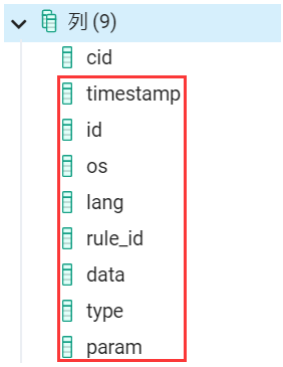
说明

插入数据库中的检查项数据为图中红线框部分：timestamp, id, os, lang, rule_id, data, type, param



	timestamp	id	os	lang	rule_id	data	type	param
类型	timestamp	int	string	string	string	string[]	int	string[]
值	now()	2	'windows10'	'Chinese'			0	
说明	固定值	固定值	固定值	固定值	手动填入	手动填入	固定值	手动填入

四个手动填入的值参考 **windows.xlsx** 文件和**进度表.docx**

注：

- 类型为 string 的需要加单引号（举例：'windows10'）
- 类型为 string[] 的要加单引号和花括号，值之间以逗号隔开（举例：'{"windows10", "debain10"}'）
- data 列中单个项不用加双引号（举例：'{1,AllSigned}'），param 列中单个项需要加双引号（举例：'{"windows10", "debain10"}'）
- string[] 是因为一个检查项可能有多个检查点，即一个 rule_id 对应多个 param 和 data

步骤

1、进度表.docx

有两类检查项：**services** 和**组策略**

- services，一个检查项只有一个检查点
- 组策略，一个检查项可能有多个检查点，更为复杂

2、services

以 **524、Xbox Live Networking Service (XboxNetApiSvc)** 为例

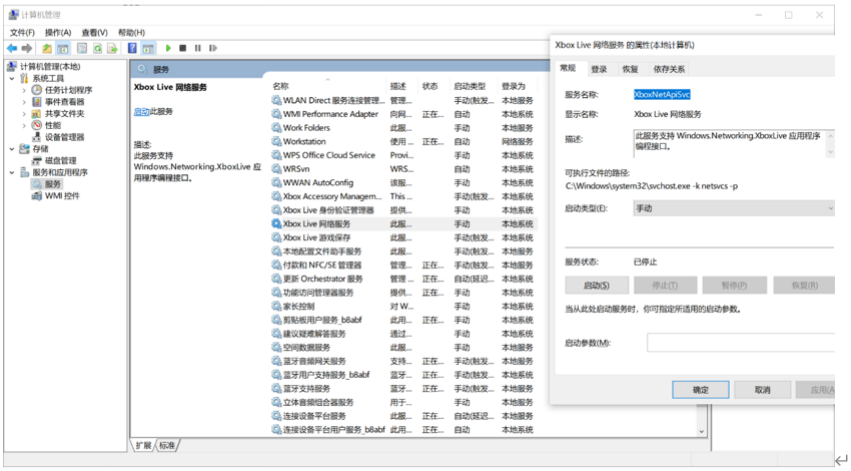
（1）param（string[]）

param 为图中红线框即**检查语句**中 name = 后面的内容，所以第 524 条的 **param 填写 '{"XboxNetApiSvc"}'**

- 524、Xbox Live Networking Service (XboxNetApiSvc)

- 要求

Disable the Service 'Xbox Live Networking Service (XboxNetApiSvc)'



```
osquery> select * from services
   ...> where name = "XboxNetApiSvc";
          name = XboxNetApiSvc
  service_type = SHARE_PROCESS
  display_name = Xbox Live 网络服务
        status = STOPPED
           pid = 0
    start_type = DEMAND_START
 win32_exit_code = 1077
service_exit_code = 0
          path = C:\Windows\system32\svchost.exe -k netsvcs -p
   module_path = C:\Windows\system32\XboxNetApiSvc.dll
   description = 此服务支持 Windows.Networking.XboxLive 应用程序编程接口。
  user_account = LocalSystem
```

关闭服务：status = STOPPED

开启服务：status = RUNNING

- 检查语句

```
select status from services
where name = "XboxNetApiSvc";
```

(2) data（string[]）

data 则看检查结果中的内容，有两种情况，开启（RUNNING）和关闭（STOPPED）：

- 开启（RUNNING），**data 填写 '{1}'**
- 关闭（STOPPED），**data 填写 null**

·检查结果

```
osquery> select status from services
    ...> where name = "XboxNetApiSvc";
status = STOPPED
```

status = STOPPED，则该检查项通过。

(3) rule_id（string）

查看 windows.xlsx 文件，根据最前面的序号找到对应的 Rule ID，如下图所示，第 524 条的 **rule_id 填写 'BL696-0461'**

	A	B	C	D
1	Document Type	Document	Rule ID	Target Audier
2				Asset Managt
3				
523		Security Measure Plan for Microsoft Windows 10	BL696-0946	✓
524		Security Measure Plan for Microsoft Windows 10	BL696-0461	✓
525		Security Measure Plan for Microsoft Windows 10	BL696-0086	✓

(4) 总结

综上所述，第 524 条填入的数据就是：

(now(), 2, 'windows10', 'Chinese', 'BL696_0461', null, 0, '{"Xbox Live 网络服务"}'),

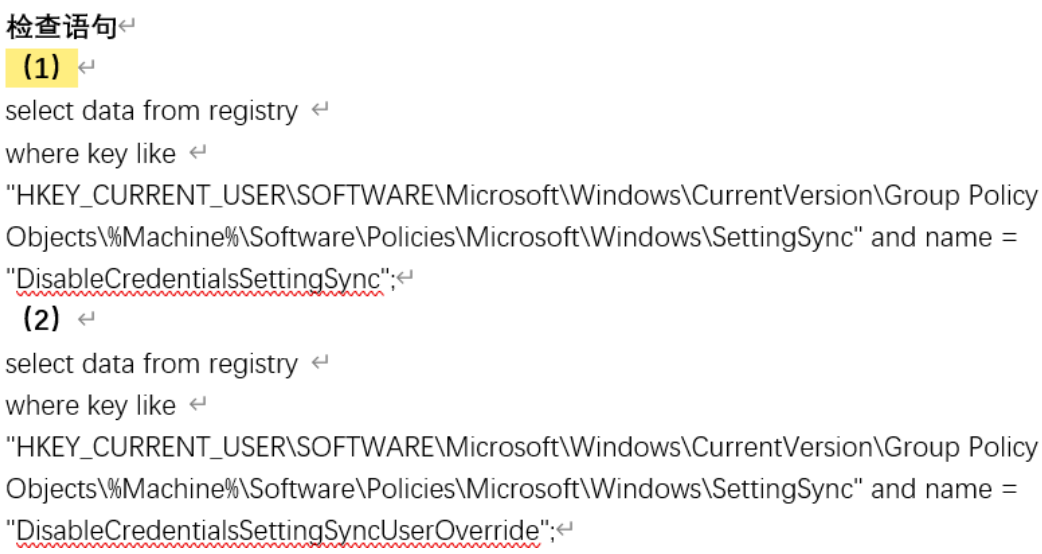
3、组策略

以一个检查项对应多个检查点的 **387、Configure 'Do not sync passwords'** 为例

（1）param（string[]）

param **检查语句**中的内容，可以从图中发现该检查项有两个检查点，每个检查点都包含了 key 和 name 的查询条件，所以 param 由 key 和 name 构成，之间用引号隔开：

- 每个 key 取从 % 开始到结尾的字符串，比如这里两个百分号之间为 Machine，那么去掉百分号，取从 Machine 到结尾的内容，注意**单斜杠 \ 要替换成四个单斜杠 **
- 每个 name 接在 key + 引号之后，直接取 name = 后面的值即可



所以第 387 条的 **param 填写 '{"Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\SettingSync:DisableCredentialsSettingSync", "Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\SettingSync:DisableCredentialsSettingSyncUserOverride"}'**

注：通常多个检查点的 param 中的 key 是一样的，只是 name 不一样，直接复制 key 可以节约时间

（2）data（string[]）

data 是看检查结果中的内容，和上面一样，由于该检查项有两个检查点，所以 data 有多个值，这里取 data = 后面的值即可，所以第 387 条的 **data 填写 '{1, 2}'**

注：无需加双引号

检查结果↵

（1）↵

```
osquery> select data from registry
    ...> where key like
    ...> "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\%Machine%\Software\Policies\M
icrosoft\Windows\SettingSync" and name = "DisableCredentialsSettingSync";
W0223 21:19:36.508044 29948 registry.cpp:528] CURRENT_USER hives are not queryable by osqueryd; query HKEY_USERS with th
e desired users SID instead
 data = 2
```

data = 2，则该检查项通过。↵

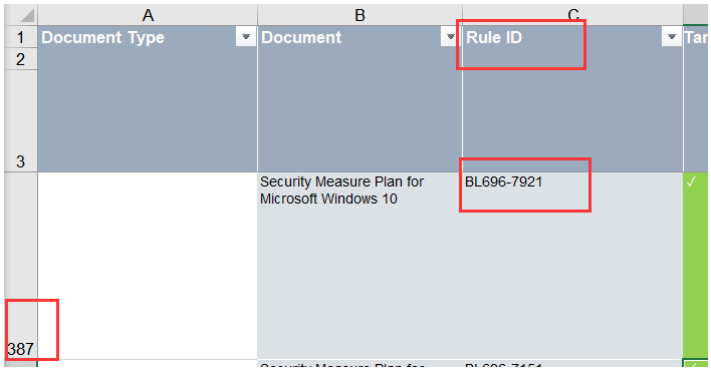
（2）↵

```
osquery> select data from registry
    ...> where key like
    ...> "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\%Machine%\Software\Policies\M
icrosoft\Windows\SettingSync" and name = "DisableCredentialsSettingSyncUserOverride";
W0223 21:20:05.838604 29948 registry.cpp:528] CURRENT_USER hives are not queryable by osqueryd; query HKEY_USERS with th
e desired users SID instead
 data = 1
```

data = 1，则该检查项通过。↵

（3）rule_id（string）

查看 windows.xlsx 文件，根据最前面的序号找到对应的 Rule ID，如下图所示，第 387 条的 **rule_id 填写 'BL696-7921'**



（4）总结

综上所述，第 387 条填入的数据就是：

(now(), 2, 'windows10', 'Chinese', 'BL696-7921', '{1, 2}', 0, '{"Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\SettingSync:DisableCredentialsSettingSync", "Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\SettingSync:DisableCredentialsSettingSyncUserOverride"}'),

检查方式

数据库：PostgreSQL

（1）建库：PG

（2）建表：config

（3）成功按下述配置插入该数据库

配置模板

注：一行一个检查项，以（timestamp, id, os, lang, rule_id, data, type, param）的顺序填入，最后以逗号结尾

```
ALTER TABLE config ALTER COLUMN cid SET default nextval('public.cid');
INSERT INTO config
    (timestamp, id, os, lang, rule_id, data, type, param)
VALUES
    (now(), 2, 'windows10', 'Chinese', 'BL696_0086', '{1}', 0,
'{"Machine\\\\System\\\\CurrentControlSet\\\\Control\\\\SCMConfig:EnableSvchostM
itigationPolicy"}'),
    (now(), 2, 'windows10', 'Chinese', 'BL696_7921', '{1,2}',   0,
'{"Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\PowerShell:EnableS
cripts","Software\\\\Policies\\\\Microsoft\\\\Windows\\\\PowerShell:ExecutionPol
icy"}'),
    (now(), 2, 'windows10', 'Chinese', 'BL696_0461', null,  0,  '{"Xbox Live 网络
服务"}'),
    (now(), 2, 'windows10', 'Chinese', 'BL696-0711', '{1,AllSigned}',   0,
'{"Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\PowerShell:EnableS
cripts","Machine\\\\Software\\\\Policies\\\\Microsoft\\\\Windows\\\\PowerShell:E
xecutionPolicy"}');
```