Configuración de LDAP

Introducción

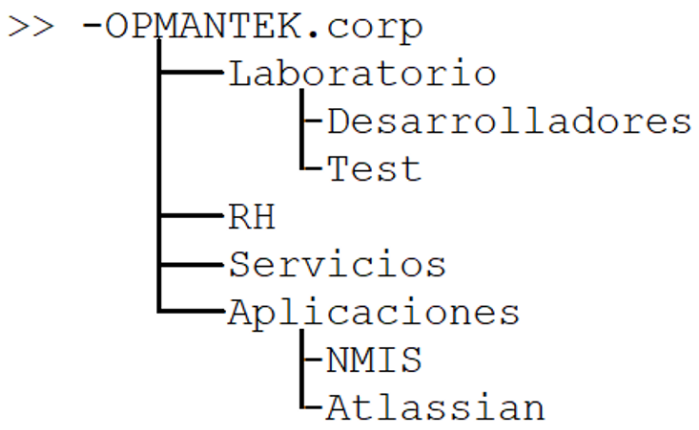
En este documento se describen los pasos para poder realizar la configuración del servicio LDAP en la MV OPMANTEK. Se requiere conocer la estructura del Directorio Activo para poder efectuar la configuración del servicio.

Requisito

- Se requiere que los puertos del servicio se encuentren abiertos:

Puerto#	Protocolo	Nombre del Servicio	Iniciación de la Conexión	Aplicación	Notas
389	TCP	LDAP	Servidor a LDAP Servidor	NMIS	NMIS Authentication

- Estructura del Directorio Activo: Imagen representativa.



- Usuario LDAP (Directorio activo): Este usuario permitirá hacer la conexión entre la aplicación y el directorio activo, en este proceso se generará un usuario (**omklatam**) en el directorio **Servicios,** el usuario generado debe tener los permisos suficientes para poder hacer una búsqueda en los demás directorios. dicho usuario tendrá la capacidad de autenticarse con la aplicación y así poder realizar una búsqueda de los demás usuarios que requieren autenticarse en la aplicación.
- Definir el método de autenticación que se requiere implementar en NMIS. La configuración se realizará en el archivo **/usr/local/nmis8/conf /Config.nmis**

Método	Descripción
apache	Apache realizará la autenticación y proporcionará un usuario autenticado a NMIS, al que se aplicarán políticas de autorización.
htpasswd	NMIS utilizará los usuarios definidos en el archivo de usuarios de NMIS, de forma predeterminada /usr/local/nmis8/conf/users.dat

ldap	NMIS utilizará el servidor LDAP configurado para realizar la autenticación
	
	Requiere módulo Perl opcional: Net :: LDAP
	
	Configurar:
	
	auth_ldap_server => 'host[:port]'
	auth_ldap_attr => '' # attributes to match to username, can be blank, then defaults to ('uid','cn')
	auth_ldap_context => 'ou=people,dc=opmantek,dc=com', # base of context to attempt to bind to

ldaps (secure)	NMIS utilizará el servidor LDAP configurado para realizar la autenticación
	
	Requiere módulos Perl opcionales: IO :: Socket :: SSL y Net :: LDAPS
	
	Configurar:
	
	auth_ldaps_server => 'host[:port]'
	auth_ldap_attr => '' # attributes to match to username, can be blank, then defaults to ('uid','cn')
	auth_ldap_context => 'ou=people,dc=opmantek,dc=com', # base of context to attempt to bind to

ms-ldap	NMIS utilizará el servidor configurado de Microsoft Active Directory (LDAP) para realizar la autenticación Requiere módulo Perl opcional: Net :: LDAP Configurar: 'auth_ldap_context' => 'ou=ejemplo,dc=ejemplo.ejemplo,dc=ejemplo', # base de contexto LDAP para enlazar. 'auth_method_1' => 'ms-ldap',#Primer tipo de Autenticación 'auth_method_2' => '', #Segundo tipo de Autenticación 'auth_method_3' => '', 'auth_ms_ldap_attr' => 'sAMAccountName', #los atributos que coinciden con el nombre de usuario, pueden estar en blanco. 'auth_ms_ldap_base' => 'ou=ejemplo,dc=ejemplo.ejemplo,dc=ejemplo', #base para buscar en LDAP 'auth_ms_ldap_debug' => 'false',#Cambiar valor a true 'auth_ms_ldap_dn_acc' => 'CN=ejemplo,ou=ejemplo,dc=ejemplo.ejemplo,dc=ejemplo', 'auth_ms_ldap_dn_psw' => 'password,', 'auth_ms_ldap_server' => 'host_LDAP:389', 'auth_ms_ldaps_server' => 'host_LDAP:389',

ms-ldaps (secure)	NMIS utilizará el servidor configurado de Microsoft Active Directory (LDAP) para realizar la autenticación
	
	Requiere módulos Perl opcionales: IO :: Socket :: SSL y Net :: LDAPS
	
	Configurar:
	auth_ms_ldaps_server => 'host[:port]'
	auth_ms_ldap_dn_acc => '' # the DN/account to bind with
	auth_ms_ldap_dn_psw => 'password'
	auth_ms_ldap_attr => 'sAMAccountName', # attribute to match to username
	auth_ms_ldap_base => 'dc=corp,dc=opmantek,dc=com' # base to search from

radius	NMIS utilizará el servidor de radio configurado (Cisco ACS o Steel Belted Radius, por ejemplo) Requiere módulos Perl opcionales: Authen :: Simple :: RADIUS Configurar: auth_radius_server => 'host:port' auth_radius_secret => 'secret'
tacacs	NMIS utilizará el servidor Tacacs + configurado (Cisco ACS, por ejemplo) Requiere módulos Perl opcionales: Authen :: TacacsPlus Configuracion: auth_tacacs_server => 'host:port' auth_tacacs_secret => 'secret' # Also known as the "Key"

Nota: En este caso el método de autenticación que se utilizara es **ms-ldap,** lo cual procederemos a configurar.

- El cliente deberá proporcionar los siguientes datos para poder realizar la configuración:

```
'auth_ldap_context' => 'dc=ejemplo.ejemplo,dc=ejemplo', # contexto LDAP para enlazar.

'auth_method_1' => 'ms-ldap',#Primer tipo de Autenticación

'auth_ms_ldap_attr' => 'sAMAccountName', #los atributos que coinciden con el nombre de usuario.

'auth_ms_ldap_base' => 'dc=ejemplo.ejemplo,dc=ejemplo', #base para buscar en LDAP

'auth_ms_ldap_dn_acc' => 'CN=ejemplo,ou=ejemplo,dc=ejemplo.ejemplo,dc=ejemplo',

'auth_ms_ldap_dn_psw' => 'password,',

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

Aspectos a considerar:

Base de LDAP: La base es la raíz del Directorio Activo, ya que es el lugar donde se realizará la búsqueda de los usuarios que se requieren autenticar. Tomando como referencia la estructura del Directorio Activo quedará de la siguiente manera:

```
'auth_ms_ldap_base' => 'dc=OPMANTEK, dc=corp', #base para buscar en LDAP

'auth_ldap_context' => 'dc=OPMANTEK, dc=corp', #Contexto de LDAP
```

El account es el parámetro que indica qué usuario se va a autenticar con el directorio activo, este usuario es el que permitirá hacer la búsqueda de los demás usuarios que requieren acceder al servicio.

Por lo tanto, se agrega la primera parte es el usuario **CN = omklatam**

La segunda parte es el contenedor **OU = Servicios**.

La tercera parte es el dominio **DC = OPMANTEK y DC = corp**.

el resultado sería lo siguiente:

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

Si el dominio fuera example.net, la sintaxis sería DC = ejemplo, DC = net. DC se usa para la parte del dominio, y CN se usa para las credenciales de usuario.

Instalacion y configuracion.

- Asegúrese de que **Net::LDAP** esté actualizado (versión mínima 0.64).

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

- Asegúrese de que **IO::Socket::SSL** sea lo suficientemente nuevo (debe ser 1.998 o más reciente).

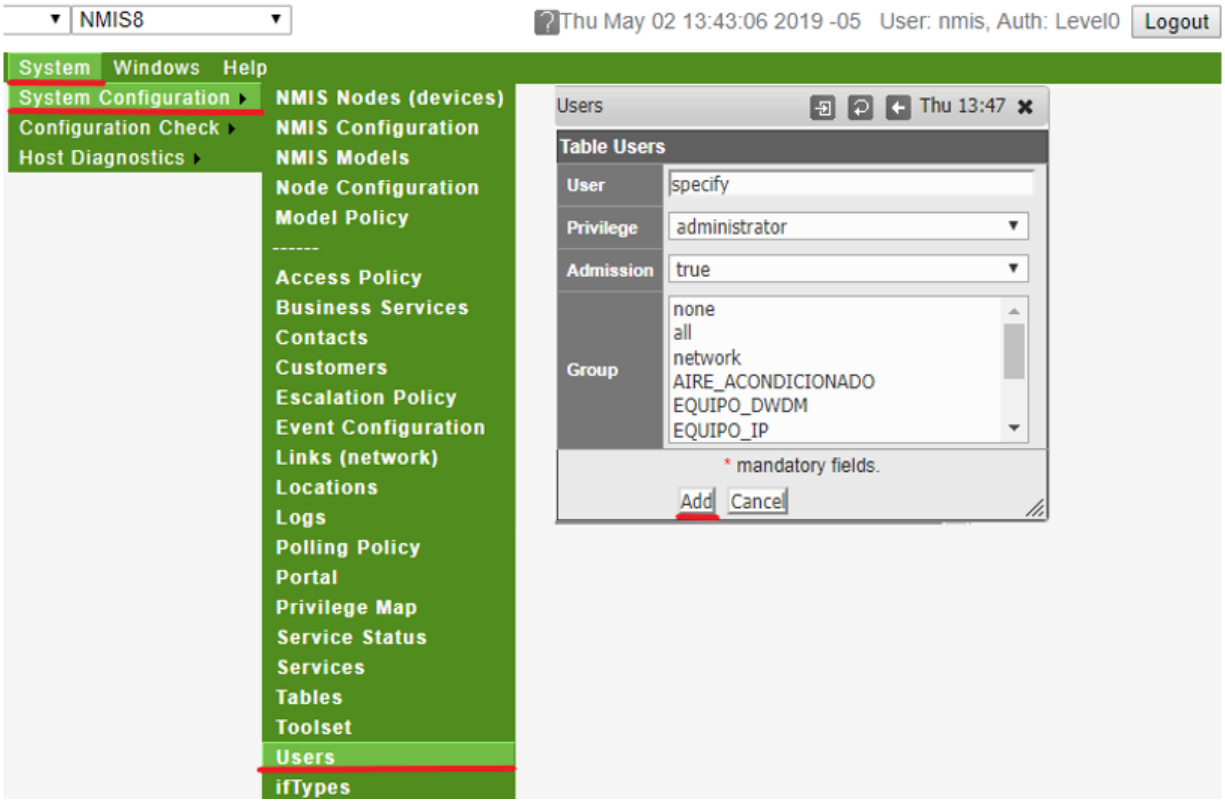
```
[root@opmantek]# cpan -f IO::Socket::SSL
```

Nota: **-f** es porque algunas pruebas no pasan en algunas máquinas virtuales.

- Realizar la instalación del siguiente paquete.

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

- Realizar este procedimiento para agregar usuarios por medio de la GUI, si no se quiere alterar los privilegios por defecto, hay que acceder a NMIS usando el usuario "nmis" y agregar el usuario ("System -> System Configuration -> Users") que el cliente requiere y asignarle privilegios.



Nota: Esto es para que no tenga que definir a cada usuario en el sistema si el sistema de autenticación proporciona una lista reducida de usuarios, para que los usuarios se conviertan en un operador o invitado por defecto y puedan ver todos los grupos de dispositivos, lo siguiente aplicaría.

'auth_default_privilege' => 'guest',

'auth_default_groups' => 'all',

Para evitar la autorización predeterminada, simplemente defínalos como en blanco, que es el valor predeterminado en la configuración de instalación de NMIS8.

- Configurar el archivo **/usr/local/nmis8/conf/Config.nmis** con los siguientes parámetros:

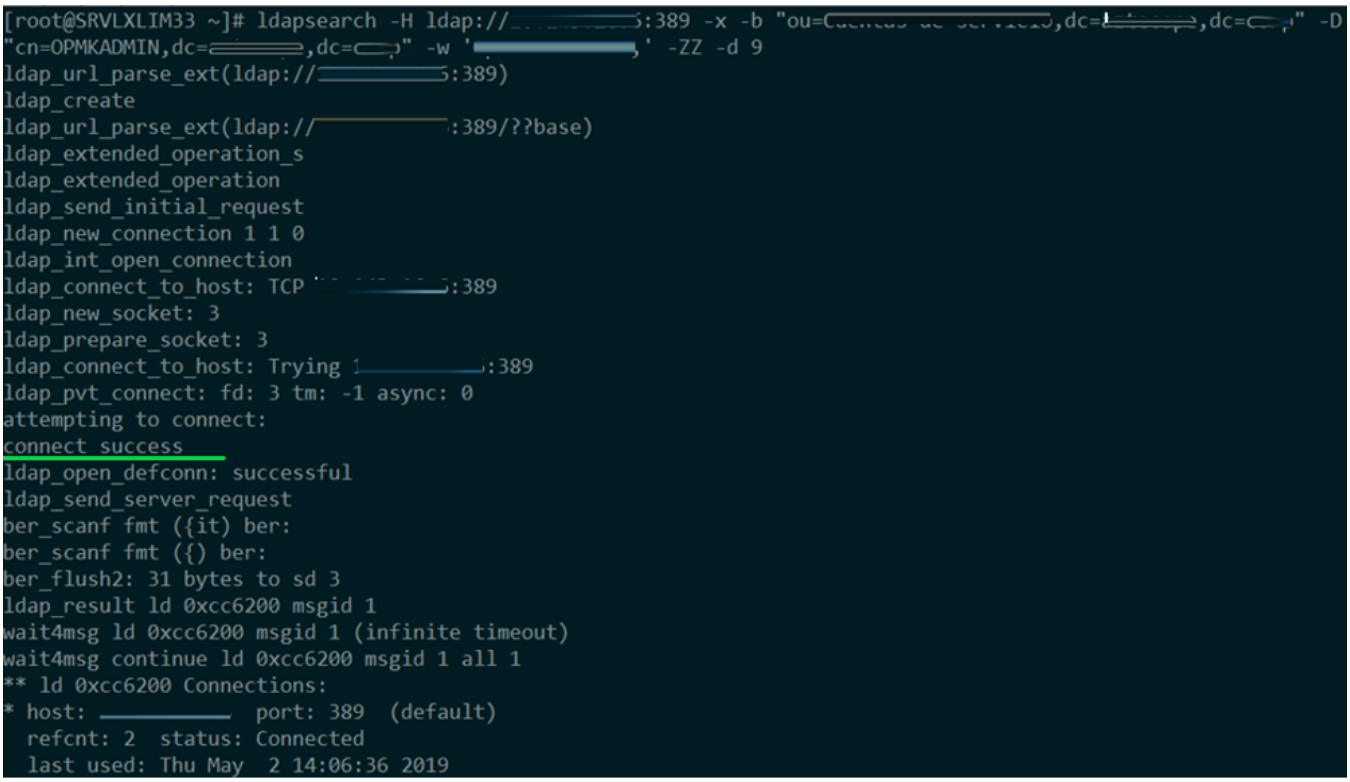
*Datos de Ejemplo.

```
'auth_ldap_context' => 'dc=OPMANTEK, dc=corp',   # contexto LDAP para enlazar.

'auth_method_1' => 'ms-ldap',      #Primer tipo de Autenticacion

'auth_method_2' => 'htpasswd',   #Segundo tipo de Autenticacion

'auth_method_3' => '',

'auth_ms_ldap_attr' => 'sAMAccountName',   #los atributos que coinciden con el nombre de usuario.

'auth_ms_ldap_base' => 'dc=OPMANTEK, dc=corp',   #base para buscar los usuarios de LDAP

'auth_ms_ldap_debug' => 'true',   #Cambiar valor a true

'auth_ms_ldap_dn_acc' => 'CN=omklatam,ou=Servicios,dc=OPMANTEK,dc=corp', #Cuenta para autenticarse en LDAP

'auth_ms_ldap_dn_psw' => 'password,',

'auth_ms_ldap_server' => 'host_LDAP:389',

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

Ejecutar un **perl -c** al archivo para comprobar que no existan errores de sintaxis.

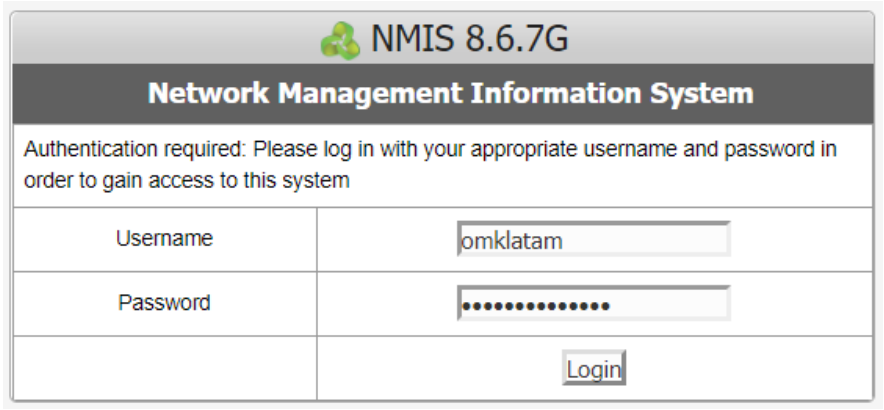
- Verifique la conectividad LDAP usando **ldapsearch**, tendrá que configurar -H, -b y -D, pueden provenir de su configuración actual de ms-ldap de NMIS si tiene una: -b es **auth_ms_ldap_base**, -D es **auth_ms_ldap_dn_acc**

ldapsearch -H ldap://ip_LDAP:389 -x -b "ou=Contenedor de usuario, dc=dominio,dc=dominio" -D "cn=user_ldap,dc=dominio,dc=dominio" -w 'password_user' -ZZ -d 9



Nota: Posiblemente muestre un error de certificados SSL, este error es irrelevante ya que si bien se muestra la conexión ha sido exitosa.

- Intentar acceder con las credenciales otorgadas por el cliente en el portal de NMIS.



Nota: Si todo está bien configurado, el usuario de conexión de la aplicación existe y los usuarios que desean acceder a NMIS ya están registrados no se debe de presentar ningún inconveniente al querer ingresar a los módulos.

Revisión de errores.

Nota: el archivo **/usr/local/nmis8/conf/Users.nmis** deberá tener una entrada para cada usuario que pueda autenticarse o se deberá establecer la configuración predeterminada para un usuario.

- Revisar los archivos siguientes archivos **/var/log/httpd/error_log** y **/usr/local/nmis8/logs/auth.log** estos deberán poder proporcionar suficiente información de los intentos de autenticación además de poder identificar un acceso al sistema o un posible error.

```
tail -f /usr/local/nmis8/logs/auth.log
```

Nota:

Posiblemente presente un error de este tipo si es que el Usuario o Password no se encuentran en LDAP por lo tanto no se podrá autenticar la aplicación con el servicio, para solucionar esto es necesario que se realice una validación con los administradores del servicio y así poder corregir este error.

Ejemplo:

```
[root@opmantek ~]# tail -f /usr/local/nmis8/logs/auth.log

28-May-2019 09:59:59,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#456Auth:

:_ms_ldap_verify#759<br>ERROR LDAP validation of CN=omklatam,ou=Servicios,dc=OPMANTEK,dc=corp, error msg 80090308: LdapErr: DSID-0C090421, comment: AcceptSecurityContext error, data 52e, v23f0

28-May-2019 09:59:59,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#494<br>INFO login request of user=1 method=ms-ldap failed
```

Nos podemos ayudar del siguiente sitio para hacer la búsqueda del error y poder identificar con más precisión el detalle de este: https://ldapwiki.com/wiki/Common%20Active%20Directory%20Bind%20Errors

Microsoft Active Directory LDAP Result Codes sub-codes for Bind Response:

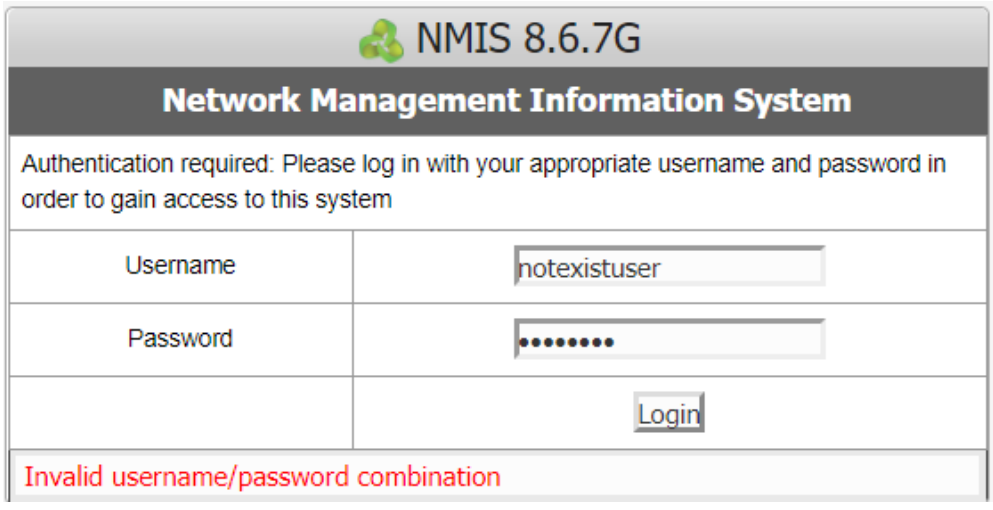
LDAP Result Code 49 sub-codes [1] for Authentication Failures:

▼ 52e

Code	hex	DEC	Short Description	More Information	Comments
49	52e	1326	ERROR_LOGON_FAILURE	Returns when username is valid but password/credential is invalid.	Will prevent most other errors from being displayed as noted.

Un siguiente error común es cuando no se encuentra el usuario en el directorio activo, para esto es necesario validar que este usuario esté registrado en el directorio activo además de que se realice la verificación de password, lo siguiente que se revisará es que dicho usuario esté dado de alta en la herramienta NMIS.

Ejemplo:



[root@opmantek ~]# tail -f /usr/local/nmis8/logs/auth.log

**28-May-2019 10:28:11,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#456Auth::_ms_ldap_verify#763
DEBUG LDAP Base user=CN=Opmantek,ou=Cuentas de servicio,dc=dominio,dc=corp authorized**

**28-May-2019 10:28:11,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#456Auth::_ms_ldap_verify#767
DEBUG LDAP search, base=dc=dominio,dc=corp, filter=sAMAccountName=hola, attr=distinguishedName**

**28-May-2019 10:28:11,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#456Auth::_ms_ldap_verify#783
DEBUG LDAP search failed**

**28-May-2019 10:28:11,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#456Auth::_ms_ldap_verify#788
DEBUG user hola not found in Active Directory**

**28-May-2019 10:28:11,nmiscgi.pl#95Auth::loginout#1311Auth::user_verify#494
INFO login request of user=hola method=ms-ldap failed**