## v1.1 Spirnt1合规测试记录

## R1.1 Sprint1 Compliance Test Record

## 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

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1. 首页的分析analyz接口；
2. 任务管理页面下的批量删除batch\_delete接口。

对analyze接口抓包，尝试删除cookie信息，无法正常响应。

对batch\_delete接口抓包，尝试删除cookie信息，无法正常响应。

**测试结论**：**PASS**

[【MEP】APP Instance Termination Enhancement](https://gitee.com/OSDT/dashboard?issue_id=I2DQV5)

测试方法：尝试调用该接口，分别添加和删除token信息，查看接口能否正确响应。

可以看到，删除token信息后返回401认证失败。Ok

通过curl命令测试，结果相同。

curl -k -X DELETE https://x.x.x.x:x/mep/mec\_app\_support/v1/applications/5abe4782-2c70-4e47-9a4e-0ee3a1a0fd1f/AppInstanceTermination -H "Authorization: Bearer eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MTQzMDgzODAuNzMyNzg1LCJpc3MiOiJtZXBhdXRoIiwic3ViIjoiNWFiZTQ3ODItMmM3MC00ZTQ3LTlhNGUtMGVlM2ExYTBmZDFmIiwiY2xpZW50aXAiOiIyMDAuMS4xLjIifQ.oyp3k9n01CiC9xiZYev\_n3P-9yCr\_kSaKZEJhOYqjVzT8sBSaIlCC0rjqSHzWVFt\_9sEIewtjXOgk5p2MCw1DQFRDm1Td4LhIH96IPYzkwJ3IgiHJa4AyIdANGD9bezA\_p42RRrl3Hsr15m-R3MVGbmc0LzjKbcRmd6t585F098a8iuaDtlMu\_V9Tr00fElnRBvPrXfxq8JUWiza47Q35pyzsIXZoUB153DH14rK9Fp50Qn5pfGmr\_0bY3PX9\_edoyNoQ\_tVg-MElVW4R0GoGcCEAGiSxccVmRvIrrBjfip7YueiYPjMneNvmzmmN\_2VmYe531A4bCysC7oIKrvW5w"

**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。

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

由于sprint1还未完成分权分域控制编码，待sprint3编码完成后再进行测试。

**测试结论**：待定

[【UserMgmt】用户统一管理功能支持设置用户所属角色](https://gitee.com/OSDT/dashboard?issue_id=I23FRE)

测试方法：尝试使用普通用户访问设置角色接口，看能否设置成功

抓取admin设置角色的请求包，将cookie更换为普通用户，提交后报403forbidden，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

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

Analyze接口为GET方法，不向后端服务器传入数据，所以不涉及此条。

对batch\_delete接口抓包，修改POST参数内容（格式，长度等），查看接口能否正常响应。

无法正确响应，提示解析错误，ok

超长数据解析失败，ok

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-1-12

#### 测试说明：

基于角色的访问控制。version：v1.0 注意：必须定义并遵循基于角色的访问控制，才能访问系统中的资源。适用于用户以及应用程序。（此规则将在R1.0 \*中生效）

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

由于sprint1还未完成分权分域控制编码，待sprint3编码完成后再进行测试。

## Test case EG-TST-SEC-CP-1-15

#### 测试说明：

不再使用的账号必须删除或停用。删除账号时，必须同时删除相应的凭据（如密码、秘钥等），以防止这些被认为是后门。

[【UserMgmt】用户统一管理功能支持对用户停用/启用](https://gitee.com/OSDT/dashboard?issue_id=I2E9MB)

[【UserMgmt】支持用户统一管理基本查询展示功能](https://gitee.com/OSDT/dashboard?issue_id=I2E9M8)

此2条story针对1.15测试内容相同，故合并测试。

登录admin用户，查看当前用户。

未发现默认的特权用户。删除用户后，用户全部数据删除。停用功能正常。Ok

**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

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

使用sslscan x.x.x.x:x进行测试。Ok

**测试结论**：**PASS**

[【MEP】APP Instance Termination Enhancement](https://gitee.com/OSDT/dashboard?issue_id=I2DQV5)

Kubectl get svc -n mep查看mm5端口

./sslscan x.x.x.x:x

可以看到TLS1.2和1.3允许使用。Ok

**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

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

Analyze接口为GET接口，不涉及此条。

对batch\_delete接口传入超长内容，解析失败，ok

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-7-2

#### 测试说明：

必须接受XML或JSON模式，并在接受输入之前对其进行验证。 **注意**：模式验证是针对应用程序逻辑攻击的第一级防御。

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

Analyze接口为GET接口，不涉及此条。重点测试batch\_delete接口（需要传入json格式数据）

尝试传入非标准的json数据，查看后端是否进行了格式校验。

提示格式解析错误，ok

**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-7-9

#### 测试说明：

Web页面必须提供注销功能。注销服务必须清除正在使用的会话。用户关闭浏览器后（并非点击页面上的“注销”按钮），服务器可以保持会话直到会话超时之后立即清除会话。tag: version v1.1

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

测试方法：ATP页面存在注销功能，ok。登录用户账户，记录session内容，点击注销，（此时session应该已失效）。再次使用该session，查看能否使用。

首先登录账户，记录session值，点击注销；再次登录用户，将session值替换为之前的session值，无法正确响应，ok

登录后，不注销的情况下关闭浏览器，再次访问时session已失效，ok

**测试结论**：**PASS**

## 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

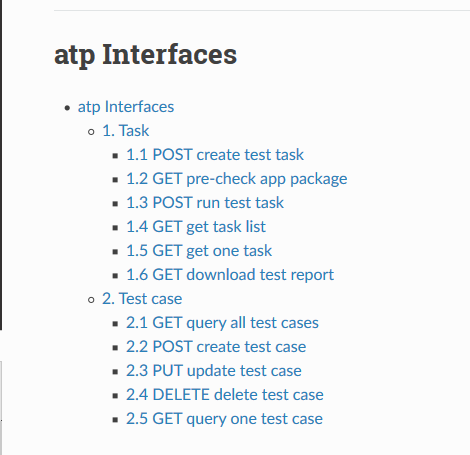
[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

查看docs中是否存在这两个接口的说明文档。未发现新增接口的说明文档。



**测试结论**：**Not PASS**

**不通过原因：新增接口未及时更新docs文档。**

[【UserMgmt】用户统一管理功能支持对用户停用/启用](https://gitee.com/OSDT/dashboard?issue_id=I2E9MB)

该story包括停用用户/v1/users/status/{userId}/disallow

和启用用户 /v1/users/status/{userId}/allow

2个接口。未发现接口说明文档。



**测试结论**：**Not PASS**

**不通过原因：新增接口未及时更新docs文档。**

[【UserMgmt】支持用户统一管理基本查询展示功能](https://gitee.com/OSDT/dashboard?issue_id=I2E9M8)

包括查询所有用户信息 /v1/users/list

1个接口。未发现接口说明文档。



**测试结论**：**Not PASS**

**不通过原因：新增接口未及时更新docs文档。**

[【MEP】APP Instance Termination Enhancement](https://gitee.com/OSDT/dashboard?issue_id=I2DQV5)

新增接口

/mep/mec\_app\_support/v1/applications/:appInstanceId/AppInstanceTermination

未找到新增接口文档。



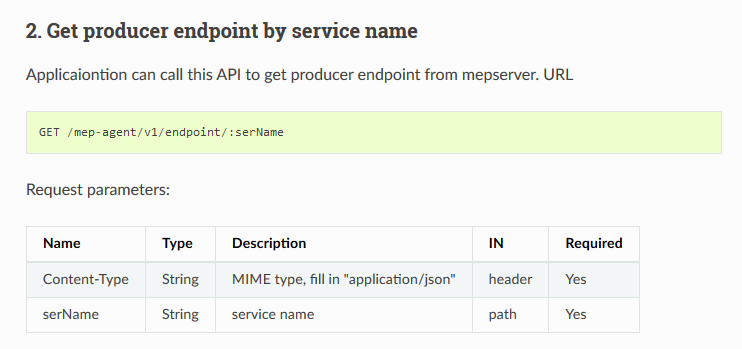
**测试结论**：**Not PASS**

**不通过原因：新增接口未及时更新docs文档。**

[【mep-agent】mep-agent提供根据service name返回endpoint信息](https://gitee.com/OSDT/dashboard?issue_id=I2CXVE)

新增接口：

/mep-agent/v1/endpoint/:serName



**测试结论**：**PASS**

## Test case EG-TST-SEC-CP-9-1

#### 测试说明：

请勿记录未经消毒的用户输入。 **注意**：未经消毒的日志记录可能使攻击者伪造日志条目或将恶意内容注入日志。

[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

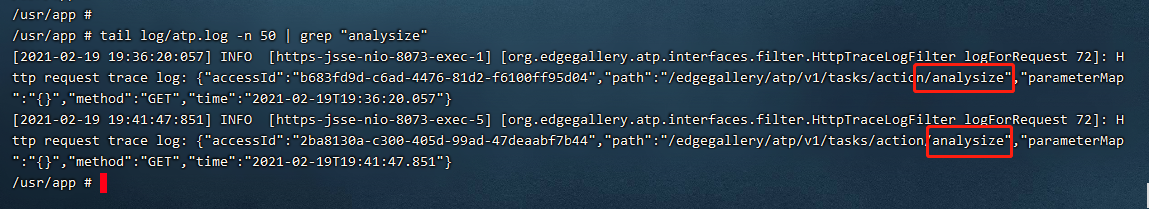
此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

测试方法：构造CRLF请求（%0d%0a%20[aaatime]analysize222）并访问，登录服务器后台，进入ATP相关pod，查看日志，是否CRLF请求伪造成功。

发送请求。然后登陆atp后台，查看日志记录，该CRLF注入是否生效。



可以看到，CRLF注入未生效，日志中未搜索到注入payload。Ok

同样方法测试batch\_delete接口，未发现CRLF注入漏洞。Ok

**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

**测试结论**：**PASS**

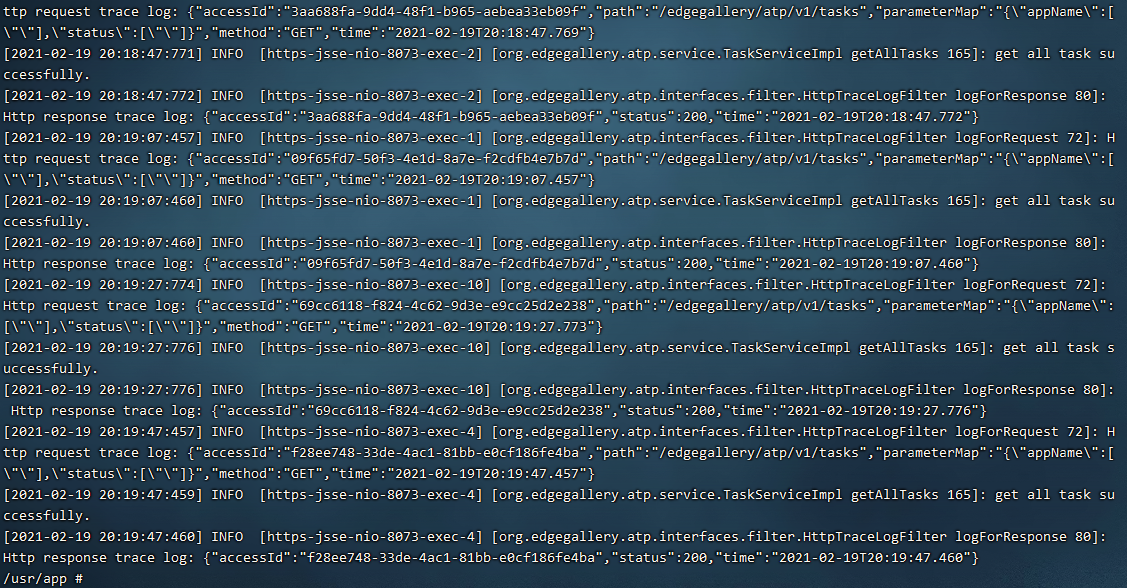
[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

测试方法：进行接口可能的房屋、删除操作，查看日志是否记录。



相关操作均有记录。Ok

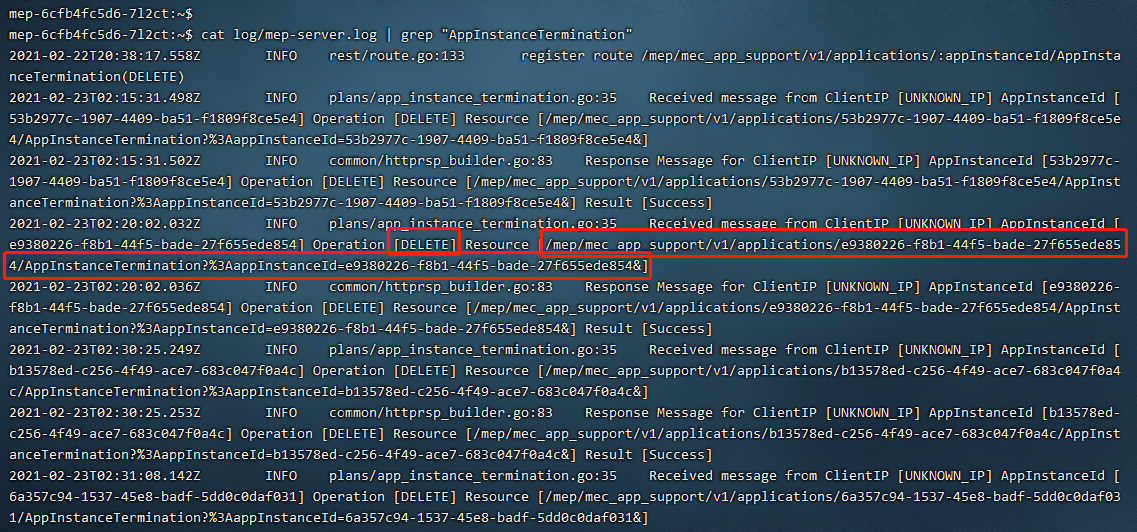
**测试结论**：**PASS**

[【MEP】APP Instance Termination Enhancement](https://gitee.com/OSDT/dashboard?issue_id=I2DQV5)

测试方法：登录mecm，新建applcm、rulemgr、边缘节点。创建部署应用实例。进入mepserver的pod，查看日志记录。

可以看到新增接口，ok

/mep/mec\_app\_support/v1/applications/:appInstanceId/AppInstanceTermination



**测试结论**：**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

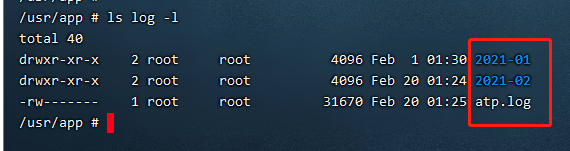
[ATP管理面portal优化](https://gitee.com/OSDT/dashboard?issue_id=I2EC3E)

此条story具体包含2条内容：

1.首页的分析analyz接口；

2.任务管理页面下的批量删除batch\_delete接口。

由于45环境为日构建环境，pod中日志每天会清空。所以在166环境进行查看。可以看到已经按日期分类，避免数据记录过多。Ok



**测试结论**：**PASS**