How to AD and LDAP configuration

Contents

This page reviews AD and LDAP configuration and integration.

1.0 Introduction to Authentication

GroundWork Monitor supports single sign-on authentication through an external authentication source. Authentication services can be provided by Microsoft Active Directory or through a standards-compliant LDAP server. Most user accounts need not be defined in GroundWork Monitor a priori. User accounts must still be assigned system-specific roles and privileges, and the use of LDAP for authentication changes the way this is done. Configuring the GroundWork JBoss Portal for LDAP allows user passwords and other details such as role membership to be managed by the external directory service. User accounts and roles are synchronized with the GroundWork JBoss Portal when the user logs in, and users are assigned a default role as well as any roles they are members of in LDAP.

It is also possible to enable LDAPS, or LDAP over SSL, as well as many other alternate configurations. Please see the reference materials for JBoss LDAP configuration available here if you would like to study the various options and customize your LDAP setup with GroundWork Monitor. GroundWork Monitor 6.4 introduced Single Sign-on (JOSSO), which entails additional security for applications managed by the portal, and thus requires a few additional steps for configuration when using LDAP.

This how-to goes through an example of setup, configuration, and assignment of users to roles in the context of users and groups that are managed by LDAP. The following sections outline some important points before you start, requirements and options, and then describes an example of configuring GroundWork Monitor for Microsoft Active Directory authentication. LDAP configuration is similar and is described in a subsequent example.

2.0 Active Directory and LDAP Configuration

2.1 Important Points Before You Start

- LDAP users cannot be assigned to roles using the portal administrator application
- LDAP users do not need to be defined in the portal (this is different from GroundWork Monitor 5.x)
- Configuration of LDAP parameters is done outside of the UI and requires a restart of gwservices.
- User passwords are never synchronized from LDAP to the GroundWork Monitor portal database
- A default webservices user wsuser account is maintained in LDAP. If you plan to change the password for this user, you will need to change it in LDAP
- Any LDAP user who needs to access the GroundWork Monitor portal needs to be part of Authenticated group in LDAP/AD in addition to the regular GroundWork Monitor groups such as GWAdmin, GWOperator and GWUser. If not, the user may get an unauthorized HTTP 403 error when they try to login to GroundWork Monitor.
- GroundWork Monitor must be configured with the LDAP server name, a user name and password to bind to LDAP, and the specific container or organizational unit containing the users to be allowed access.
- The bind user will need browse and search permissions for the locations in LDAP where the users and groups are stored
- These values must be input into an XML configuration file in a specific location, and the GroundWork Monitor portal must be restarted for the configuration to take effect.
- If your LDAP server is down for some reason, you can revert the GroundWork authentication mechanism back to the GroundWork database. In this case, stock user accounts can be used to login to the portal. Also the passwords for stock user accounts will be the last changed password before switching to LDAP. You would edit the file:

  ```
  /usr/local/groundwork/josso-1.8.4/lib/josso-gateway-config.xml
  ```

  and replace:

  ```
  <s:import resource="josso-gateway-ldap-stores.xml" />
  ```

  with:

  ```
  <s:import resource="josso-gateway-gatein-stores.xml" />
  ```

2.2 Requirements and Options

- (Required) Active Directory domain controller to which you have administrative access
- (Required) Account with rights to browse the container in which you store the users. Example **ldapauth**, context:

```
cn=ldapauth,ou=GWUsers,dc=demo,dc=com
```

- (Optional) Roles in the portal for desired access levels
- (Optional) A container and groups set up to match roles in the portal
- (Useful) adsiedit.msc utility

2.2.1 Web Service Security

As mentioned above, web services are secured using a **webservices** proxy user **wsuser** by default. This user is managed in AD LDAP.

- The user name and password used are stored in the file:

```
/usr/local/groundwork/config/ws_client.properties
```

- The default user name is **wsuser** and is a member of the **GWwsuser** group
- Keep in mind that changing the Web Services user name or changing the password for the default **wsuser** requires an update of the **ws_client.properties** file. You should restart **gwservices** if you modify this file.

2.2.2 Portal Proxy User

The portal proxy user is used to access API's of applications secured by the portal. You can either use an existing user or create a new one. If you do change from the default, you must add this user to the LDAP system you are using to synchronize from. Make sure that the user is member of **GWUser** .The login ID and password in LDAP always has to match the entries for the proxy user settings in the **/usr/local/groundwork/config/foundation.properties** file. You should restart **gwservices** if you modify this file.

```
portal.proxy.user=user
portal.proxy.password=password
```

2.2.3 GDMA Auto Register User

The **gdma** auto register user is used to access the Foundation API. You can either use an existing user or create a new one. If you do change from the default, you must add this user to the LDAP system you are using to synchronize from. Make sure that the user is a member of the **gdma** group in LDAP. The login ID and password in LDAP must always match the entries for the **Auto_Register_User** setting in the gdma client's **gdma_auto.conf** file.

2.2.4 Recommended LDAP Setup

Portal access authentication is controlled by **Role** permissions. Users gain access to different sections of the portal through role membership. In LDAP, group membership is used to map Role membership in GroundWork Monitor. In order to manage roles in GroundWork Monitor you should setup a new context (an Organizational Unit in AD by default) for the GroundWork Monitor roles.

Example: GWRoles (OU=GWRoles)

To this monitoring specific context add the following **Groups**. With this setup only GroundWork monitoring specific roles will be synchronized even if the user is member of other groups in different contexts (containers). This avoids crowding the GroundWork Monitor administration pages with roles unrelated to monitoring. You can then add company specific groups to the **GWRoles** context, which you can use to define specific access rights in GroundWork Monitor. When a user logs in, **Groups** in the **GWRoles** context of which the user is member of will be synchronized with **Roles** in the portal.

- GWRoot
- GWAdmin
- GWOperator
- GWUser
- Authenticated
- GWwsuser

3.0 Integration with OpenLDAP Directory

3.1 Configuration Steps

1. Before changing the authentication method the portal should be stopped using the following command. All users will be logged out, so be sure to do this in a downtime window:

```
service groundwork stop gwservices
```

2. To enable Active Directory or LDAP authentication, login to the command line as root or equivalent, and modify:

```
/usr/local/groundwork/josso-1.8.4/lib/josso-gateway-config.xml
```

   Replacing:

```
<s:import resource="josso-gateway-gatein-stores.xml" />
```

   with the following and saving the file:

```
<s:import resource="josso-gateway-ldap-stores.xml" />
```

3. Edit the following file with your appropriate LDAP/AD properties. You will be replacing **ldapservername** with the resolvable hostname or IP address of your LDAP server, **Administrator** with the user name of your LDAP user (authorized to browse the containers where your users are), **password** with that users password, and the **cn=XXX** names with those appropriate for your AD system.

```
/usr/local/groundwork/josso-1.8.4/lib/josso-gateway-ldap-stores.xml
```

   For example, if your domain is demo.com and following the recommendations above, you might;

   - Set securityPrincipal="cn=Administrator,dc=demo,dc=com" to use the Administrator user in the Users container to be able to browse the AD tree.
   - Set usersCtxDN="ou=Users,dc=demo,dc=com" to be able to see all the users in the default location.
   - Set rolesCtxDN="ou=Groups,dc=demo,dc=com" if you set up the OU, and added the groups GWAdmin, GWOperator, GWUser, and GWRoot, as recommended.

```
<ldap-istore:ldap-bind-store
            id="josso-identity-store"
            initialContextFactory="com.sun.jndi.ldap.LdapCtxFactory"
            providerUrl="ldap://@ldapservername@"''
securityPrincipal="cn=Administrator,dc=demo,dc=com"
            securityCredential="password"
            securityAuthentication="simple"
            ldapSearchScope="SUBTREE"
            usersCtxDN="ou=Users,dc=demo,dc=com"
            principalUidAttributeID="uid"
            uidAttributeID="member"
            rolesCtxDN="ou=Groups,dc=demo,dc=com"
            roleAttributeID="cn"
            updateableCredentialAttribute="userPassword"
            userPropertiesQueryString="givenName=firstname,sn=lastname,mail=mail"
            />
```

4. Now, start the GroundWork Monitor portal with the following command. At this point, all the users in the **Groups OU** should be able to log in. If they are not members of a group named the same as a role in the portal, they will be mapped to the default **GWUser** role. This allows them essentially view-only access to the portal screens, including the status viewer. The groups they are members of in the **GWRoles OU** will be created as roles in the portal if they do not already exist, and you may proceed to grant access to pages for these roles in the usual way. If users are members of the **GWOperator** group, they will have access to **Event Console** and **Nagios** screens, as well as the **Actions** menus in the **Status** screen. If they are members of the **GWAdmin** group, they will have administrative access to the **GroundWork Monitor** portal. Note that only the **Portal Admin** user will be able to set up shared dashboards with portlet preferences that are inherited by other users.

```
service groundwork start gwservices
```

4.0 Integration with Microsoft Active Directory

By default, the Active Directory system places all users into a container defined by the system as **cn=Users,dc=<myorganization>,dc=<com>**. Where **<myorganization>** is specific to the domain name of your implementation and **<com>** is the typical default suffix. For instance, if the Active Directory domain is **groundworkers.com**, the users would be stored in;

```
cn=Users,dc=groundworkers,dc=com
```

Through the Active Directory administration tool an administrator can add Organizational Units (OU), which are functionally the same as Containers (CN) to organize Roles. The distinction between Container and Organizational Unit is important when configuring the portal for LDAP, since if you specify a **CN** in the file in GroundWork Monitor, but create an **OU** in Active Directory, it will not find the Container and login will fail to assign roles correctly. It's easy to see the difference;

- The configuration entry for a Container uses the CN prefix:

```
rolesCtxDN="CN=GWRoles,dc=demo,dc=com"
```

- While for an Organizational Unit the prefix is OU:

```
rolesCtxDN="OU=GWRoles,dc=demo,dc=com"
```

When you use the Active Directory Users and Computers tool and create new objects, the only container you can create is an **OU**, so the latter of the above formats is the one to use.

Setting the **SynchronizeRoles** option to **true** will set up this role in GroundWork Monitor automatically when the first Active Directory user logs in. This is the recommended configuration, as it will make management transparent. If you decide not to use SynchronizeRoles, you will need to create any roles you wish to have the users be members of in GroundWork Monitor, and manually match the names of these roles to the group names in Active Directory.

The default role all users are assigned to is **GWUser**, so you can create a group called **GWUser** in Active Directory, and place users to whom you wish to grant default access to GroundWork Monitor into this group.

Similarly, if you wish to designate operators or administrators from among the Active Directory users, you should create groups named **GWOperator** and **GWAdmin**, and add your users to these groups. It is recommended that you place these groups in an alternate organizational unit (see above for Recommended LDAP Setup section).

In previous versions of GroundWork Monitor, the default role names were *Admin, Operator,* and *User*. These generic names often conflicted with default group names in Active Directory, and so they were changed as of GroundWork Monitor 6.2. If you are using a system upgraded from before 6.2 to 6.2 or later, you must change the group names in Active Directory, and add new roles to the GroundWork Monitor portal to match the Group names. The **GWAdmin** role (formerly *Admin*) is special, and you can't grant the same rights to another role. Please use the **GWAdmin** role for your administrative users. If you need to have this role name changed, please contact GroundWork Support.

This example assumes that you have created the organizational unit **GWUsers**, and that you have added your users to groups in this **OU**.

4.1 Configuration Steps

1. Before changing the authentication method the portal should be stopped by issuing the following command. All users will be logged out, so be sure to do this in a downtime window:

```
service groundwork stop gwservices
```

2. To enable Active Directory or LDAP authentication, log in to the command line as root or equivalent, and modify:

```
/usr/local/groundwork/josso-1.8.4/lib/josso-gateway-config.xml
```

Replace the following section:

```
<s:import resource="josso-gateway-gatein-stores.xml" />
```

with:

```
<s:import resource="josso-gateway-ldap-stores.xml" />
```

3. Save the file.
4. Edit the following file with your appropriate LDAP/AD properties:

```
/usr/local/groundwork/josso-1.8.4/lib/josso-gateway-ldap-stores.xml
```

You will be replacing the ldapservername with the resolvable hostname or IP address of your LDAP server, Administrator with the user name of your LDAP user (authorized to browse the containers where your users are), password with that users password, and the cn=XXX names with those appropriate for your AD system. For example, if your domain is demo.com, following the recommendations above you might:

- Set securityPrincipal="cn=ldapauth,cn=Users,dc=demo,dc=com" to use the ldapauth user in the Users container to be able to browse the AD tree
- Set usersCtxDN="CN=Users,dc=demo,dc=com" to be able to see all the users in the default location
- Set rolesCtxDN="OU=GWRoles,dc=demo,dc=com" if you set up the OU, and added the groups GWAdmin, GWOperator, GWUser, and GWRoot, as recommended

> ⚠ The rolesCtxDN="OU=GWRoles,dc=demo,dc=com" is an OU, not a CN in Active Directory.

```
<ldap-istore:ldap-bind-store
id="josso-identity-store"
initialContextFactory="com.sun.jndi.ldap.LdapCtxFactory"
providerUrl="ldap://server:389"
securityPrincipal="cn=Administrator,cn=Users,dc=demo,dc=com"
securityCredential="password"
securityAuthentication="simple"
ldapSearchScope="SUBTREE"
usersCtxDN="CN=Users,dc=demo,dc=com"
principalUidAttributeID="sAMAccountName"
uidAttributeID="member"
rolesCtxDN="OU=GWRoles,dc=demo,dc=com"
roleAttributeID="sAMAccountName"
credentialQueryString="uid=sAMAccountName"
userPropertiesQueryString="mail=mail,cn=description"
/>
```

5. Save the file.
6. Run as **root**:

```
service groundwork start gwservices
```

At this point, all the users in the **GWRoles OU** should be able to log in. If they are not members of a group named the same as a role in the portal, they will be mapped to the default **GWUser** role. This allows them essentially view-only access to the portal screens, including the status viewer. The groups they are members of in the **GWRoles OU** will be created as roles in the portal if they do not already exist, and you may proceed to grant access to pages for these roles in the usual way.

- If they are members of the **GWOperator** group, they will have access to **Event Console** and **Nagios** screens, as well as the **Actions** menus in the **Status** screen.
- If they are members of the **GWAdmin** group, they will have administrative access to the **GroundWork** portal.

Only the **root** user within the **GWRoot** membership can create shared dashboards with portlet preferences that are inherited by other users.