SSSD AD GPO Regression Tests

1 Introduction

This manual describes the required proceeding to perform regression and non-regression tests for the SSSD AD GPO patches in https://pagure.io/SSSD/sssd/pull-request/3320.

Following settings are used by this specification and need to be adapted to the real test environment:

AD domain	mydomain.local
AD domain controller	TACITUS (tacitus.mydomain.local)
AD domain administrator	administrator
Test user name	adgpo.testuser
Test user UID	1999
Test user SID	S-1-5-21-1961322486-2366424238-2351687912-1138
Test machine	SCIPIO (scipio.mydomain.local)

2 Preparation of Test Environment

2.1 Create Windows/Unix test user for AD GPO Tests

On the Samba 4 AD DC create domain user “adgpo.testuser” by entering the following command.

```
sudo samba-tool user create adgpo.testuser --given-name "Test User" --surname
 "SSSD" --nis-domain mydomain --login-shell /bin/bash --unix-home /tmp --
 description "Test user for SSSD AD GPO handling" --uid-number=1999 --gid-
 number=513
```

Please replace “mydomain” by the correct NIS domain name and choose a UID number of your choice. For further information execute the following command on the AD DC and check the values for your domain (controller):

```
kinit administrator
ldapsearch -Y GSSAPI -H ldap://tacitus.mydomain.local -b
 cn=ypservers,cn=ypServ30,cn=RpcServices,cn=system,DC=mydomain,DC=local
 "(objectClass=msSFU30DomainInfo)"
```

Check for correct creation of the test user:

a) On SSSD workstation:

```
getent passwd adgpo.testuser
getent group "Domain Users"
```

b) On Samba AD DC

```
kinit administrator
```

```
ldapsearch -Y GSSAPI -H ldap://tacitus.mydomain.local -b DC=mydomain,DC=local
 "(uidNumber=1999)"
```

Check that the user can logon onto the SSSD AD test workstation.

After successful creation of user *adgpo.testuser* retrieve the user's SID, which is required for the group policy objects:

```
sudo wbinfo -U 1999
S-1-5-21-1961322486-2366424238-2351687912-1138
```

2.2 Create Group Policy Objects

The following steps are all performed on the Samba AD DC:

1. Unpack the provided policy templates into a folder of your choice:

```
tar -xzf SeInteractiveLogonRight.tgz
tar -xzf SeDenyInteractiveLogonRight.tgz
tar -xzf SeAllowDenyInteractiveLogonRight.tgz
```

2. Replace the user's SID (S-1-5-21-1961322486-2366424238-2351687912-1138) in file GptTmpl.inf of all three provided GPO templates with the one fetched in chapter 2.1.

3. Create Group Policy Objects and note the returned GPO unique IDs:

```
sudo samba-tool gpo create "AD GPO Test - Allow Login" -U administrator
-->  {8F712A4D-52C5-419F-A34C-CA760EF1599B}
sudo samba-tool gpo create "AD GPO Test - Deny Login" -U administrator
-->  {D63716E9-43CB-4708-AD5C-DEB5355B6CDB}
sudo samba-tool gpo create "AD GPO Test - Allow/Deny Login" -U administrator
-->  {F77CA036-26E4-43FA-92F3-8342FA960EEA}
sudo samba-tool gpo create "AD GPO Test - Deny Login (MACHINE)" -U administrator
-->  {F50AB220-5160-4236-8E07-7B58574FF259}
```

4. Copy the content of the GPOs into the GPO folders:

```
sudo cp -r SeInteractiveLogonRight/*
 /var/lib/samba/sysvol/mydomain.local/Policies/\{8F712A4D-52C5-419F-A34C-
 CA760EF1599B\}
sudo cp -r SeDenyInteractiveLogonRight/*
 /var/lib/samba/sysvol/mydomain.local/Policies/\{D63716E9-43CB-4708-AD5C-
 DEB5355B6CDB\}
sudo cp -r SeAllowDenyInteractiveLogonRight/*
 /var/lib/samba/sysvol/mydomain.local/Policies/\{F77CA036-26E4-43FA-92F3-
 8342FA960EEA\}
sudo cp -r SeDenyInteractiveLogonRight/*
 /var/lib/samba/sysvol/mydomain.local/Policies/\{F50AB220-5160-4236-8E07-
 7B58574FF259\}
```

5. Rename folder Machine of GPO "AD GPO Test - Deny Login (MACHINE)" to upper case letters:

```
sudo mv /var/lib/samba/sysvol/mydomain.local/Policies/\{F50AB220-5160-4236-
 8E07-7B58574FF259\}/Machine
 /var/lib/samba/sysvol/mydomain.local/Policies/\{F50AB220-5160-4236-8E07-
 7B58574FF259\}/MACHINE
```

6. Complete GPO attributes:
   Add gPCMachineExtensionNames and set GPO status flag to disable user settings.

   For each GPO

   - Replace the GPO unique ID within the provided LDIF file gPCMachineExtensionNames.ldif with the GPO's unique ID (see above)
   - Run ldapmodify:

     ```
     ldapmodify -Y GSSAPI -H ldap://tacitus.mydomain.local -f
      gPCMachineExtensionNames.ldif
     ```

7. Check GPO ACLs:

   ```
   sudo samba-tool gpo aclcheck -U administrator
   ```

8. Fix sysvol ACLs to ensure access to the GPO settings:

   ```
   sudo samba-tool ntacl sysvolreset
   ```

9. Retrieve a list of the created GPOs and their settings:

   ```
   sudo samba-tool gpo show {8F712A4D-52C5-419F-A34C-CA760EF1599B} -U
    administrator
   sudo samba-tool gpo show {D63716E9-43CB-4708-AD5C-DEB5355B6CDB} -U
    administrator
   sudo samba-tool gpo show {F77CA036-26E4-43FA-92F3-8342FA960EEA} -U
    administrator
   sudo samba-tool gpo show {F50AB220-5160-4236-8E07-7B58574FF259} -U
    administrator
   ```

2.3 Create GPO Test Container

Create a special test container in the active directory for linking of GPOs to the SSSD test machine:

1. Adapt DN within the provided LDIF file *SSSDTestServerContainer.ldif*

2. Add container to AD:

   ```
   ldapadd -Y GSSAPI -H ldap://tacitus.mydomain.local -f
    SSSDTestServerContainer.ldif
   ```

3 Test Preparation

3.1 Move SSSD test server/workstation into the special test container

Check current container (DN) of the SSSD test machine and temporarily move it to the new GPO container created above. This guarantees, that only the GPOs to be tested are applicable to the test machine and that other domain members are not affected by the tested changes of login policies.

1. Adapt DN within the provided LDIF file *SSSDTestServerModDN.ldif*

2. Move SSSD test machine to the special test container

   ```
   ldapmodify -Y GSSAPI -H ldap://tacitus.mydomain.local -f
    SSSDTestServerModDN.ldif
   ```

3. Check for existing GPO links of the container, where the SSSD test server/workstation is stored:

```
sudo samba-tool gpo getlink "OU=SSSD Test Servers,DC=mydomain,DC=local"
```

4. Remove unwanted GPO (links) that manage interactive logons rights

4 Regression Testing

4.1 Test 1 - Allow Login

Note: Replace the GPO unique ID by the one retrieved in chapter 2.2.

1. Link GPO to the container, where the SSSD test server/workstation is stored:

```
sudo samba-tool gpo setlink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {8F712A4D-52C5-419F-A34C-CA760EF1599B} -U administrator
```

2. On the test machine flush the SSSD cache:

```
sudo sss_cache -E
```

3. Check login of adgpo.testuser and other users

Expected result:

Login of adgpo.testuser succeeds, login of all other users will fail in enforce mode or create a warning in the system log:

```
Warning: user would have been denied GPO-based logon access if the
 ad_gpo_access_control option were set to enforcing mode.
```

4. Delete GPO link

```
sudo samba-tool gpo dellink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {8F712A4D-52C5-419F-A34C-CA760EF1599B} -U administrator
```

4.2 Test 2 – Deny Login

Note: Replace the GPO unique ID by the one retrieved in chapter 2.2.

1. Link GPO to the container, where the SSSD test server/workstation is stored:

```
sudo samba-tool gpo setlink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {D63716E9-43CB-4708-AD5C-DEB5355B6CDB} -U administrator
```

2. On the test machine flush the SSSD cache:

```
sudo sss_cache -E
```

3. Check login of adgpo.testuser and other users

Expected result:

Login of adgpo.testuser fails in enforce mode or creates a warning in the system log:

```
Warning: user would have been denied GPO-based logon access if the
 ad_gpo_access_control option were set to enforcing mode.
```

Login of all other users will succeed.

4. Delete GPO link

```
sudo samba-tool gpo dellink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {D63716E9-43CB-4708-AD5C-DEB5355B6CDB} -U administrator
```

4.3 Test 3 – Allow/Deny Login

Note: Replace the GPO unique ID by the one retrieved in chapter 2.2.

1. Link GPO to the container, where the SSSD test server/workstation is stored:

```
sudo samba-tool gpo setlink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {F77CA036-26E4-43FA-92F3-8342FA960EEA} -U administrator
```

2. On the test machine flush the SSSD cache:

```
sudo sss_cache -E
```

3. Check login of adgpo.testuser and other users

Expected result:

Login of all other users will fail in enforce mode or create a warning in the system log:

```
Warning: user would have been denied GPO-based logon access if the
 ad_gpo_access_control option were set to enforcing mode.
```

4. Delete GPO link

```
sudo samba-tool gpo dellink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {F77CA036-26E4-43FA-92F3-8342FA960EEA} -U administrator
```

4.4 Test 4 – Capital Letter GPO Folder MACHINE

Note: Replace the GPO unique ID by the one retrieved in chapter 2.2.

1. Link GPO to the container, where the SSSD test server/workstation is stored:

```
sudo samba-tool gpo setlink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {F50AB220-5160-4236-8E07-7B58574FF259} -U administrator
```

2. On the test machine flush the SSSD cache:

```
sudo sss_cache -E
```

3. Check login of adgpo.testuser and other users

Expected result:

Login of adgpo.testuser fails in enforce mode or creates a warning in the system log:

```
Warning: user would have been denied GPO-based logon access if the
 ad_gpo_access_control option were set to enforcing mode.
```

Login of all other users will succeed.

4. Delete GPO link

```
sudo samba-tool gpo dellink "OU=SSSD Test Servers,DC=mydomain,DC=local"
 {F50AB220-5160-4236-8E07-7B58574FF259} -U administrator
```

5 Test Clean-up

Move the SSSD test server/workstation back into its original container if required.

6 Test Results:

The following table shows the test results on the author's machine:

Test	sssd-1.16.0	sssd-1.16.0 (with patches)	Remarks
1	Failed	Passed	Login of all users succeeds
2	Failed	Passed	Login of test user succeeds
3	Failed	Passed	Login of all users succeeds
4	Failed	Passed	Login of test user succeeds