



HOWTO Integrate MediaWiki with Grouper on Ubuntu Linux 12.04

19 November 2014

Author: Marco Malavolti, Andrea Biancini

Index

1) Introduction.....	3
2) Requirements.....	3
3) Installation.....	4
4) Install and Configure Shibboleth plugin for MediaWiki.....	5
5) Add the MediaWiki groups to Grouper.....	8
6) Add new MediaWiki groups and link them to Grouper.....	13
7) How to prevent the access to an user.....	16
8) How to protect wiki with a lazy session.....	16
9) Bibliography.....	17

1 Introduction

This is a tutorial for users that want integrate the authentication for a MediaWiki site with Grouper on an Service Provider based on Ubuntu Linux 12.04.

2 Requirements

- A machine with Grouper installed and configured.
- A Shibboleth SP (sp.example.it) with Apache2 Web Server, PHP 5.3.2 or later and MySQL 5.0.2 or later.
- MediaWiki plugin

3 Installation

Install and Configure MediaWiki on your Service Provider

1. Install the software requirements for MediaWiki on your SP:

- sudo su -
- apt-get install apache2 mysql-server php5-mysql phpmyadmin php5-intl php-apc

2. Install MediaWiki on your SP:

- sudo su -
- cd /usr/local/src
- wget http://releases.wikimedia.org/mediawiki/1.23/mediawiki-1.23.6.tar.gz
- tar xzf mediawiki-1.23.6
- mv mediawiki-1.23.6 /var/www
- vim /etc/apache2/sites-available/mediawiki.conf :

```
<IfModule mod_alias.c>
    Alias /wiki /var/www/mediawiki-1.23.6/
<Directory /var/www/mediawiki-1.23.6/>
    Options Indexes MultiViews FollowSymLinks
    Order deny,allow
    Allow from all
</Directory>
</IfModule>
```

- a2ensite mediawiki.conf ; service apache2 reload
- mysql -u root -p (type your mySQL root password to access)
 - create database wikidb;
 - grant index, create, select, insert, update, delete, alter, lock tables on wikidb.* to 'wikiuser'@'localhost' identified by '##wikiuserPassword_CHANGE_ME##';
 - flush privileges;
 - quit

3. Configure MediaWiki on your SP:

- Open the page “<https://sp.example.it/wiki/mw-config/index.php>” and follow the instructions until the end.
- Download the “**LocalSettings.php**” file and put it into the MediaWiki directory (/var/www/mediawiki-1.23.6/)

4 Install and Configure Shibboleth plugin for MediaWiki

The following instruction is based on the page:

<http://www.mediawiki.org/wiki/Extension:Shibboleth.Authentication>

1. Configure Shibboleth SP to support the MediaWiki authentication plugin:

- vim /etc/shibboleth/shibboleth2.xml

```
<Host name="sp.example.it">
  <Path name="wiki" authType="shibboleth" requireSession="false"/>
</Host>

...

<SessionInitiator type="Chaining" Location="/DS" id="DS" relayState="cookie"
isDefault="true">
  <SessionInitiator type="SAML2" acsIndex="1" template="bindingTemplate.html"/>
  <SessionInitiator type="Shib1" acsIndex="5"/>
  <SessionInitiator type="WAYF" acsIndex="5" URL="https://dsc.example.it/DS"/>
</SessionInitiator>
```

- shibd -t /etc/shibboleth/shibboleth2.xml
- service shibd restart

2. Edit the apache2 wiki configuration to support the Shibboleth authentication:

- vim /etc/apache2/sites-enabled/mediawiki.conf:

```
<IfModule mod_alias.c>
  Alias /wiki /var/www/mediawiki-1.23.6/

  <Directory /var/www/mediawiki-1.23.6/>
    Options Indexes MultiViews FollowSymLinks
    Order deny,allow
    Allow from all
  </Directory>

  <Location /wiki>
    AuthType shibboleth
    ShibRequireSession On
    require entitlement urn:mace:garr.it:wiki
  </Location>
</IfModule>
```

(This rules require apache 2.4 and Shibboleth SP software v2.4.3.

If you use a Shibboleth SP release >= 2.5.1, please, use this:

```
<Location /wiki>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require shib-attr entitlement urn:mace:garr.it:wiki
</Location>
)
```

3. Copy the extension code provide by [THIS PAGE](#) into
`/var/www/mediawiki-1.23.6/extensions/ShibAuthPlugin.php`
4. Modify the “`/var/www/mediawiki-1.23.6/LocalSettings.php`” by adding these lines:

```
# The following permissions were set based on your choice in the installer
$wgGroupPermissions['*']['edit'] = false;

# Add more configuration options below.

// Shibboleth Authentication Stuff
// Load ShibAuthPlugin
require_once('extensions/ShibAuthPlugin.php');

// Last portion of the shibboleth WAYF url for lazy sessions.
// This value is found in your shibboleth.xml file on the setup for your SP
// WAYF url will look something like: /Shibboleth.sso/WAYF/$shib_WAYF
$shib_WAYF = "DS";

// Are you using an old style WAYF (Shib 1.3)
// or new style Discover Service (Shib 2.x)?
// Values are WAYF or DS, defaults to WAYF
$shib_WAYFStyle = "DS";

// Is the assertion consumer service located
// at an https address (highly recommended)
// Default for compatibility with previous version: false
$shib_Https = true;

// Prompt for user to login
$shib_LoginHint = "Login via Single Sign-on";

// Where is the assertion consumer service located on the website?
// Default: "/Shibboleth.sso"
$shib_ASSERTIONConsumerServiceURL = "/Shibboleth.sso";

// Map Real Name to what Shibboleth variable(s)?
# $shib_RN = ucfirst(strtolower($_SERVER['HTTP_FIRST_NAME'])) . ' '
#     . ucfirst(strtolower($_SERVER['HTTP_LAST_NAME']));
$shib_RN = $_SERVER['cn'];

// Map e-mail to what Shibboleth variable?
$shib_email = $_SERVER['mail'];

// Field containing groups for the user
if (array_key_exists("isMemberOf", $_SERVER)) {
    $shib_groups = $_SERVER['isMemberOf'];
}

//This value must match with the FolderID of Wiki on the Grouper instance
$shib_group_prefix = "wiki";
```

```
// The ShibUpdateUser hook is executed on login.
// It has two arguments:
// - $existing: True if this is an existing user, false if it is a new user being
added
// - &$user: A reference to the user object.
//           $user->updateUser() is called after the function finishes.
// In the event handler you can change the user object, for instance set the email
address or the real name
// The example function shown here should match behavior from previous versions of
the extension:

$wgHooks['ShibUpdateUser'][] = 'ShibUpdateTheUser';

function ShibUpdateTheUser($existing, $user) {
    global $shib_email;
    global $shib_RN;
    if (! $existing) {
        if($shib_email != null)
            $user->setEmail($shib_email);
        if($shib_RN != null)
            $user->setRealName($shib_RN);
    }
}

// This is required to map to something
// You should beware of possible namespace collisions, it is best to chose
// something that will not violate MW's usual restrictions on characters
// Map Username to what Shibboleth variable?
$shib_UN = ucfirst(strtolower($_SERVER['eppn']));

// Shibboleth doesn't really support logging out very well. To take care of
// this we simply get rid of the logout link when a user is logged in through
// Shib. Alternatively, you can uncomment and set the variable below to a link
// that will either clear the user's cookies or log the user out of the Idp and
// instead of deleting the logout link, the extension will change it instead.
$shib_logout = "/Shibboleth.sso/Logout";

//Add to permit the management of the User rights
$wgUserrightsInterwikiDelimiter = '#';

// Activate Shibboleth Plugin
SetupShibAuth();
```

5. Modify the value “**protected mRemember**” to “**var mRemember**” into the “/var/www/mediawiki-1.23.6/includes/specials/SpecialUserlogin.php” file.
6. Modify the “**attribute-filter.xml**” of your Identity Provider and restart its Tomcat server to release the attributes “**commonName**”, “**eduPersonPrincipalName**” and “**mail**” to this SP.

5 Add the MediaWiki groups to Grouper

1. Open Grouper application, log-in as Admin and create the folder for the WiKi (“WiKi of MediaWiki” with Folder ID = “**wiki**”) under the relying party’s folder:

The screenshot shows the Grouper application's 'New folder' creation interface. On the left, there's a sidebar with 'Quick links' for 'My groups', 'My folders', 'My favorites', 'My services', 'Admin UI', and 'Lite UI'. Below that is a 'Browse folders' section showing a tree structure: 'Root' is expanded to show 'Grouper Administration', 'QS University of Bristol', and 'SPhost for GN3+'. The main area is titled 'New folder' and contains fields for creating a new folder. The 'Create in this folder' field is set to 'SPhost for GN3+'. The 'Folder name' field is 'Wiki of MediaWiki'. The 'Folder ID' field is 'wiki', with a checked checkbox next to it labeled 'Edit the ID'. A note below says 'ID is the unique identifier for this folder. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.' The 'Description' field contains 'Brief description of Wiki'. A note below it says 'Description contains notes about the folder, which could include: what the folder represents, why it was created, etc.' At the bottom are 'Save' and 'Cancel' buttons.

2. Create the “service” folder into the “**wiki**” folder and add to it these groups:

- a) authorized group:
 - Name: **auhtorized**
 - ID: **authorized**
 - Description: **Group used to identify the users that are authorized to use the Wiki**
- b) eligible group:
 - Name: **eligible**
 - ID: **eligible**
 - Description: **Group used to identify the users that are eligible to use the Wiki**
- c) blocked group:
 - Name: **blocked**
 - ID: **blocked**
 - Description: **Group used to identify the users that are blocked when they try to use the Wiki**

3. Make the “**authorized**” group a composite group that involves “**eligible**” and “**blocked**” groups:

The screenshot shows the Grouper web interface. The left sidebar has sections for Quick links (My groups, My folders, My favorites, My services, Admin UI, Lite UI), Browse folders (Root, Grouper Administration, QS University of Bristol, SPhost for GN3+), and a Create new group button. The main content area shows the 'authorized' group details. The title is 'authorized' with a user icon. Below it is a description: 'Group used to identify the users that are authorized to use the Wiki'. A 'More' dropdown menu is open, showing options like Add members, More actions, Add to my favorites, Join group, Copy group, Delete group, Edit group, **Edit composite** (which is highlighted in blue), Move group, Export members, Import members, Remove all members, View audit log, and Admin UI. Below the description is a table titled 'The following table lists all entities which are members of this group.' with columns Entity name and Membership. A filter for 'All members' and a member name search input are present. The table shows 0 results. At the bottom, there are buttons for Show: 50 and Showing 1-0.

The screenshot shows the 'Edit group composite' configuration for the 'authorized' group. The left sidebar is identical to the previous screenshot. The main content area has a title 'Edit group composite' with a user icon. It contains fields for 'Composite': 'Yes' (radio button selected), 'First factor group': 'SPhost for GN3+:Wiki of MediaWiki:service:eligible' (with a note to search for the first factor), 'Operation': 'not (complement)' (with a note about three composite operations: intersection, complement, and union), and 'Second factor group': 'SPhost for GN3+:Wiki of MediaWiki:service:blocked' (with a note to search for the second factor). At the bottom are 'Save' and 'Cancel' buttons.

4. Add the group designed to contain the users that are blocked on all services hosted by the SP to the “**blocked**” group:

The screenshot shows the Grouper web interface. On the left, there's a sidebar with 'Quick links' (My groups, My folders, My favorites, My services, Admin UI, Lite UI) and 'Browse folders' (Root, Grouper Administration, QS University of Bristol, SPhost for GN3+). The main content area is titled 'blocked'. It shows a search bar with 'Member name or ID: SPhost for GN3+:service.quickdisable' and a note to 'Enter an entity name or ID, or [search for an entity](#)'. Below it, there are options to 'Assign these privileges:' (radio buttons for Default privileges and Custom privileges), an 'Add' button, and a link to 'import a list of members'. A note says 'Group used to identify the users that are blocked when they try to use the Wiki'. There's a 'More' dropdown menu with tabs for 'Members', 'Privileges', and 'More'. Below this, a table header reads 'The following table lists all entities which are members of this group.' with columns for 'Entity name' and 'Membership'. At the bottom, there are filters for 'Filter for: All members', 'Member name', 'Apply filter', 'Reset', and a 'Show: 50' dropdown. A note at the bottom right says 'Showing 1-0 of 0 - First | Prev | Next | Last'.

5. Into the main “**wiki**” folder create these new groups:

a) Administrators Group:

- Name: **Administrators Group**
- ID: **sysop**
- Description: **Brief description of Administrators Group**

b) Bureaucrats Group:

- Name: **Bureaucrats Group**
- ID: **bureaucrat**
- Description: **Brief description of Bureaucrats Group**

c) Users Group:

- Name: **Users Group**
- ID: **user**
- Description: **Brief description of Users Group**

(each ID value matches with the default groups of MediaWiki software and stored into its DB)

6. Add the new groups created to the “eligible” group of “wiki”, for example:

The screenshot shows the Grouper web interface. On the left, there's a sidebar with 'Quick links' for 'My groups', 'My folders', 'My favorites', 'My services', 'Admin UI', and 'Lite UI'. Below that is a 'Browse folders' section with 'Root' expanded, showing 'Grouper Administration', 'QS University of Bristol', and 'SPhost for GN3+'. The main content area is titled 'eligible'. It has a 'Member name or ID:' input field containing 'SPhost for GN3+:Wiki of MediaWiki:Administrators Group'. There's a search bar below it. Under 'Assign these privileges:', the 'Default privileges' radio button is selected. A 'More' dropdown menu is open. At the bottom, there's a table showing membership details with columns for 'Entity name' and 'Membership', and a note indicating 1-0 of 0 members.

7. Add the members that you want elevate to administrators of Wiki to the *Administrators Group* and to *Bureaucrats Group*. For Example:

The screenshot shows the Grouper web interface. The sidebar and navigation are identical to the previous screenshot. The main content area is titled 'Administrators Group'. It has a 'Member name or ID:' input field containing 'Name Surname'. There's a search bar below it. Under 'Assign these privileges:', the 'Default privileges' radio button is selected. A 'More' dropdown menu is open. At the bottom, there's a table showing membership details with columns for 'Entity name' and 'Membership', and a note indicating 1-0 of 0 members.

8. Try to access into the Wiki and navigate through the special pages to understand if your user is administrator or not.
If you are Administrator of the Wiki, you can find the page “**User Rights Management**” between the special pages.

6 Add new MediaWiki groups and link them to Grouper

1. Modify the “/var/www/mediawiki-1.23.6/LocalSettings.php” by adding these lines:

```
// New GN3+ group and its permissions
$wgGroupPermissions['GN3+']['move'] = true;
$wgGroupPermissions['GN3+']['move-subpages'] = true;
$wgGroupPermissions['GN3+']['move-rootuserpages'] = false;
$wgGroupPermissions['GN3+']['movefile'] = true;
$wgGroupPermissions['GN3+']['read'] = true;
$wgGroupPermissions['GN3+']['edit'] = true;
$wgGroupPermissions['GN3+']['createpage'] = true;
$wgGroupPermissions['GN3+']['createtalk'] = true;
$wgGroupPermissions['GN3+']['writeapi'] = false;
$wgGroupPermissions['GN3+']['upload'] = true;
$wgGroupPermissions['GN3+']['reupload'] = true;
$wgGroupPermissions['GN3+']['reupload-shared'] = true;
$wgGroupPermissions['GN3+']['minoredit'] = true;
$wgGroupPermissions['GN3+']['purge'] = false;
$wgGroupPermissions['GN3+']['sendemail'] = false;

// Activate Shibboleth Plugin
SetupShibAuth();
```

(Each line defines each permission that the “GN3+” group will have. See the MediaWiki User Rights [2])

2. Move on your Grouper instance and:

a) Create this new GN3+ group under the “**wiki**” folder:

- Name: **GN3+ Group**
- ID: **GN3+**
- Description: **Brief description of GN3+ Group**

(the value of “ID” must match with the name of the new MediaWiki group)

The screenshot shows the 'New group' creation interface in the Grouper web application. The left sidebar has 'Create new group' at the top, followed by 'Quick links' with options like 'My groups', 'My folders', 'My favorites', 'My services', 'Admin UI', and 'Lite UI'. Below that is 'Browse folders' with a tree view showing 'Root' expanded, containing 'Grouper Administration', 'QS University of Bristol', 'SPhost for GN3+', 'Secure Application', 'service', and 'Wiki of MediaWiki'. The main right panel has a title 'New group' and a breadcrumb 'Home > New group'. It contains fields for 'Create in this folder:' (set to 'SPhost for GN3+:Wiki of MediaWiki'), 'Group name:' (set to 'GN3+ Group'), 'Group ID:' (set to 'GN3+' with a checked checkbox for 'Edit the ID'), and 'Description:' (set to 'Brief description of GN3+ Group'). A note below the description field says 'Description contains notes about the group, which could include: what the group represents, why it was created, etc.' At the bottom are 'Save' and 'Cancel' buttons.

- b) Add the members that you want to be part of this new GN3+ group.

The screenshot shows the 'GN3+ Group' configuration page. On the left, there's a sidebar with 'Quick links' to 'My groups', 'My folders', 'My favorites', 'My services', 'Admin UI', and 'Lite UI'. Below that is a 'Browse folders' section showing a tree structure: Root > SHost for GN3+ > Wiki of MediaWiki. The 'Wiki of MediaWiki' folder is selected. The main content area has a title 'GN3+ Group' with a 'GN3+' icon. It includes fields for 'Member name or ID:' (with a search bar), 'Assign these privileges:' (radio buttons for 'Default privileges' and 'Custom privileges'), and a button to 'Add' or 'import a list of members'. A brief description field and a 'More' dropdown are also present. At the bottom, there's a table showing member entities, with columns for 'Entity name' and 'Membership'. The table shows three entries: Administrators Group, Bureaucrats Group, and Users Group, all with 'Direct' membership. There are buttons for 'Remove selected members', 'Filter for:', 'Apply filter', and 'Reset'.

- c) Add the new “GN3+” group to the “eligible” group under “service” folder:

The screenshot shows the 'eligible' group configuration page. The sidebar and folder structure are identical to the previous screenshot. The main content area has a title 'eligible' with a 'GN3+' icon. It includes fields for 'Member name or ID:' (with a search bar), 'Assign these privileges:' (radio buttons for 'Default privileges' and 'Custom privileges'), and a button to 'Add' or 'import a list of members'. A brief description field and a 'More' dropdown are also present. At the bottom, there's a table showing member entities, with columns for 'Entity name' and 'Membership'. The table shows three entries: Administrators Group, Bureaucrats Group, and Users Group, all with 'Direct' membership. There are buttons for 'Remove selected members', 'Filter for:', 'Apply filter', and 'Reset'.

3. Access to the Wiki and navigate through the special page “**User group rights**” and find the new MediaWiki group called “**GN3+**”.
4. Verify that the GN3+ group has all its members by open the link called “(*list of members*)”.

7 How to prevent the access to an user

1. Add the user that you want block to the “**blocked**” group on the Grouper instance.
2. After that, when the user will try to access on the Wiki, he will meet the **401 Unauthorized** error page.

8 How to protect wiki with a lazy session

1. Modify the “**mediawiki.conf**”:

- vim /etc/apache/site-enabled/mediawiki.conf:

```
<IfModule mod_alias.c>
  Alias /wiki /var/www/mediawiki-1.23.6/

  <Directory /var/www/mediawiki-1.23.6/>
    Options Indexes MultiViews FollowSymLinks
    Order deny,allow
    Allow from all
  </Directory>

  <Location /wiki>
    AuthType shibboleth
    require shibboleth
  </Location>

  <Location /wiki/login.php>
    AuthType shibboleth
    ShibRequireSession On
    require entitlement urn:mace:garr.it:wiki
  </Location>
</IfModule>
```

2. Create the “**login.php**” file:

```
<?php
$target = isset($_GET['target']) ? $_GET['target'] : '/';
header('Location: '.$target);
die();
?>
```

3. Modify the “**LocalSettings.php**” into this way:

```
$shib_WAYFStyle = "CustomLogin";
...
$shib_ASSERTIONConsumerServiceURL = $wgScriptPath."/login.php";
```

9 Bibliography

- [1] MediaWiki: <https://www.mediawiki.org/wiki/MediaWiki>
- [2] MediaWiki User Rights: http://www.mediawiki.org/wiki/Manual:User_rights