使用审计中间件

背景

审计中间件是一个Python中间件逻辑，通过粘贴部署过滤器到服务请求处理管道中。审计中间件以CADF格式构造审计事件数据。

审计中间价支持通过oslo消息通知程序功能提供CADF审计事件。根据 *notification_driver*配置，审计事件可以路又道消息传递基础结构（notification_driver = messagingv2）,也可以路由到日志文件（notification_driver = log）。

审计中间件为每一个RESA API交互创建两个事件：一个事件从请求数据中提取信息，一个事件请求结果（即响应）。

启用API请求审核

审计中间件是keystonemiddleware(>=1.6)库的一部分。假设Barbican部署已经使用Keystone进行令牌验证，那么审计支持只需要更改配置即可。它具有oslo消息库依赖性，因为要是改库进行审计事件传递。pyCADF库用来以CADF格式创建事件。

步骤

1. 关闭所有Barbican实例。 2. 将 *api_audit_map.conf*复制到 **/etc/barbican** 目录下 3. 编辑 **/etc/barbican/barbican-api-paste.ini**

将/v1 app管道由 **barbican_api**替换为 **barbican-api-keystone-audit** 管道：

```
    [pipeline:barbican-api-keystone-audit]
    pipeline = authtoken context audit apiapp
```

4.编辑 **barbican.conf**,更新 *notification_driver*值。

5. 重启barbican服务

审计时间样例

如下，是对称密钥创建请求的审计事件样例

```
{
   "priority":"INFO",
   "event_type":"audit.http.request",
   "timestamp":"2015-12-11 00:44:26.412076",
   "publisher_id":"uwsgi",
   "payload":{
      "typeURI":"http://schemas.dmtf.org/cloud/audit/1.0/event",
```

```
      "eventTime":"2015-12-11T00:44:26.410768+0000",
      "target":{
         "typeURI":"service/security/keymanager/secrets",
         "addresses":[
            {
               "url":"http://{barbican_admin_host}:9311",
               "name":"admin"
            },
            {
               "url":"http://{barbican_internal_host}:9311",
               "name":"private"
            },
            {
               "url":"https://{barbican_public_host}:9311",
               "name":"public"
            }
         ],
         "name":"barbican_service_user",
         "id":"barbican"
      },
      "observer":{
         "id":"target"
      },
      "tags":[
         "correlation_id?value=openstack:7e0fe4a6-e258-477e-a1c9-
0fd0921a8435"
      ],
      "eventType":"activity",
      "initiator":{
         "typeURI":"service/security/account/user",
         "name":"cinder_user",
         "credential":{
            "token":"***",
            "identity_status":"Confirmed"
         },
         "host":{
            "agent":"curl/7.38.0",
            "address":"192.168.245.2"
         },
         "project_id":"8eabee0a4c4e40f882df8efbce695526",
         "id":"513e8682f23446ceb598b6b0f5c4482b"
      },
      "action":"create",
      "outcome":"pending",
      "id":"openstack:3a6a961c-9ada-4b81-9095-90968d896c41",
      "requestPath":"/v1/secrets"
   },
   "message_id":"afc3fd93-51e9-4c80-b330-983e66962265"
}
```