GWME-7.1.1-13 - LDAP Fix Where Group has Empty Alias or Description Field

Problem

GroundWork 7.1.1 LDAP is not happy with AD which includes groups where certain attributes like "description" or "alias" include empty values. These groups are often some in the AD tree that coincidentally contain the GW users, and do not have to be the GW groups, they are just associated with the user who is logging in to GW using LDAP.

The error manifests itself by the symptom that the user does not get the default start page, as he does not have any GW role recognized and so will see a 403 error "unauthorized". In the framework log the login sequence comes to the point where you would expect a list of authorized roles and instead you see *.

Solution

Apply the attached patch to upgrade to a version of the LDAP aggregator which accepts corrupted AD records without falling over. Such group names will be ignored. Of course if the group with the corrupted field is a GW Role then the code will ignore it and the user will not have that role's capabilities in the portal.

> ⚠ You must have applied TB7.1.1-11 before you may apply TB7.1.1-13.

Installation

1. Download the patch file tar archive

Name	Size	Creator	Creation Date	Comment
TB7.1.1-13.LDAP-Empty-Alias-Fix.tgz	56 kB	Hans Kriel	Jun 08, 2018 11:11	md5sum 48f746e4a3b07d36de65a53936d46ed6

2. Decompress the install script and files and run the install script. They will appear in subdirectory `TB7.1.1-12.tomcat-6.0.53`.

```
tar xvf TB7.1.1-13.LDAP-Empty-Alias-Fix.tgz
cd TB7.1.1-13.LDAP-Empty-Alias-Fix
./TB7.1.1-13_install.sh
```

You can see a list of patches and installation logs at:

```
/usr/local/groundwork/common/var/patches/
```

In the event that you had **not** previously installed TB7.1.1-11 this patch will exit. As noted above you are required to apply that patch first.

Uninstallation

1. Run the uninstall script, and respond to the prompts.

```
./TB7.1.1-13_uninstall.sh
```

The patch directory will be updated to reflect the restoration of the files and uninstall steps. Note that uninstall will revert to the prepatched state.

Notes

We tested this patch with LDAP and with LDAPs.

Basic testing of LDAP against both AD servers validated LDAP and LDAPs were both working. For LDAPs, if the certificates are not valid you may add the following two lines to the GroundWork server ldap.conf file to ensure that it could get past the cert issue:

```
TLS_CACERTDIR /usr/local/groundwork/common/openssl/certs/
TLS_REQCERT never
```

Make sure to encrypt the LDAPs password with **single quotes** around the password to ensure that password was encrypted with special characters correctly.

After basic LDAP testing, we added a new group to the GWRoles OU in the DC. We called the group "test" and added gw-admin to the group. The framework.log file (see attached) shows that the new role mapping is seen. The new role is seen and the lack of role mapping in ldap-mapping file is noted.

We then changed the LDAP settings to match role on "description" instead of "sAMAccountName" to replicate issues customers see when matching role on other field than our default "sAMAcoountName".
We verified that LDAP mappings were still working. We removed the description for the "test" role to see that processing still works and the role is simply skipped if it doesn't have a description (matching up to the original test failure case).

We completed testing by removing the values in /usr/local/groundwork/config/josso-gateway-ldap-stores.xml and moving those values to /usr/local/groundwork/foundation.properties as (example):

core.security.ldap.config.server_type = AD
core.security.ldap.config.provider_url = ldaps://<SERVERNAME>:636
core.security.ldap.config.security_principal = cn=BINDUSER,cn=Users,dc=gwostechlab,dc=com
core.security.ldap.config.security_credential = ENCRYPTEDPASSWORD
core.security.ldap.config.users_ctx_dn = cn=Users,dc=gwostechlab,dc=com
core.security.ldap.config.roles_ctx_dn = ou=GWRoles,dc=gwostechlab,dc=com
core.security.ldap.config.role_attribute_id = description

We tested users with and without test role and with and without description field populated in test role.

Logging

Refer to these tech notes to increase the logging level should you have trouble or wish to validate:
https://kb.groundworkopensource.com/display/STAFF/standalone.xml+settings
https://kb.groundworkopensource.com/display/STAFF/Changing+log+level+in+GroundWork+7.x+without+restarting+Portal

Take special note to add these levels which are relevant:
1. DEBUG must be enabled on the file handler
2. DEBUG must be set on the com.groundwork.core.security.GroundworkJbossLoginModule logger
3. DEBUG must be set on the com.groundwork.core.security logger

or, #3 can be:
3. DEBUG must be set on the com.groundwork.core.security.ldap.LDAPAggregator logger
but it renders setting com.groundwork to DEBUG less than effective
since the default ERROR level is more specific

duplicates should be avoided in the file

there is no assurance of order when loading XML