Point in Time Auditing

Grouper 2.0+ has point in time auditing. The feature is enabled automatically when upgrading. The general design is to keep separate tables for many of the regular Grouper database tables that have start and end times associated with each row. This allows you to perform efficient queries to find out the state of the data at any point in time or range.

The point in time tables are populated by the change log processor that runs every minute (by default) by the Grouper loader. The point in time tables are also used for flattened notifications of memberships, privileges, and permissions.

If you need just an audit log of high level user actions, you may want to know about User Auditing.

With point in time auditing, you can do the following queries at a single time in the past or for a date range.

- Determine if a person was a member of a group.
- Get all the members of a group.
- Find out what groups a person was a member.
- Find what permissions a person had.
- Get all the attributes assigned to an object (group, etc).
- Get the values that an attribute had.

The following Grouper Web Services support point in time queries.

- Get Members
- hasMember
- getGroups
- getPermissionAssignments

If you have old objects in your point in time data that you don't want anymore, you can delete them using GSH. See edu.internet2.middleware.grouper.pit.PITUtils for various options for deleting old data. Note that point in time data can only be deleted after the actual objects have been deleted and those deletions have been processed by the changeLogTempToChangeLog job, which runs once a minute by default with the Grouper Daemon.

```
gsh 0% // delete objects that ended before a given date
gsh 0% edu.internet2.middleware.grouper.pit.PITUtils.deleteInactiveRecords(new Date(), true);
gsh 1%
gsh 2% // delete objects that have ended below a given stem
gsh 2% edu.internet2.middleware.grouper.pit.PITUtils.deleteInactiveObjectsInStem("test", true)
```

If your need to sync your point in time data, you can run the following to make sure all of the objects currently active in Grouper are marked as active in point in time. It's probably a good idea to turn off the Grouper Daemon when you run this.

```
gsh 0% new edu.internet2.middleware.grouper.misc.SyncPITTables().syncAllPITTables()


Searching for missing active point in time fields
Found 0 missing active point in time fields


Searching for missing active point in time members
Found 0 missing active point in time members


Searching for missing active point in time stems
Found 0 missing active point in time stems


Searching for missing active point in time groups
Found 0 missing active point in time groups


Searching for missing active point in time role sets
Found 0 missing active point in time role sets


Searching for missing active point in time attribute defs
Found 0 missing active point in time attribute defs
```

```
Searching for missing active point in time attribute def names
Found 0 missing active point in time attribute def names


Searching for missing active point in time attribute def name sets
Found 0 missing active point in time attribute def name sets


Searching for missing active point in time actions
Found 0 missing active point in time actions


Searching for missing active point in time action sets
Found 0 missing active point in time action sets


Searching for missing active point in time group sets
Found 0 missing active point in time group sets


Searching for missing active point in time memberships
Found 0 missing active point in time memberships


Searching for missing active point in time attribute assigns
Found 0 missing active point in time attribute assigns


Searching for missing active point in time attribute assign values
Found 0 missing active point in time attribute assign values


Searching for point in time attribute assign values that should be inactive
Found 0 active point in time attribute assign values that should be inactive


Searching for point in time attribute assigns that should be inactive
Found 0 active point in time attribute assigns that should be inactive


Searching for point in time memberships that should be inactive
Found 0 active point in time memberships that should be inactive


Searching for point in time group sets that should be inactive
Found 0 active point in time group sets that should be inactive


Searching for point in time action sets that should be inactive
Found 0 active point in time action sets that should be inactive


Searching for point in time actions that should be inactive
Found 0 active point in time actions that should be inactive


Searching for point in time attribute def name sets that should be inactive
Found 0 active point in time attribute def name sets that should be inactive


Searching for point in time attribute def names that should be inactive
Found 0 active point in time attribute def names that should be inactive


Searching for point in time attribute defs that should be inactive
Found 0 active point in time attribute defs that should be inactive


Searching for point in time role sets that should be inactive
```

```
Found 0 active point in time role sets that should be inactive


Searching for point in time groups that should be inactive
Found 0 active point in time groups that should be inactive


Searching for point in time stems that should be inactive
Found 0 active point in time stems that should be inactive


Searching for point in time members that should be inactive
Found 0 active point in time members that should be inactive


Searching for point in time fields that should be inactive
Found 0 active point in time fields that should be inactive
java.lang.Long: 0
gsh 1%
```

Example query

Find members in a group on a certain point in time. First generate the millis (times 100) of the point in time (or multiple)

```
import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Date;



public class Temp {

  /**
   * @param args
   */
  public static void main(String[] args) throws Exception {
    DateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd kk:mm");

    String dateString = "2013/07/21 12:00";
    Date date = dateFormat.parse(dateString);
    System.out.println(dateString + ": " + 1000 * date.getTime());

    dateString = "2013/07/22 12:00";
    date = dateFormat.parse(dateString);
    System.out.println(dateString + ": " + 1000 * date.getTime());

    dateString = "2013/07/23 12:00";
    date = dateFormat.parse(dateString);
    System.out.println(dateString + ": " + 1000 * date.getTime());

  }

}
```

That will print the millis times 1000

```
2013/07/21 12:00: 1374422400000000
2013/07/22 12:00: 1374508800000000
2013/07/23 12:00: 1374595200000000
```

Execute a SQL query against the point in time tables using the id path of the group to find the members on a certain point in time

```
select gpg.name, gpf.name, gpm.subject_id, gpm.subject_source, gpmav.membership_start_time, gpmav.
membership_end_time
from
  grouper_pit_memberships_all_v gpmav,
  grouper_pit_members gpm,
  grouper_pit_fields gpf,
  grouper_pit_groups gpg
where
  gpmav.member_id = gpm.id
  and gpm.subject_source = 'pennperson'
  and gpmav.owner_group_id = gpg.id
  and gpg.name = 'penn:sas:service:mailing_list:staff:permanent_staff:list'
  and gpmav.field_id = gpf.id
  and (gpmav.membership_start_time is null or gpmav.membership_start_time < 1374595200000000)
  and (gpmav.membership_end_time is null or gpmav.membership_end_time > 1374595200000000 )
```

Find where org groups are used outside of the org folder from a day a few days ago (day is hard-coded)

```
select gpg.name, gpf.name, gpg_member.name, gpmav.membership_start_time, gpmav.membership_end_time
from
  grouper_pit_groups gpg_member,
  grouper_pit_memberships_all_v gpmav,
  grouper_pit_members gpm,
  grouper_pit_fields gpf,
  grouper_pit_groups gpg
where
  gpmav.member_id = gpm.id
  and gpf.name = 'members'
  and gpm.subject_source = 'g:gsa'
  and gpm.subject_id = gpg_member.source_id
  and gpg_member.name like 'penn:community:employee:org%'
  and gpmav.owner_group_id = gpg.id
  and gpg.name not like 'penn:community:employee%'
  and gpmav.field_id = gpf.id
  and (gpmav.membership_start_time is null or gpmav.membership_start_time < 1364270400000000)
  and (gpmav.membership_end_time is null or gpmav.membership_end_time > 1364270400000000 )
```

Find subjects in a group from a certain day, excluding some

```
select gpg.name, gpm.subject_id
from
  grouper_pit_memberships_all_v gpmav,
  grouper_pit_fields gpf,
  grouper_pit_groups gpg,
  grouper_pit_members gpm
where
  gpm.subject_source != 'g:gsa'
  and gpmav.member_id = gpm.id
  and gpm.subject_id not in ('10094590', '10037375', '10033223')
  and gpg.name like 'penn:community:employee:org:TOPU%'
  and gpg.name not like '%_rolluporg_systemOfRecordAndIncludes'
  and gpg.name not like '%systemOfRecord'
  and gpg.name not like '%_personorg'
  and gpg.name not like '%_rolluporg'
  and gpmav.owner_group_id = gpg.id
  and gpf.name = 'members'
  and gpmav.field_id = gpf.id
  and (gpmav.membership_start_time is null or gpmav.membership_start_time < 1364270400000000)
  and (gpmav.membership_end_time is null or gpmav.membership_end_time > 1364270400000000 )
  ;
```

Find attribute assignments for a certain provisioning target

```
select gpadn_metadata.name, gpaav_metadata.value_string, gpaa_metadata.end_time
from grouper_pit_attribute_assign gpaa_marker, grouper_pit_attribute_assign gpaa_target,
grouper_pit_attribute_assign gpaa_do_provision, grouper_pit_attribute_assign gpaa_metadata,
grouper_pit_attr_assn_value gpaav_target, grouper_pit_attr_assn_value gpaav_do_provision,
grouper_pit_attr_assn_value gpaav_metadata,
grouper_pit_attr_def_name gpadn_marker, grouper_pit_attr_def_name gpadn_target, grouper_pit_attr_def_name
gpadn_do_provision, grouper_pit_attr_def_name gpadn_metadata,
grouper_attribute_def_name gadn_marker, grouper_attribute_def_name gadn_target, grouper_attribute_def_name
gadn_do_provision,
grouper_pit_groups gpg
where gpg.name = 'test:testGroup8' and gpaa_marker.owner_group_id = gpg.id
and gadn_marker.name = 'penn:etc:provisioning:provisioningMarker' and gpadn_marker.source_id = gadn_marker.id
    and gpaa_marker.attribute_def_name_id = gpadn_marker.id
and gadn_target.name = 'penn:etc:provisioning:provisioningTarget' and gpadn_target.source_id = gadn_target.id
    and gpaa_target.attribute_def_name_id = gpadn_target.id and gpaa_target.owner_attribute_assign_id =
gpaa_marker.id
        and gpaav_target.attribute_assign_id = gpaa_target.id and gpaav_target.value_string =
'myGoogleGroupsProvisioner'
and gadn_do_provision.name = 'penn:etc:provisioning:provisioningDoProvision' and gpadn_do_provision.source_id =
gadn_do_provision.id
    and gpaa_do_provision.attribute_def_name_id = gpadn_do_provision.id and gpaa_do_provision.
owner_attribute_assign_id = gpaa_marker.id
        and gpaav_do_provision.attribute_assign_id = gpaa_do_provision.id and gpaav_do_provision.value_string =
'true'
and gpaa_metadata.attribute_def_name_id = gpadn_metadata.id and gpaa_metadata.owner_attribute_assign_id =
gpaa_marker.id
        and gpaav_metadata.attribute_assign_id = gpaa_metadata.id
```

Find groups which are in a certain folder and have not been edited since a certain time (micros)

```
select gg.name from grouper_groups gg where gg.name like 'test:%'
and not exists (select 1 from
  grouper_pit_memberships_lw_v gpmlv,
  grouper_pit_fields gpf,
  grouper_pit_groups gpg
where
  gpmlv.owner_group_id = gpg.id
  and gpg.name like gg.name
  and gpmlv.field_id = gpf.id
  and gpf.name = 'members'
  and (gpmlv.membership_start_time > 1703764800000000
    or gpmlv.membership_end_time > 1703764800000000 ))
```