

APAR : R89170(IV45483)

Problem(Abstract):

The ISIM service groups extracted as permissions with the same value(group attribute mapped to account) used in different service group profiles defined for same service instance extracted as single permission instead of separate permissions.

Cause:

If the same group name is used in different service group profiles for same service then the RaPM Extract tool does not extract the service groups as permissions correctly. In import_Data_Session.csv file, there is single permission entry for those groups with comma separated attribute values instead of different permission entries.

The Permission UID attribute uniquely identifies the permissions. Before the fix of this issue, the "Permission UID" of the service group is generated in the format <Service DN> ::< group attribute mapped to account value>. In the above mentioned issue, the service has more than one group type (more than one group profiles) and the value of group attribute mapped to account is same for two groups of different type. Due to which the Permission UID value of the two groups is same.

Solution:

To fix the issue the Group Object Profile Name (Unique for each group type) is appended to the Permission UID value.

After the fix, in Extract tool the Permission UID will be unique across two group types having same value of group attribute mapped to account. The Permission UID attribute value will be generated in following format.

<Service DN> :: <Group attribute mapped to account>:: <Group Object Profile Name>

As part of defect IV45483, the Extract Utility tool is modified to append the group object profile name to the permission's (service groups extracted as permissions) 'Permission UID' attribute value. If the data is already extracted from IBM Security Identity Manager system and imported in RaPM, prior to applying this patch, then mandatory manual steps needs to be performed to update the existing permission's 'Permission UID' value stored in RaPM database. Please ensure that the data session(s) is in committed state before executing the manual steps.

If the data is already extracted from IBM Security Identity Manager System prior to applying this patch and not imported into RaPM then the mandatory manual steps needs to be performed after importing and committing the data session(s) in RaPM.

Note: The below steps will be required to execute prior to importing the new data files generated using an updated Extract tool (after this fix).

As per the default configuration of the Extract utility configuration 'ExtractConfig' file, the attribute usage related to display specified for attributes 'Identity Manager attribute-Resources', 'Identity Manager attribute-Permission Assignment Type' is '<Usage>PermissionDisplay1</Usage>' and '<Usage>PermissionDisplay2</Usage>' respectively. So if user has changed the attribute usage related to display for above mentioned attributes then please modify the "Update_Permission_UID_DB2.sql" or "Update_Permission_UID_Oracle.sql" file as follows.

For example :

If attribute usage related to display specified for attribute 'Identity Manager attribute-Resources' is '<Usage>PermissionDisplay2</Usage>'

and for attribute 'Identity Manager attribute-Permission Assignment Type' is

'<Usage>PermissionDisplay3</Usage>' then modified .sql files contents will be as follows:

The modified 'Update_Permission_UID_DB2' file contents will be as follows:

```
UPDATE PERMISSION SET PERMISSION_URI = PERMISSION_URI || ':' || PERMISSION_CUSTOM_ATTR2
where PERMISSION_CUSTOM_ATTR2 IS NOT NULL and PERMISSION_CUSTOM_ATTR2 <> " and
PERMISSION_CUSTOM_ATTR2 != 'SystemRole' and PERMISSION_CUSTOM_ATTR3 IS NOT NULL and
PERMISSION_CUSTOM_ATTR3 <> " and PERMISSION_CUSTOM_ATTR3 != 'System';
commit;
```

The modified 'Update_Permission_UID_Oracle' file contents will be as follows:

```
UPDATE PERMISSION SET PERMISSION_URI = PERMISSION_URI || ':' || PERMISSION_CUSTOM_ATTR2
where PERMISSION_CUSTOM_ATTR2 IS NOT NULL and PERMISSION_CUSTOM_ATTR2 != 'SystemRole'
and PERMISSION_CUSTOM_ATTR3 IS NOT NULL and PERMISSION_CUSTOM_ATTR3 != 'System';
commit;
```

Execute the below steps only once.

Updating the Permission UID in DB2 database:

1. Unzip the IV45483.zip to a temporary directory (say, TEMP).
2. As a DB2 instance owner, connect to the RaPM database by typing this command:
db2 connect to <RaPM Database Name> user <db2admin_name> using <db2admin_password>
3. To update the DB2 database table type this command:

Microsoft Windows operating system:

```
db2 -tf "<TEMP>\Update_Permission_UID_DB2.sql"
```

UNIX, Linux, or AIX operating systems:

```
db2 -tf "<TEMP>/Update_Permission_UID_DB2.sql"
```

4. Run this command to disconnect from the database:

```
db2 disconnect all
```

Updating the Permission UID in Oracle database:

1. Unzip the IV45483.zip to a temporary directory (say, TEMP).
2. Run this command from the command prompt: sqlplus /nolog
3. Connect to the RaPM database by typing this command:
connect <oracleadminuser>/<Oracleadminpassword>@<databasename>
4. To update the DB2 database table type this command:

Microsoft Windows operating system:

SQL> @"<TEMP>\Update_Permission_UID_Oracle.sql"

UNIX, Linux, or AIX operating systems:

SQL> @"<TEMP>/Update_Permission_UID_Oracle.sql"

5. Run this command to disconnect from the database:

SQL> disconnect

Results:

The Permission UID values stored in RaPM database are updated in the format

<Service DN> :: <Group attribute mapped to account>:: <Group Object Profile Name>