Configuring NMIS to use Active Directory Authentication (ms-ldap or ms-ldaps)

General User Authentication Information

For a simple set of configuration items for ALL types of User Authentication systems please refer here:

User Management in NMIS8

Setting up MS-LDAP authentication

Outline of the configuration items

```
'auth_ldap_context' => 'ou=people,dc = example, dc = com',# LDAP context to link.

'auth_method_1' => 'ms-ldap', #First type of Authentication can be followed by other types

'auth_ms_ldap_attr' => 'sAMAccountName',# the attribute that matches the username.

'auth_ms_ldap_base' => 'dc=corp, dc=example,dc=com',#base to search in LDAP

'auth_ms_ldap_dn_acc' => 'CN=omklatam, ou = Services, dc = OPMANTEK, dc = corp', #

'auth_ms_ldap_dn_psw' => 'password,',

'auth_ms_ldap_server' => 'host_LDAP: 389',
```

Aspects to consider:

NOTE on MS-LDAPS SSL

To use SSL/TLS secured MS-LDAP (MS-LDAPS) see the differences in the table in User Management in NMIS8 .

In summary it requires Optional Perl Modules: IO::Socket::SSL and Net::LDAPS and uses config items:
'auth_method_1' => 'ms-ldaps'
'auth_ms_ldaps_server' => 'host[:port]' (note the s at the end of ldaps vs ldap)

If you use an internal CA for your AD LDAP SSL certificates you will need to import your internal root CA public certificates so that SSL can trust the connection. Search processes for your NMIS servers OS.

LDAP Base: The base is the root of the Active Directory, since it is the place where the search of the users who need to authenticate will be carried out. Taking as reference the structure of the Active Directory will be as follows:

```
'auth_ms_ldap_base' => 'dc = OPMANTEK, dc = corp',#base to search in LDAP

'auth_ldap_context' => 'dc = OPMANTEK, dc = corp',# LDAP context
```

The account is the service account which user is going to authenticate with the active directory, to enable the search of the LDAP Database for users.

Therefore, the first part is added is the service account username **CN=omklatam**

The second part is the **OU = Servicescontainer**.

The third part is the domain **DC = OPMANTEK and DC = corp**.

The result would be the following:

```
'auth_ms_ldap_dn_acc' => 'CN = omklatam, ou = Services, dc = OPMANTEK, dc = corp',
```

To find the user and group base DN, run a query from any member server on your Windows domain:

Finding the User Base DN

a. Open a Windows command prompt.
b. Type the command:

```
dsquery user -name <known username>
```

Example: If you are searching for all users named "John", you can enter the username as John* to get a list of all users who's name is John.

The result will look like:

```
"CN=John.Smith,CN=Users,DC=MyDomain,DC=com"
```

Installation and configuration.

- Make sure**Net :: LDAP** is up to date (minimum version 0.64).

```
[root @ opmantek] #cpan Net :: LDAP
```

- Make sure that **IO :: Socket :: SSL**is new enough (must be 1998 or newer).

```
[root @ opmantek] #cpan -f IO :: Socket :: SSL
```

Note:**-f** is because some tests do not pass on some machines.

- Configuration items as above in /usr/local/nmis8/conf/Config.nmis
- Perform procedure to add users through the GUI or through the conf/Users.nmios file, the User field for each user must match the User's "sAMAccountName" attribute in AD. The Privilege should be set the appropriate Authorisation level.
- See here for more information on NMIS User authorisation User Management in NMIS8#AuthorisationinNMIS

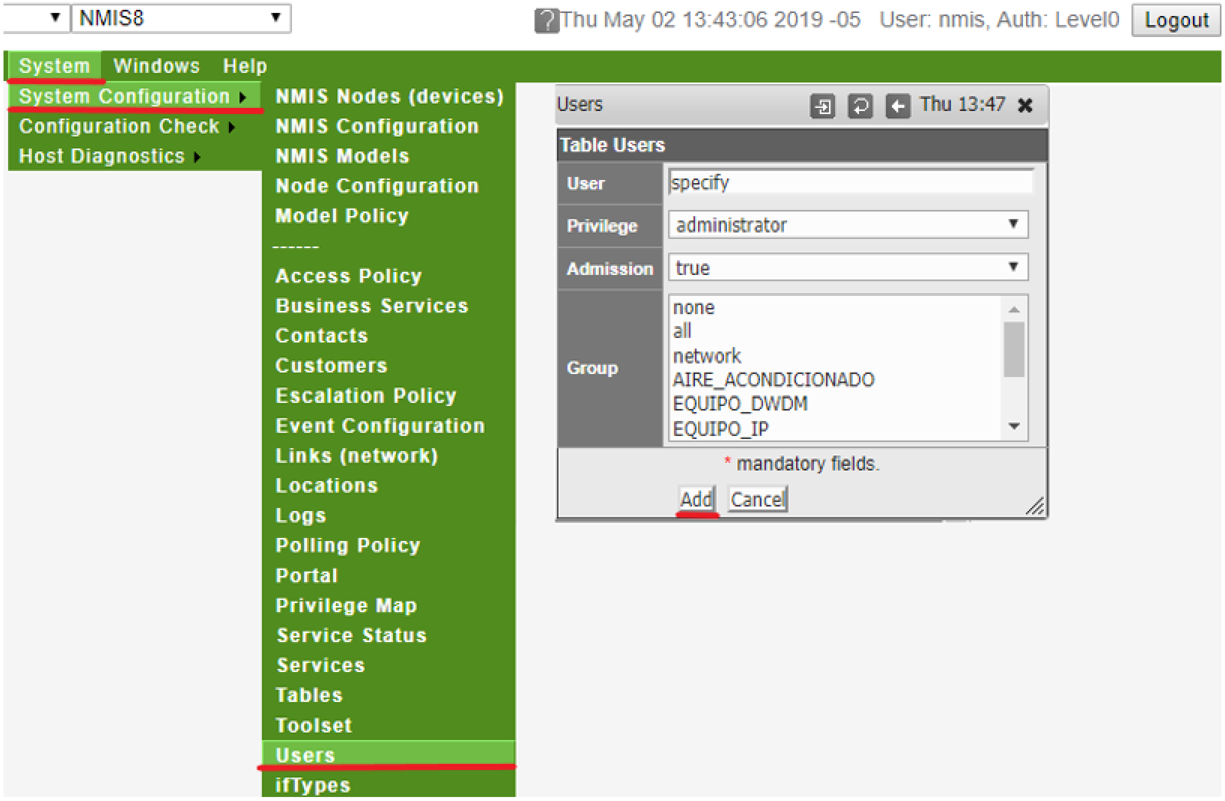


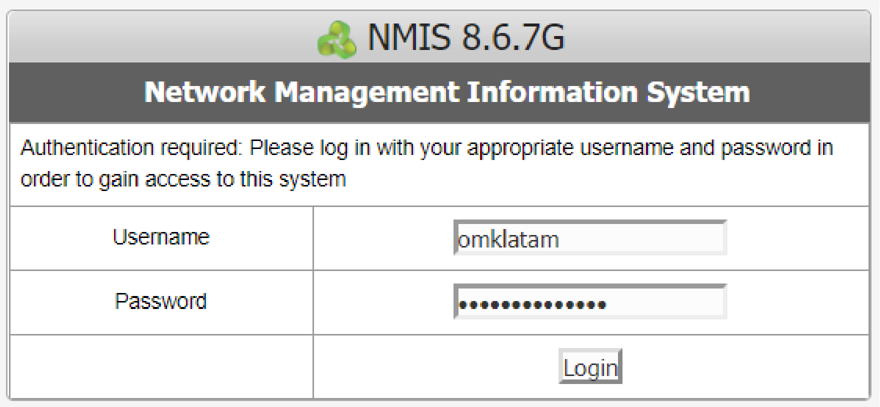
Table Users

User	specify
Privilege	administrator
Admission	true
Group	none all network AIRE_ACONDICIONADO EQUIPO_DWDM EQUIPO_IP

* mandatory fields.

Add Cancel

- Try to access the credentials granted by the client in the NMIS portal.



NMIS 8.6.7G

Network Management Information System

Authentication required: Please log in with your appropriate username and password in order to gain access to this system

Username	omklatam
Password	••••••••••••••
	Login

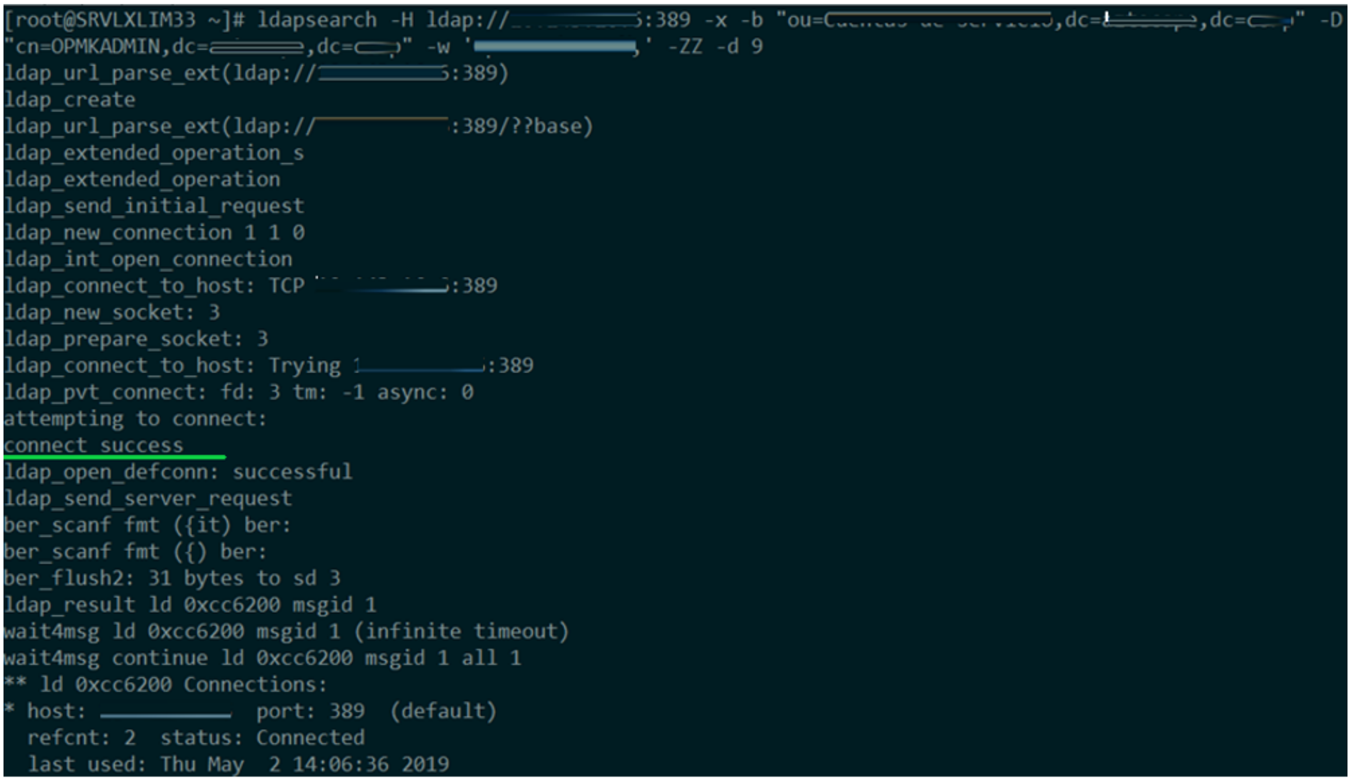
Testing LDAP access

- Perform the installation of the following packages for troubleshooting.

```
[root @ opmantek] #yum -y install openldap-clients nss-pam-ldapd
```

- Verify LDAP connectivity using **ldapsearch**, you will have to configure -H, -by -D, they can come from your current NMIS ms-ldap configuration if you have a: -b is **auth_ms_ldap_base**, -D is**auth_ms_ldap_dn_acc**

```
ldapsearch -H ldap: // ip_LDAP: 389 -x -b "ou = User container, dc = domain, dc = domain" -D "cn = user_ldap, dc = domain, dc = domain" -w 'password_user' - ZZ -d 9
```



```
[root@SRVLXLIM33 ~]# ldapsearch -H ldap://[redacted]:389 -x -b "ou=[redacted],dc=[redacted],dc=[redacted]" -D
"cn=OPMKADMIN,dc=[redacted],dc=[redacted]" -w '[redacted]' -ZZ -d 9
ldap_url_parse_ext(ldap://[redacted]:389)
ldap_create
ldap_url_parse_ext(ldap://[redacted]:389/??base)
ldap_extended_operation_s
ldap_extended_operation
ldap_send_initial_request
ldap_new_connection 1 1 0
ldap_int_open_connection
ldap_connect_to_host: TCP [redacted]:389
ldap_new_socket: 3
ldap_prepare_socket: 3
ldap_connect_to_host: Trying [redacted]:389
ldap_pvt_connect: fd: 3 tm: -1 async: 0
attempting to connect:
connect success
ldap_open_defconn: successful
ldap_send_server_request
ber_scanf fmt ({it) ber:
ber_scanf fmt ({) ber:
ber_flush2: 31 bytes to sd 3
ldap_result ld 0xcc6200 msgid 1
wait4msg ld 0xcc6200 msgid 1 (infinite timeout)
wait4msg continue ld 0xcc6200 msgid 1 all 1
** ld 0xcc6200 Connections:
* host: [redacted]  port: 389  (default)
  refcnt: 2  status: Connected
  last used: Thu May  2 14:06:36 2019
```

Note: Possibly it shows an SSL certificate error, this error is irrelevant since although the connection is shown it has been successful.