Audience: the attendees of the tutorial "The power of ACIs"

To the tutorial participants,

Most of you experimented a "bug" in the lab "Secure communication only".

Let me clarify this part of the lab

Context
Tests are `ldapsearch` based, performed by anonymous and one authenticated user
By default, all requests returned the same 23 entries

When applying the first `dsconfig` command, most of you noticed the same 23 entries returned when using LDAP, LDAPS or STARTTLS.

This is not a "bug". This is a normal behaviuor as the tests were performed partially at this stage, just using anonymous requests.
If the entire tests set had been run, the result would be all requests returned 23 entries **but** not the one with authenticated user on LDAP.

Explanation
This is because the `dsconfig` command we used set `require-secure-authentication:true` at a password policy level.
And as you know, anonymous access is not affected by any password policy as they are not by password concerned.

And now
So this is the purpose of the ACI in **`01`**`_The_Power_of_ACI.ldif`
But I made a mistake in the ACI syntax and the ACI was not relevant.
I apologize sincerely for the trouble.
The correct entry is

```
dn: dc=ldapcon,dc=2015
changetype: modify
add: aci
aci:
(target="ldap:///dc=ldapcon,dc=2015")(targetattr="*")(ver
sion 3.0;acl "Prevent plain LDAP operations"; deny (all)
(userdn="ldap:///anyone" AND ssf<="1");)
```

With this ACI, only tests on LDAPS and STARTTLS can return 23 entries.
LDAP tests return no entries
You can note this ACI applies on branch `dc=ldapcon,dc=2015` and not applies on the RootDSE.
The main advantage of this implementation is that it doesn't affect anonymous search requests on RootDSE (part of RFC).
The main cons is that anonymous requests are accepted by the LDAP engine.

Alternative

In the lab "Disable unauthenticated access", applying the file `02_The_Power_of_ACI.ldif` removes the ACI just set before.
But the `dsconfig` command set `reject-unauthenticated-requests:true` as a global configuration propertie.
So anonymous cannot connect to LDAP server using any protocol that is the goal to achieve in this exercise.
A negative side effect is that anonymous search requests on RootDSE are rejected and some applications could be impacted (heartbeat, ...) as that breaks LDAP RFC

So, consider this way with caution.
If not, adjust the global ACIs containing `userdn="ldap:///anyone"` in the subject when it is possible and use

- `userdn="ldap:///FAKE=anyone"` to "disable the ACI
- `userdn="ldap:///all"` to enable only for authenticated users

I hope this addendum could encourage you to dive into the ACIs capabilities.

Thank you

Alban Meunier
ameunier@smartwavesa.com