

Grouper rules pattern - Inherited privileges on attribute definitions

Wiki Home	Grouper Release Announcements	Grouper Guides	Grouper Deployment Guide	Community Contributions	Internal Developer Resources
---------------------------	---	--------------------------------	--	---	--

Grouper rules

If an attributeDef is created under folder a:b, then apply privileges to the attributeDef of attrRead,attrUpdate to group a:security:admins

You should use the inherited privileges screen to control this. This rule is added to the folder where attributes are created.

Configure rule for v5+

Home > Root > test2

test2

Show details ▾

Folder contents Privileges More ▾

Edit folder

Folder actions ▾

Folder rules Rules actions ▾

Documentation

Rule pattern Inherited privileges on attribute definitions *
Type of rule that solves an existing use case with a certain action, condition, and result.

Subject id or identifier test:test1 *
Generally put the group name of the group to assign privileges to. Or you can input a subject id or identifier.

Privileges to add attrRead, attrUpdate *
Comma separated attribute definition privileges: attrAdmin, attrOptin, attrOptout, attrRead, attrUpdate, attrView, attrDefAttrRead, attrDefAttrUpdate

Folder scope All groups in this folder or subfolders *
Select 'All' for everything in this folder and subfolders (most common). Otherwise, it only applies to objects directly in this folder.

Subject source Grouper: Internal Source Adapter (g:isa) *
Generally pick g:isa to input the group name. Or pick any other source.

Run daemon override
If the rule has the ability to be run by daemon (for example to clean up data corruption), then you can set this to false if you do not want the daemon to run for this rule. If the rule does not have the ability to run in the daemon then this setting is ignored.

Save Cancel

Configure rule for v4 and previous

Java example

```

//add a rule on stem2 saying if you create a group underneath, then assign a reader group
AttributeAssign attributeAssign = stem2
    .getAttributeDelegate().addAttribute(RuleUtils.ruleAttributeDefName()).getAttributeAssign();

AttributeValueDelegate attributeValueDelegate = attributeAssign.getAttributeValueDelegate();

attributeValueDelegate.assignValue(
    RuleUtils.ruleActAsSubjectSourceIdName(), "g:isa");
attributeValueDelegate.assignValue(
    RuleUtils.ruleActAsSubjectIdName(), "GrouperSystem");
attributeValueDelegate.assignValue(
    RuleUtils.ruleCheckTypeName(), RuleCheckType.attributeDefCreate.name());

//can be SUB or ONE for if in this folder, or in this and all subfolders
attributeValueDelegate.assignValue(
    RuleUtils.ruleCheckStemScopeName(), Stem.Scope.SUB.name());
attributeValueDelegate.assignValue(
    RuleUtils.ruleThenEnumName(), RuleThenEnum.assignAttributeDefPrivilegeToAttributeDefId.name());

//this is the subject string for the subject to assign to
//e.g. sourceId ::::: subjectIdentifier
//or sourceId ::: subjectId
//or ::: subjectId
//or sourceId ::::: subjectIdOrIdentifier
//etc
attributeValueDelegate.assignValue(
    RuleUtils.ruleThenEnumArg0Name(), "g:gsa ::::: stem1:admins");

//can be: attrRead, attrUpdate, attrView, attrAdmin, attrOptin, attrOptout
attributeValueDelegate.assignValue(
    RuleUtils.ruleThenEnumArg1Name(), "attrRead,attrUpdate");

//should be valid
String isValidString = attributeValueDelegate.retrieveValueString(
    RuleUtils.ruleValidName());

if (!StringUtils.equals("T", isValidString)) {
    throw new RuntimeException(isValidString);
}

```

GSH shorthand method

```

RuleApi.inheritAttributeDefPrivileges(SubjectFinder.findRootSubject(), stem2, Scope.SUB, groupA.toSubject(),
Privilege.getInstances("attrRead, attrUpdate"));

```

GSH test case

```

gsh 0% grouperSession = GrouperSession.startRootSession();
edu.internet2.middleware.grouper.GrouperSession: ad1415e66401474880e1322c250aa0fb, 'GrouperSystem', 'application'
gsh 1% stem2 = new edu.internet2.middleware.grouper.StemSave(grouperSession).assignName("stem2").
assignCreateParentStemsIfNotExist(true).save();
stem: name='stem2' displayName='stem2' uuid='f76ea3ea4ebc4b28a3a7ce650def5c8a'
gsh 2% groupA = new GroupSave(grouperSession).assignName("stem1:admins").assignCreateParentStemsIfNotExist
(true).save();
group: name='stem1:admins' displayName='stem1:admins' uuid='f10fdb4776484c94a4196c2c858eb9fb'
gsh 3% addMember("stem1:admins", "test.subject.0");
true
gsh 4% subjectActAs = SubjectFinder.findByIdAndSource("GrouperSystem", "g:isa", true);
subject: id='GrouperSystem' type='application' source='g:isa' name='GrouperSysAdmin'
gsh 5% RuleApi.inheritAttributeDefPrivileges(subjectActAs, stem2, Stem.Scope.SUB, groupA.toSubject(), Privilege.
getInstances("attrRead, attrUpdate"));
gsh 6% attributeDefB = new AttributeDefSave(grouperSession).assignName("stem2:b").
assignCreateParentStemsIfNotExist(true).save();
edu.internet2.middleware.grouper.attr.AttributeDef: AttributeDef[name=stem2:b,
uuid=960b452a59494a5c9a393906903b6b1b]
gsh 7% hasPriv("stem2:b", "test.subject.0", Privilege.getInstance("attrRead"))
true
gsh 8% hasPriv("stem2:b", "test.subject.0", Privilege.getInstance("attrUpdate"))
true
gsh 9% attributeDefD = new AttributeDefSave(grouperSession).assignName("stem3:d").
assignCreateParentStemsIfNotExist(true).save();
edu.internet2.middleware.grouper.attr.AttributeDef: AttributeDef[name=stem3:d,
uuid=6545585416004e52a49535efba1fe1b0]
gsh 10% hasPriv("stem3:d", "test.subject.0", Privilege.getInstance("attrRead"))
false
gsh 11% hasPriv("stem3:d", "test.subject.0", Privilege.getInstance("attrUpdate"))
false
gsh 12% attributeDefC = new AttributeDefSave(grouperSession).assignName("stem2:sub:c").
assignCreateParentStemsIfNotExist(true).save();
edu.internet2.middleware.grouper.attr.AttributeDef: AttributeDef[name=stem2:sub:c,
uuid=405cfab803524de59fca1e93218aa9d6]
gsh 13% hasPriv("stem2:sub:c", "test.subject.0", Privilege.getInstance("attrRead"))
true
gsh 14% hasPriv("stem2:sub:c", "test.subject.0", Privilege.getInstance("attrUpdate"))
true

```

GSH daemon

Run the above GSH code, then continue below

```

gsh 15% revokePriv("stem2:sub:c", "test.subject.0", Privilege.getInstance("attrUpdate"))
false
gsh 16% status = GrouperLoader.runOnceByJobName(grouperSession, GrouperLoaderType.GROUPER_RULES);
loader ran successfully: Ran rules daemon, changed 0 records
gsh 17% hasPriv("stem2:sub:c", "test.subject.0", Privilege.getInstance("attrUpdate"))
true

```

sdf