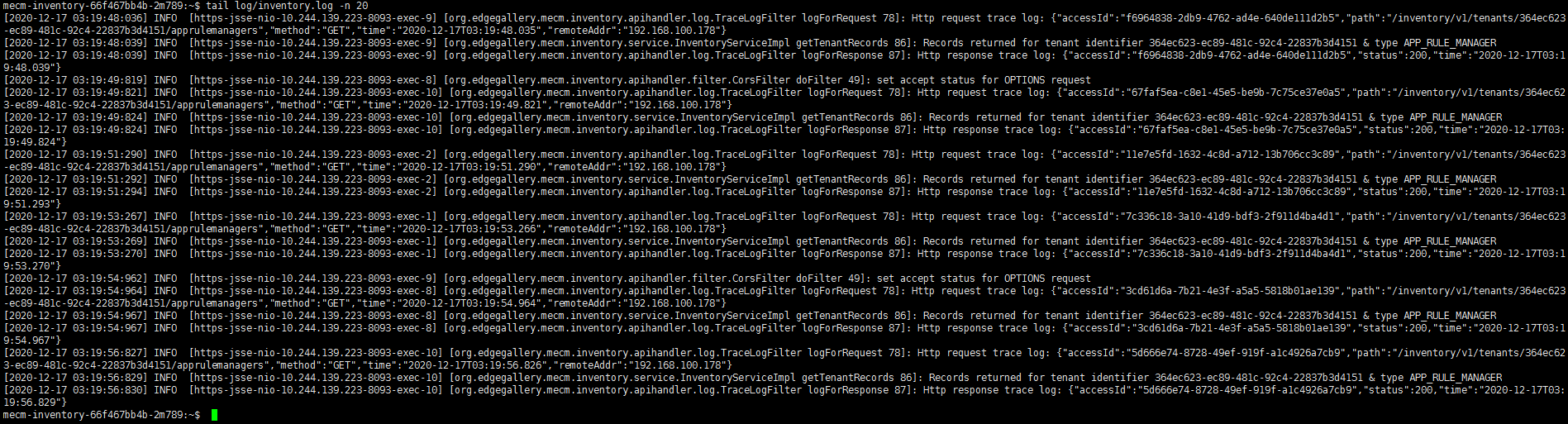
#### 测试说明：

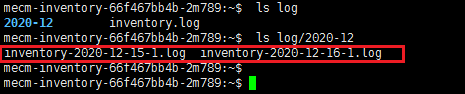
避免记录过多的数据。 **注意**：禁止大量重复的日志消息，并用定期摘要替换它们

[【MECM】MECM Support APP Rule Cofing From Portal](https://gitee.com/OSDT/dashboard?issue_id=I24700)

[【MECM】MECM Support APP Rule Config During APP Orchestration](https://gitee.com/OSDT/dashboard?issue_id=I246ZD)

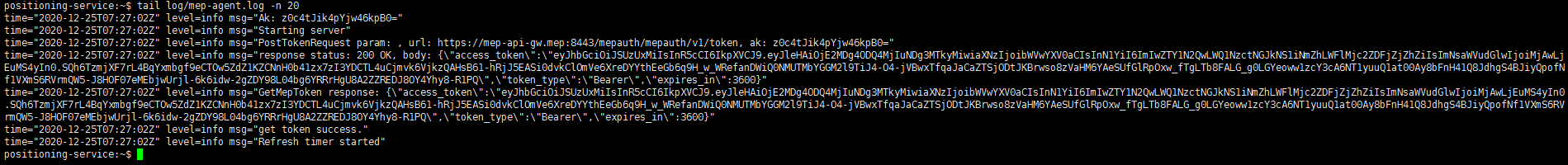
日志文件按每天生成新的文件，避免了单个文件记录过多数据。





**测试结论**：**PASS**

[【MEP-Agent】增加获取token接口](https://gitee.com/OSDT/dashboard/issues?sort=created_at desc&labels=Sprint3&id=I23QX8)



**测试结论**：**PASS**