UNIX + PAM + LDAP

Document created on 2013-10-09
Nicolas Bondier

[pdf][doc][htm]

Contents

Introduction

This document present the installation of an LDAP server for authenticating users on any server of a cluster with PAM.

This authentication will be used for many services, such as Linux command line, samba services across directories, dovecot IMAP server authentication and right enable storage, etc…

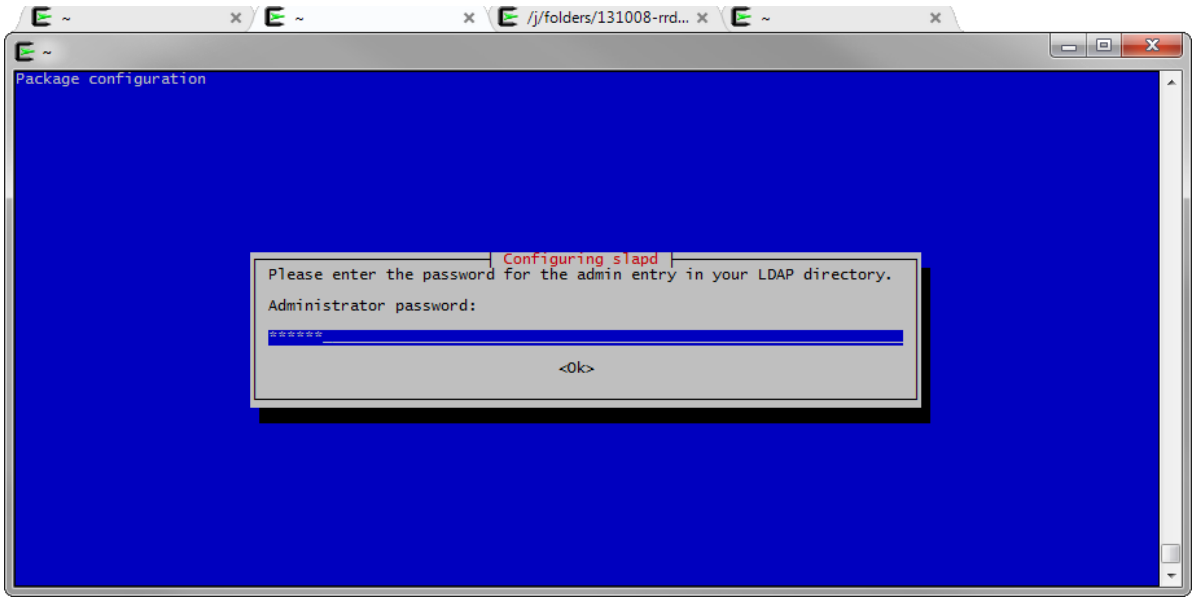
Prerequisites

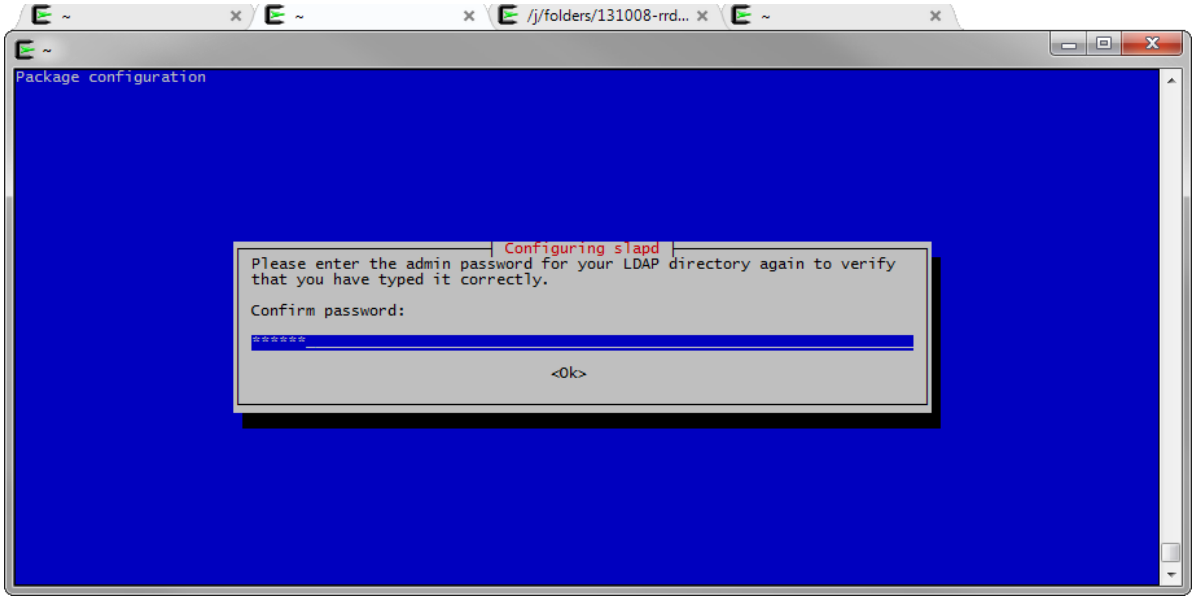
No prerequisites. We need one server for LDAP and a second one for the authentication.

Install OpenLDAP server

Install `slapd` and `ldap-utils` packages.

```
root@ldap:~# aptitude update
root@ldap:~# aptitude install slapd ldap-utils
```





Install gosa:

```
root@ldap: aptitude install gosa
```

Install additional plugins:

```
root@ldap: aptitude install gosa-plugin-ssh gosa-plugin-ssh-schema  gosa-
root@ldap: plugin-sudo gosa-plugin-sudo-schema
```

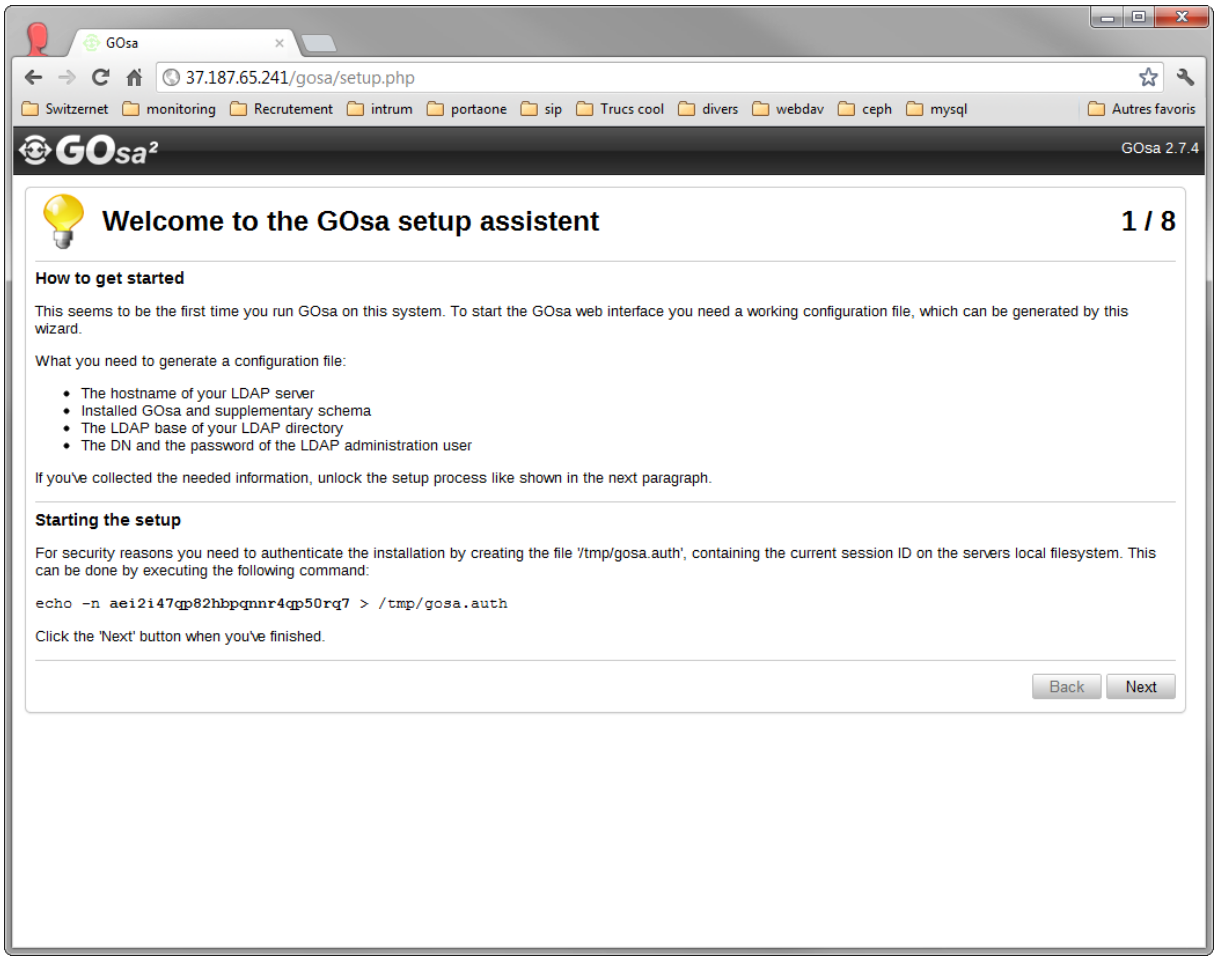
Load all the gosa plugins located under `/etc/gosa/`:

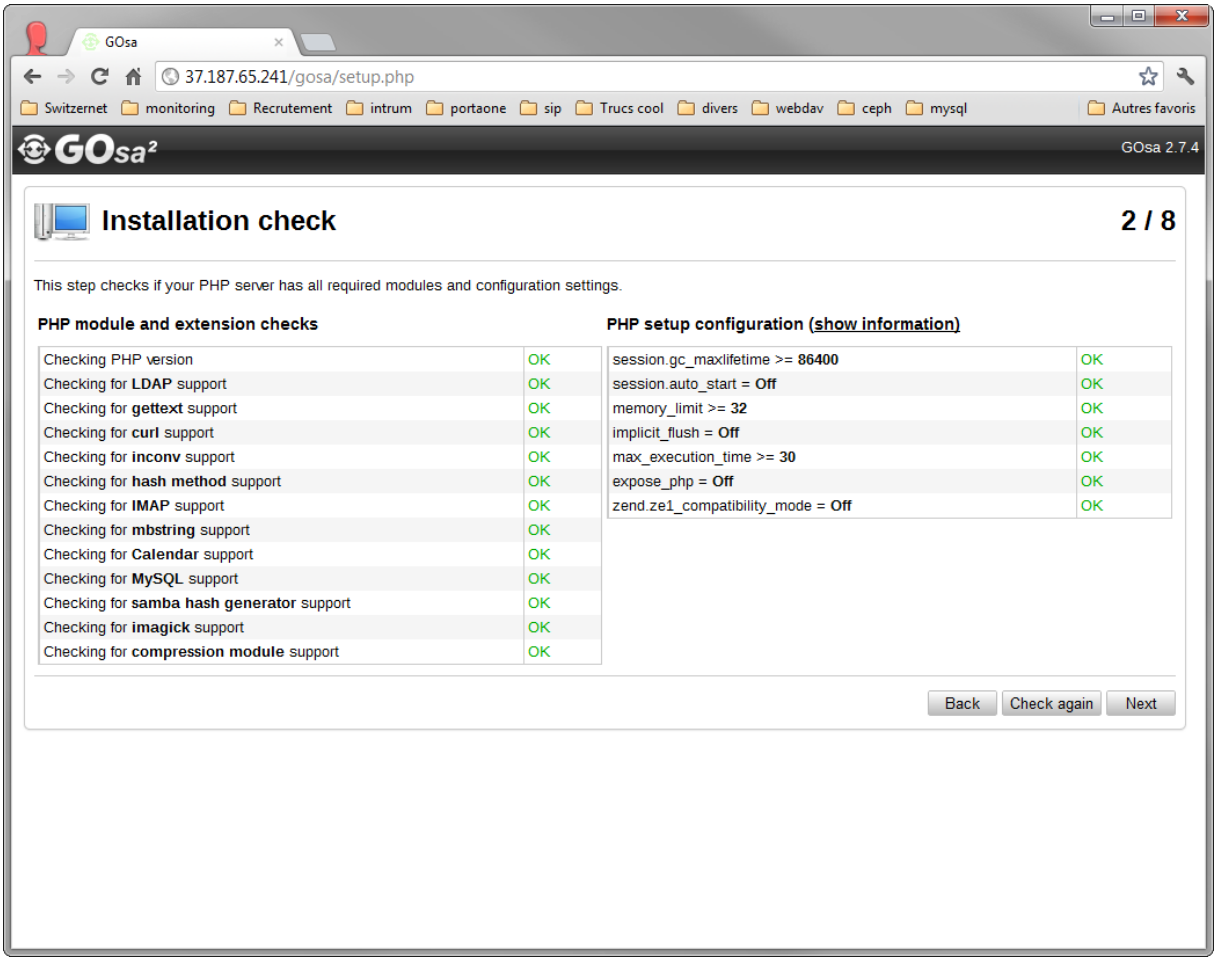
```
root@ldap:~# for schema in
  /etc/gosa/samba3.ldif
  /etc/gosa/gosystem.ldif
  /etc/gosa/gofon.ldif
  /etc/gosa/gofax.ldif
  /etc/gosa/goto.ldif
  /etc/gosa/goserver.ldif
  /etc/gosa/gosa-samba3.ldif
  /etc/gosa/goto-mime.ldif
  /etc/gosa/trust.ldif
  /etc/gosa/pureftpd.ldif
  /etc/gosa/fai.ldif
  /etc/gosa/sudo.ldif
  /etc/gosa/openssh-lpk.ldif
  /etc/gosa/nagios.ldif
  /etc/gosa/kolab2.ldif
  /etc/dyngroup.ldif;
do ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/$schema || exit 1;
done
```

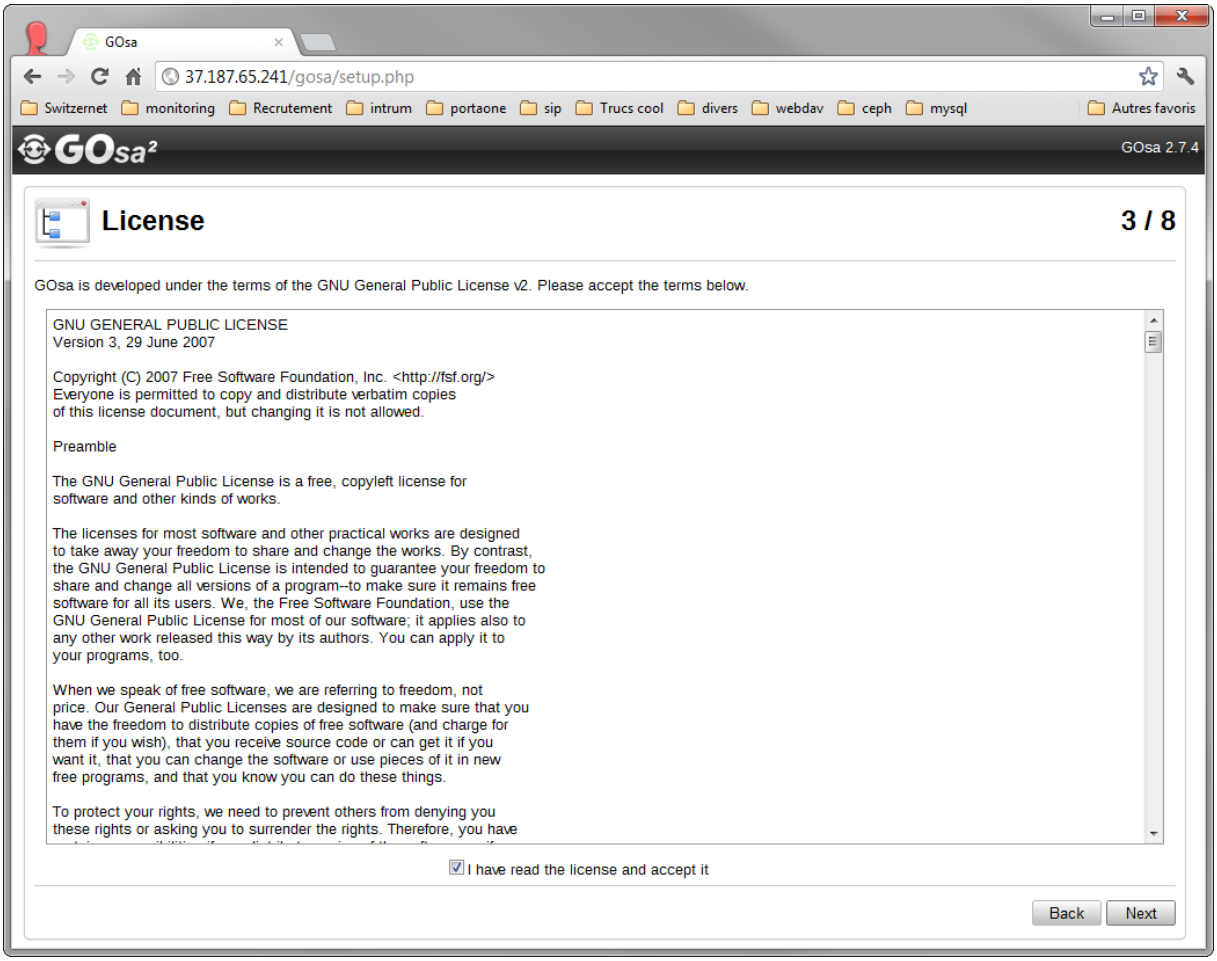
Restart your ldap:

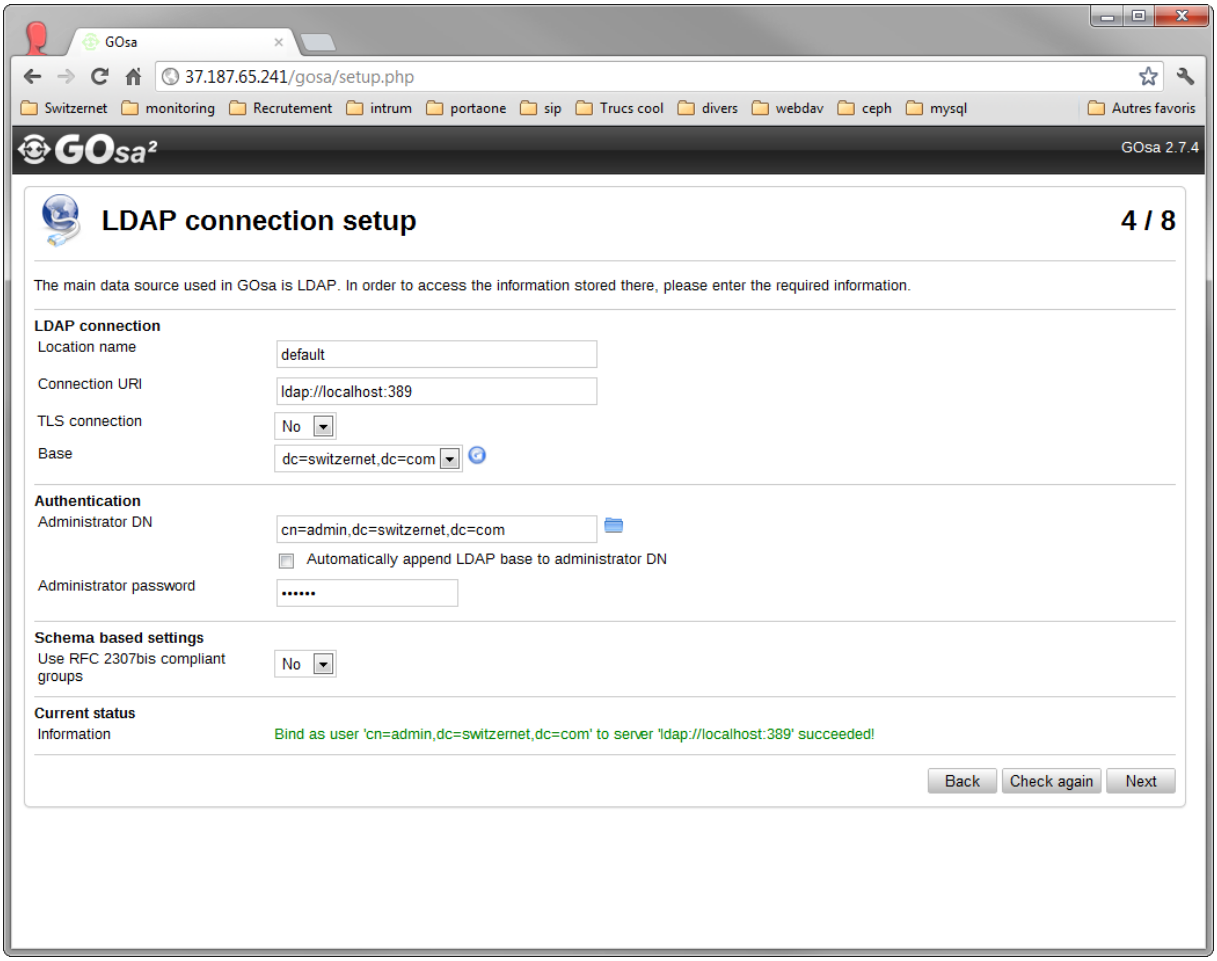
```
root@ldap:~# /etc/init.d/slapd start
```

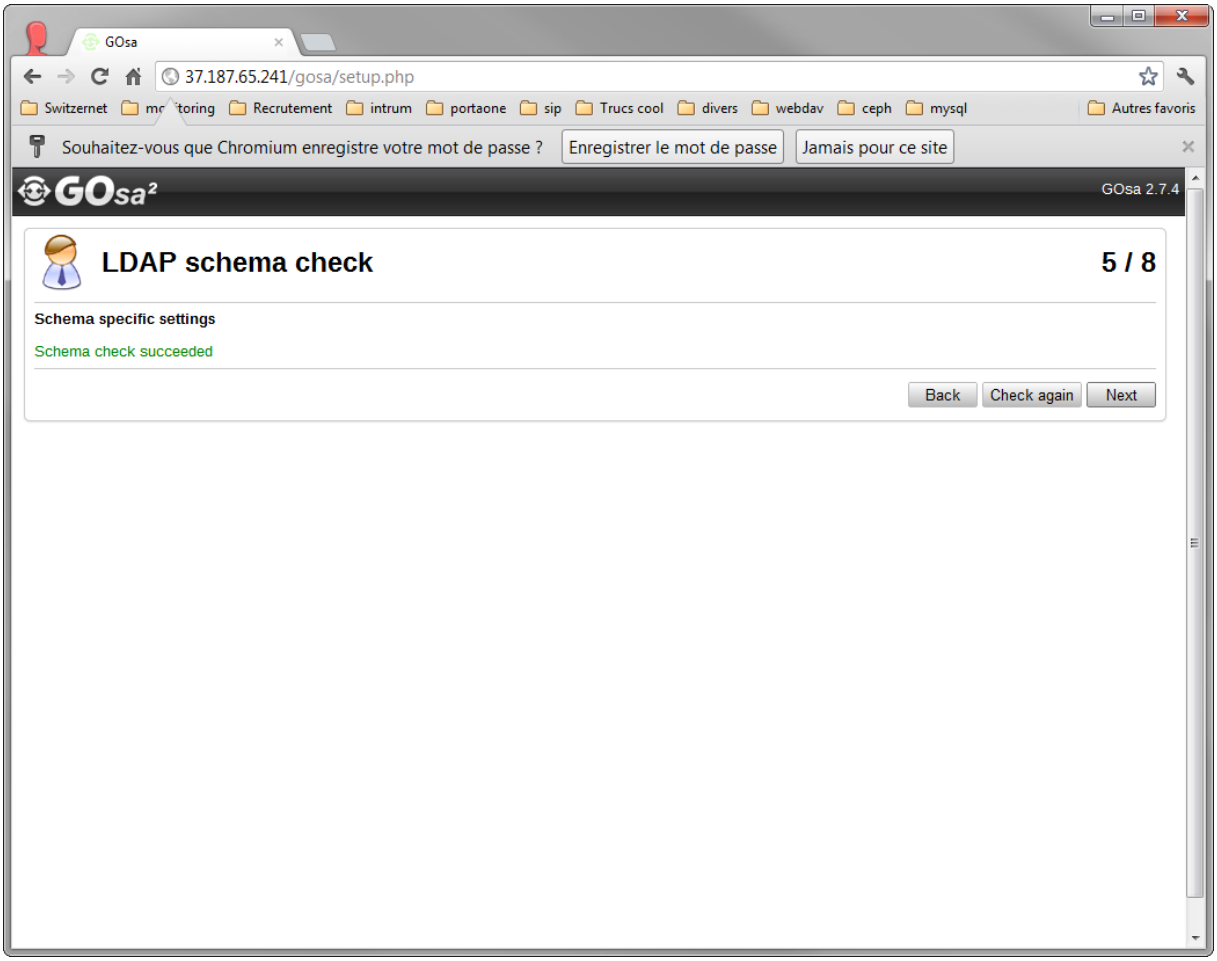
Go to the Gosa configuration interface (http://ldap-server/gosa/), and follow the instructions for configuring Gosa:

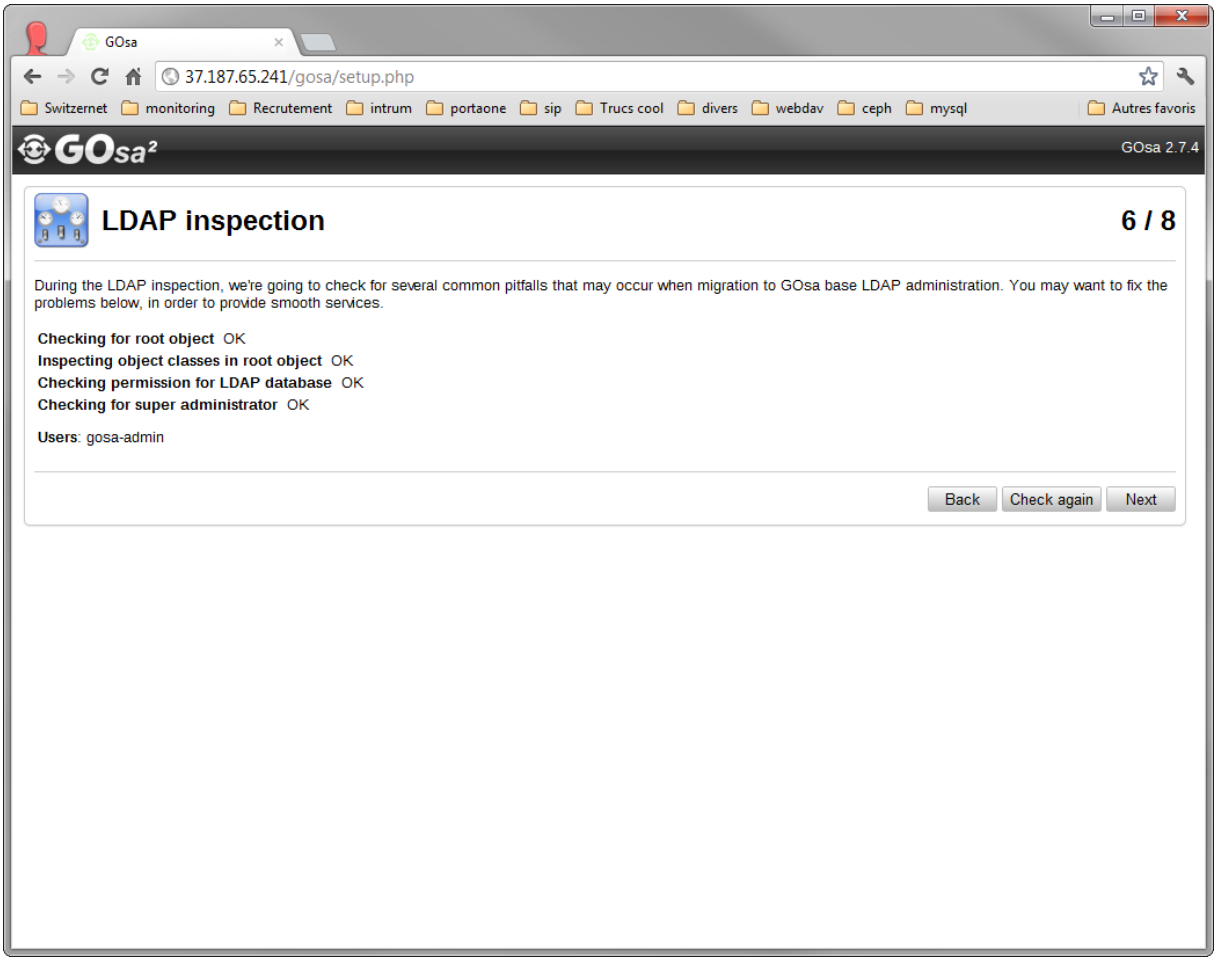


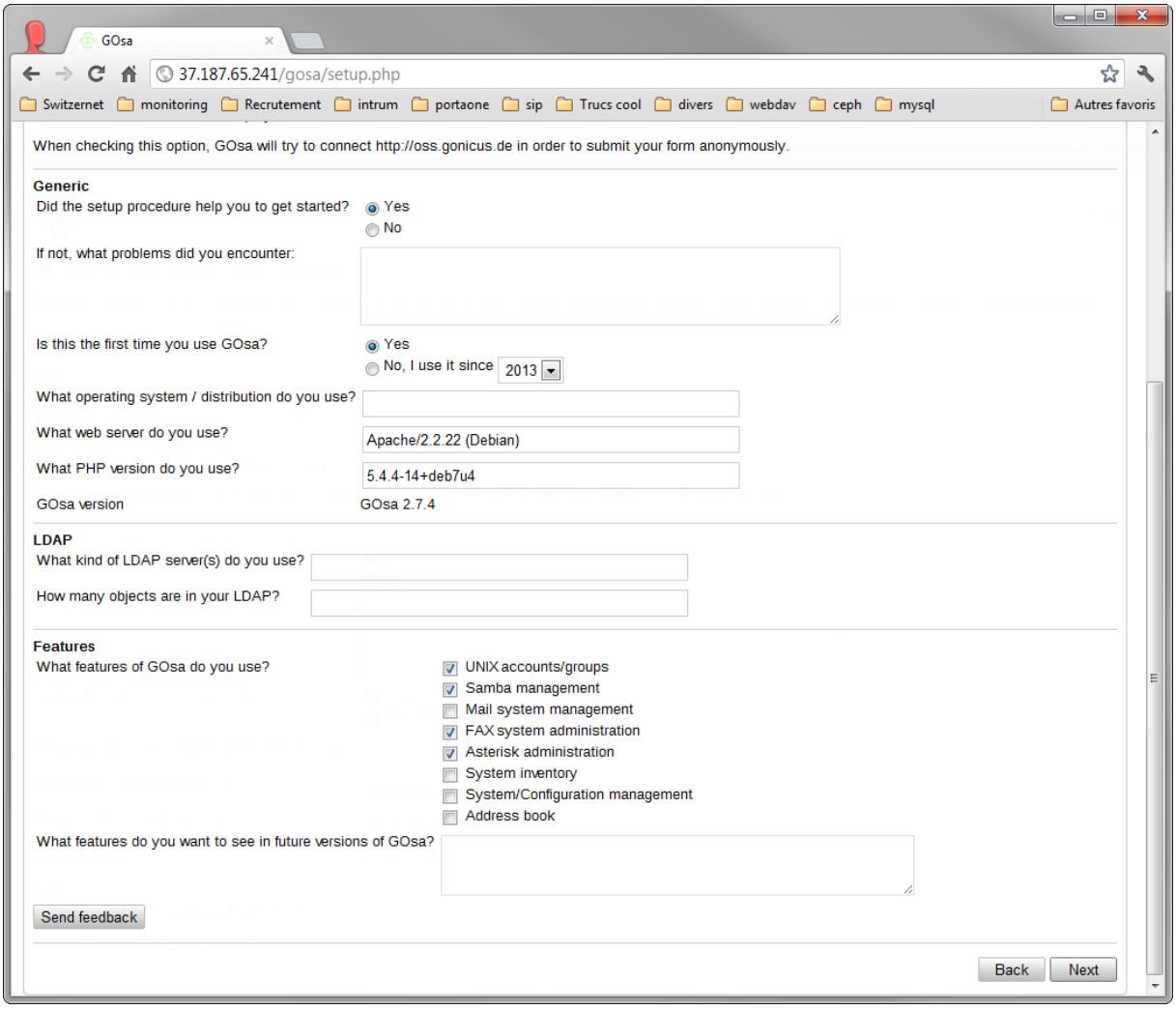

GOsa
37.187.65.241/gosa/setup.php
Switzernet monitoring Recrutement intrum portaone sip Trucs cool divers webdav ceph mysql Autres favoris
GOsa²
GOsa 2.7.4
Installation check
2 / 8
This step checks if your PHP server has all required modules and configuration settings.
PHP module and extension checks
Checking PHP version OK
Checking for LDAP support OK
Checking for gettext support OK
Checking for curl support OK
Checking for inconv support OK
Checking for hash method support OK
Checking for IMAP support OK
Checking for mbstring support OK
Checking for Calendar support OK
Checking for MySQL support OK
Checking for samba hash generator support OK
Checking for imagick support OK
Checking for compression module support OK
PHP setup configuration (show information)
session.gc_maxlifetime >= 86400 OK
session.auto_start = Off OK
memory_limit >= 32 OK
implicit_flush = Off OK
max_execution_time >= 30 OK
expose_php = Off OK
zend.ze1_compatibility_mode = Off OK
Back
Check again
Next

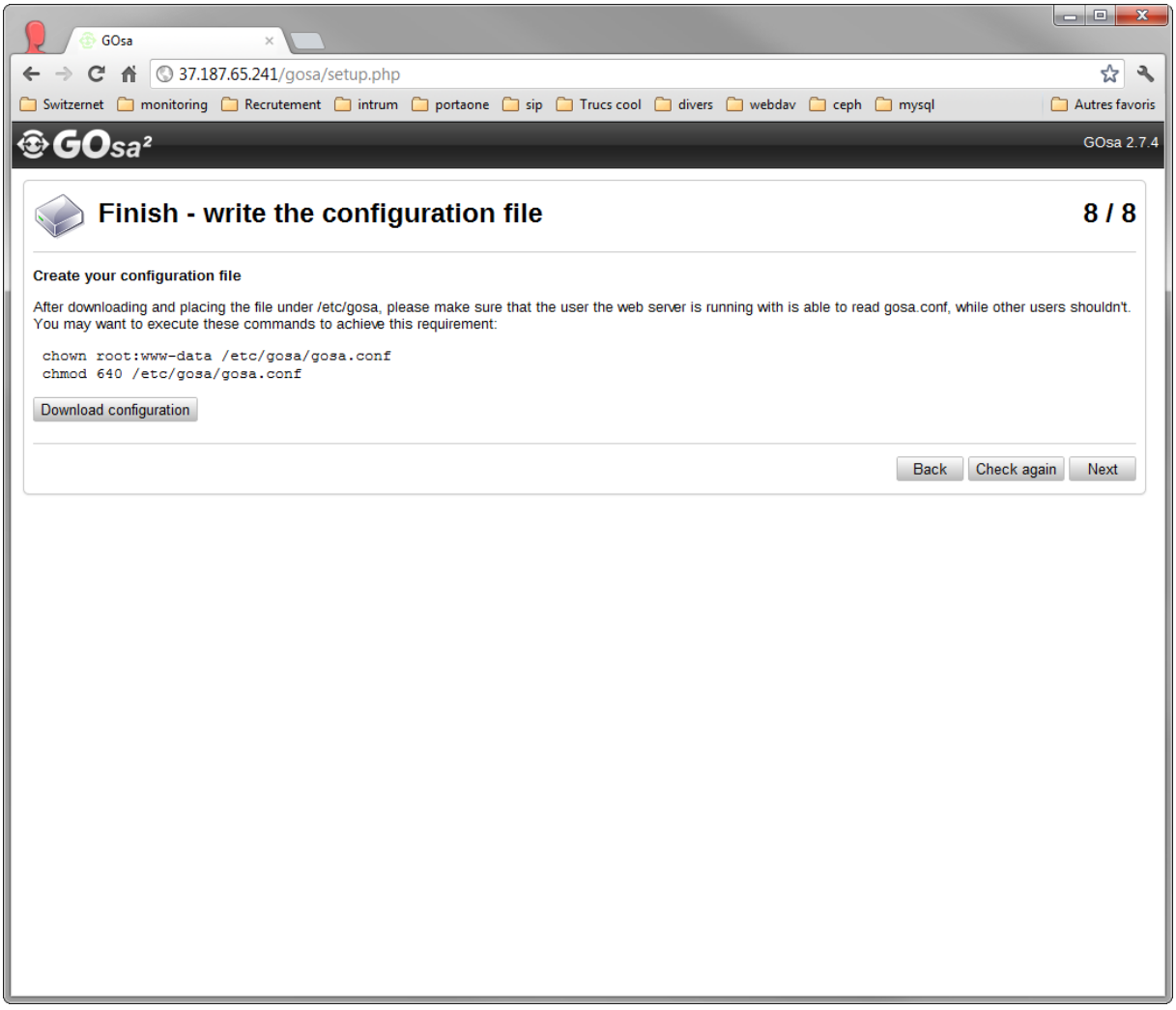

GOsa
37.187.65.241/gosa/setup.php
Switzernet
monitoring
Recrutement
intrum
portaone
sip
Trucs cool
divers
webdav
ceph
mysql
Autres favoris
GOsa²
GOsa 2.7.4
License
3 / 8
GOsa is developed under the terms of the GNU General Public License v2. Please accept the terms below.
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007
Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The GNU General Public License is a free, copyleft license for
software and other kinds of works.
The licenses for most software and other practical works are designed
to take away your freedom to share and change the works. By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users. We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors. You can apply it to
your programs, too.
When we speak of free software, we are referring to freedom, not
price. Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.
To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights. Therefore, you have
I have read the license and accept it
Back
Next


GOsa
37.187.65.241/gosa/setup.php
Switzernet
monitoring
Recrutement
intrum
portaone
sip
Trucs cool
divers
webdav
ceph
mysql
Autres favoris
GOsa²
GOsa 2.7.4
LDAP connection setup
4 / 8
The main data source used in GOsa is LDAP. In order to access the information stored there, please enter the required information.
LDAP connection
Location name
default
Connection URI
ldap://localhost:389
TLS connection
No
Base
dc=switzernet,dc=com
Authentication
Administrator DN
cn=admin,dc=switzernet,dc=com
Automatically append LDAP base to administrator DN
Administrator password
Schema based settings
Use RFC 2307bis compliant groups
No
Current status
Information
Bind as user 'cn=admin,dc=switzernet,dc=com' to server 'ldap://localhost:389' succeeded!
Back
Check again
Next


GOsa
37.187.65.241/gosa/setup.php
Switzernet
Recrutement
intrum
portaone
sip
Trucs cool
divers
webdav
ceph
mysql
Autres favoris
Souhaitez-vous que Chromium enregistre votre mot de passe ?
Enregistrer le mot de passe
Jamais pour ce site
GOsa²
GOsa 2.7.4
LDAP schema check
5 / 8
Schema specific settings
Schema check succeeded
Back
Check again
Next


GOsa
37.187.65.241/gosa/setup.php
Switzernet
monitoring
Recrutement
intrum
portaone
sip
Trucs cool
divers
webdav
ceph
mysql
Autres favoris
GOsa²
GOsa 2.7.4
LDAP inspection
6 / 8
During the LDAP inspection, we're going to check for several common pitfalls that may occur when migration to GOsa base LDAP administration. You may want to fix the problems below, in order to provide smooth services.
Checking for root object OK
Inspecting object classes in root object OK
Checking permission for LDAP database OK
Checking for super administrator OK
Users: gosa-admin
Back
Check again
Next

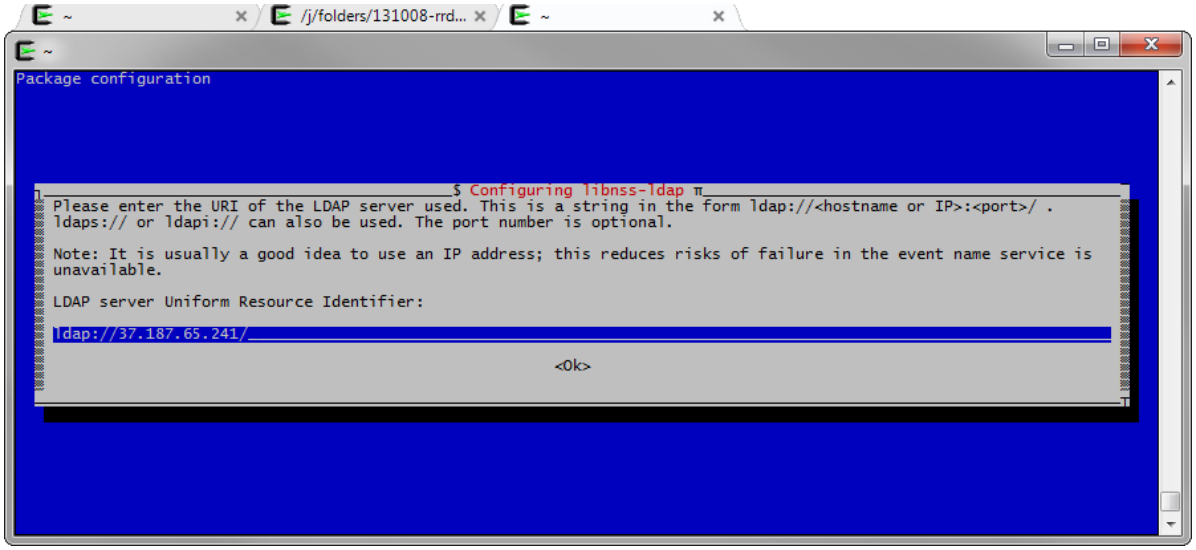

GOsa
37.187.65.241/gosa/setup.php
Switzernet
monitoring
Recrutement
intrum
portaone
sip
Trucs cool
divers
webdav
ceph
mysql
Autres favoris
When checking this option, GOsa will try to connect http://oss.gonicus.de in order to submit your form anonymously.
Generic
Did the setup procedure help you to get started?
Yes
No
If not, what problems did you encounter:
Is this the first time you use GOsa?
Yes
No, I use it since
2013
What operating system / distribution do you use?
What web server do you use?
Apache/2.2.22 (Debian)
What PHP version do you use?
5.4.4-14+deb7u4
GOsa version
GOsa 2.7.4
LDAP
What kind of LDAP server(s) do you use?
How many objects are in your LDAP?
Features
What features of GOsa do you use?
UNIX accounts/groups
Samba management
Mail system management
FAX system administration
Asterisk administration
System inventory
System/Configuration management
Address book
What features do you want to see in future versions of GOsa?
Send feedback
Back
Next

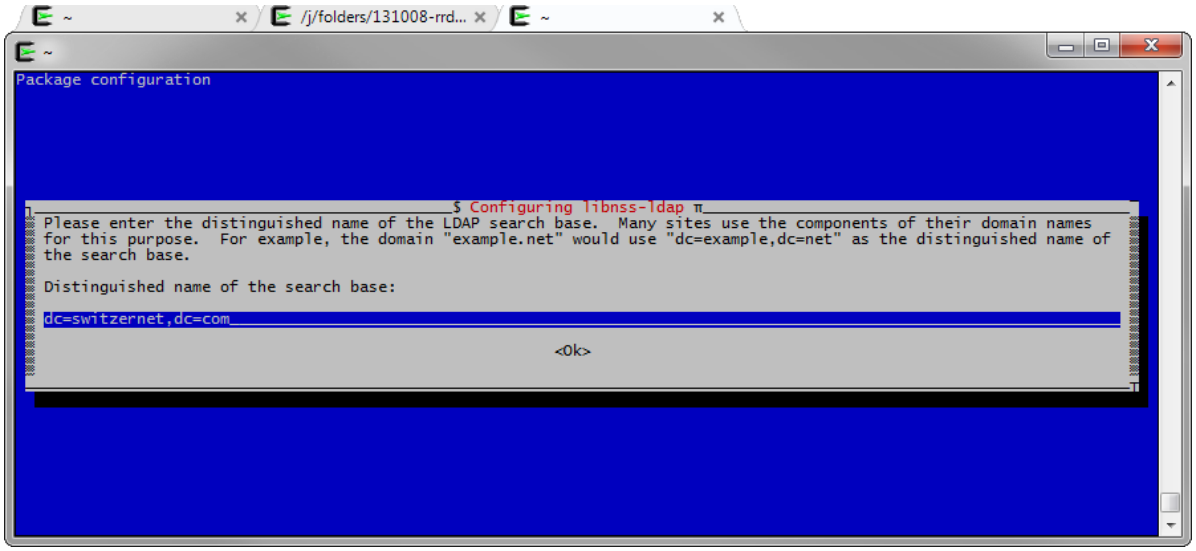


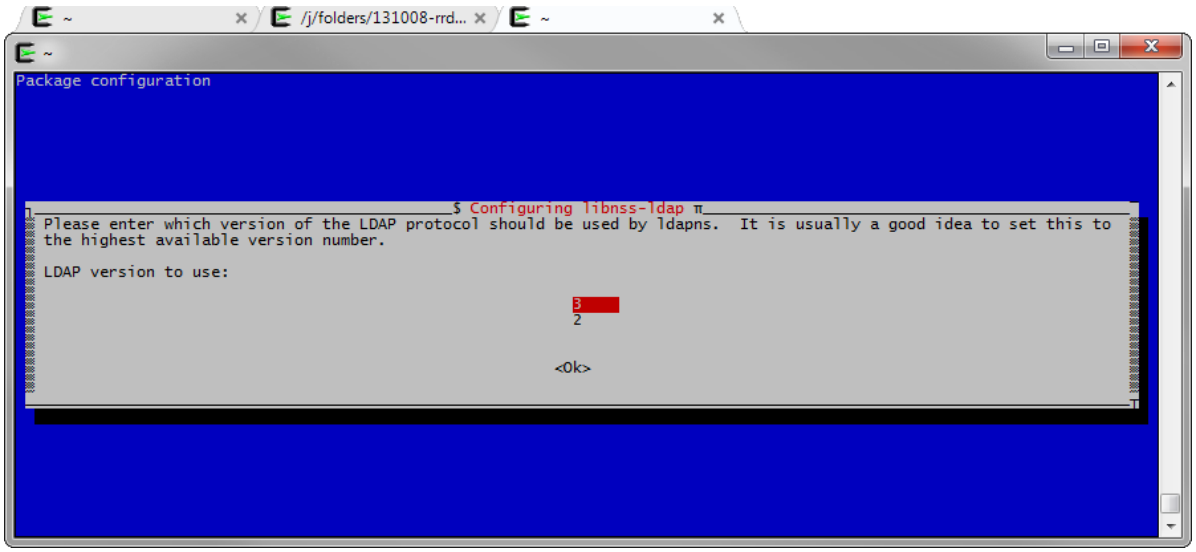
Install ldap client

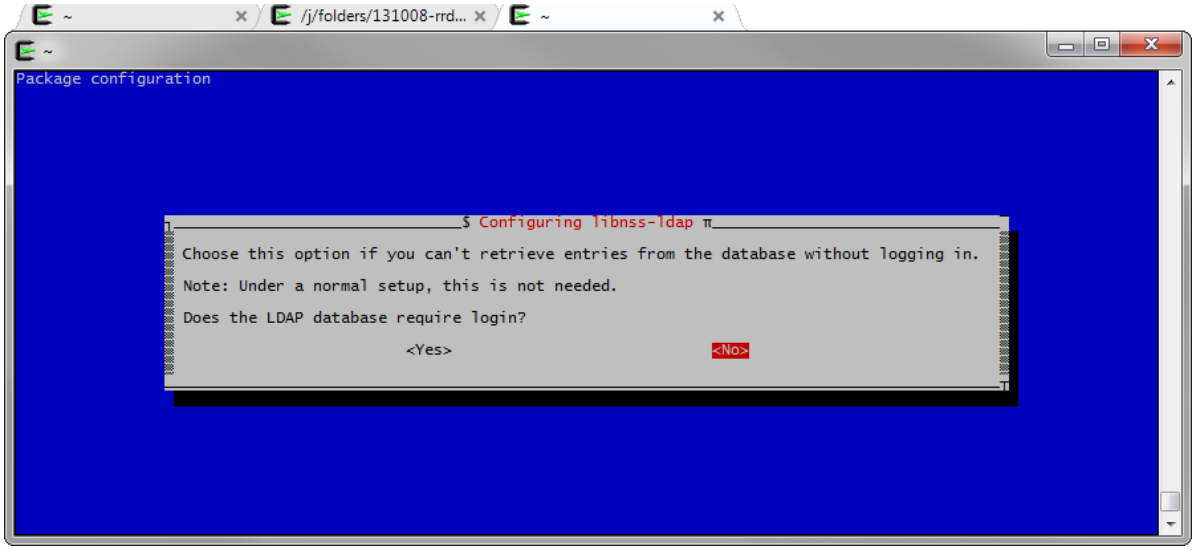
```
root@client:~# aptitude install libnss-ldap
```

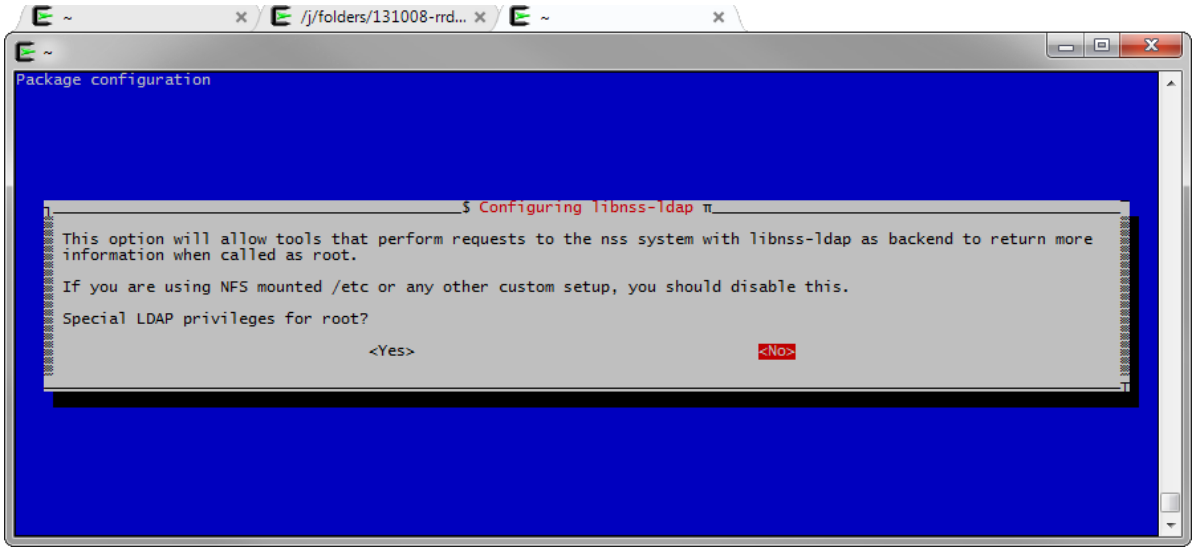
And complete the required fields:

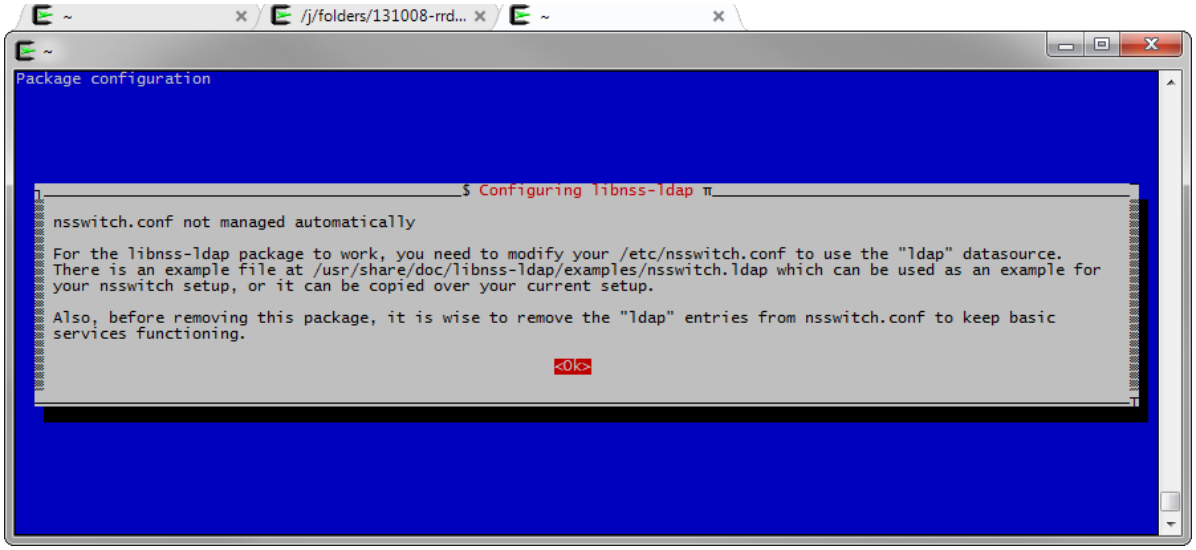

Package configuration
Configuring libnss-ldap
Please enter the URI of the LDAP server used. This is a string in the form ldap://<hostname or IP>:<port>/ . ldaps:// or ldapi:// can also be used. The port number is optional.
Note: It is usually a good idea to use an IP address; this reduces risks of failure in the event name service is unavailable.
LDAP server Uniform Resource Identifier:
ldap://37.187.65.241/
<Ok>

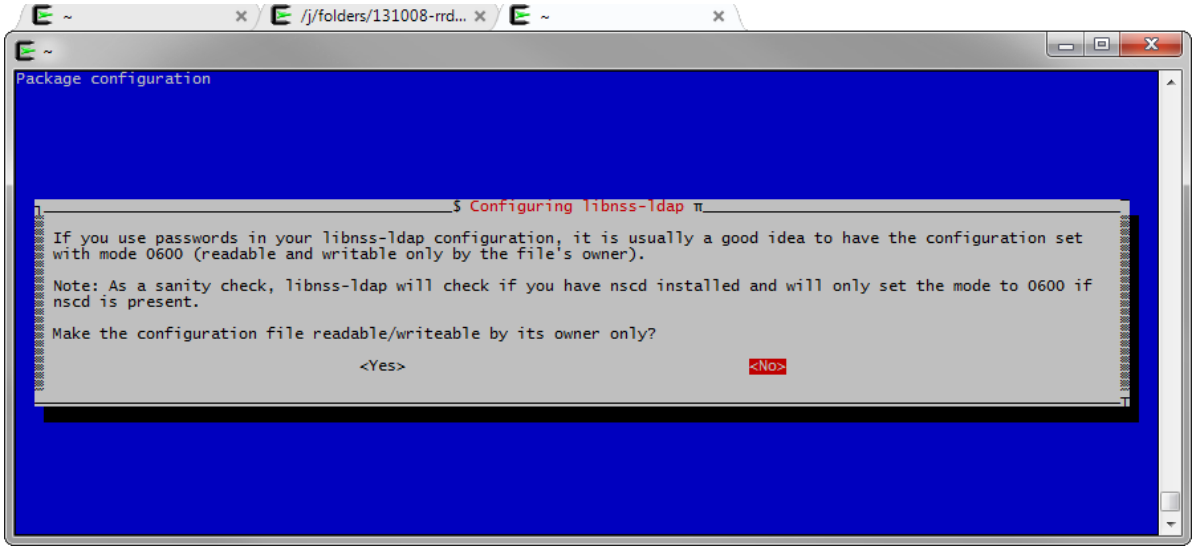

Package configuration
Configuring libnss-ldap
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.
Distinguished name of the search base:
dc=switzernet,dc=com
<Ok>


Package configuration
Configuring libnss-ldap
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version number.
LDAP version to use:
3
2
<Ok>


Package configuration
Configuring libnss-ldap
Choose this option if you can't retrieve entries from the database without logging in.
Note: Under a normal setup, this is not needed.
Does the LDAP database require login?
<Yes>
<No>


Package configuration
Configuring libnss-ldap
This option will allow tools that perform requests to the nss system with libnss-ldap as backend to return more information when called as root.
If you are using NFS mounted /etc or any other custom setup, you should disable this.
Special LDAP privileges for root?
<Yes>
<No>


Package configuration
Configuring libnss-ldap
nsswitch.conf not managed automatically
For the libnss-ldap package to work, you need to modify your /etc/nsswitch.conf to use the "ldap" datasource.
There is an example file at /usr/share/doc/libnss-ldap/examples/nsswitch.ldap which can be used as an example for your nsswitch setup, or it can be copied over your current setup.
Also, before removing this package, it is wise to remove the "ldap" entries from nsswitch.conf to keep basic services functioning.
<Ok>



Below are the pam.d configuration files without the comments (‘`egrep -v "^#|^[ ]*$" file`’ command). Add the missing lines and verify the values:

/etc/pam.d/common-auth

```
auth      [success=2 default=ignore]      pam_unix.so nullok_secure
auth      [success=1 default=ignore]      pam_ldap.so use_first_pass
auth      requisite                       pam_deny.so
auth      required                        pam_permit.so
auth      optional                        pam_smbpass.so migrate
```

/etc/pam.d/common-session

```
session       [default=1]                     pam_permit.so
session       requisite                       pam_deny.so
session       required                        pam_permit.so
session       required        pam_unix.so
session       optional                        pam_ldap.so
session       optional                        pam_ck_connector.so nox11
session required        pam_mkhomedir.so umask=0077
session optional      pam_umask.so
```

/etc/pam.d/common-account

```
account       [success=2 new_authtok_reqd=done default=ignore]
pam_unix.so
account       [success=1 default=ignore]      pam_ldap.so
account       requisite                       pam_deny.so
account       required                        pam_permit.so
```

/etc/pam.d/common-password

```
password     [success=2 default=ignore]      pam_unix.so obscure sha512
word     [success=1 user_unknown=ignore default=die]     pam_ldap.so
try_first_pass
password     requisite                       pam_deny.so
password     required                        pam_permit.so
password     optional                        pam_smbpass.so nullok
use_authtok use_first_pass
```

/etc/nsswitch.conf

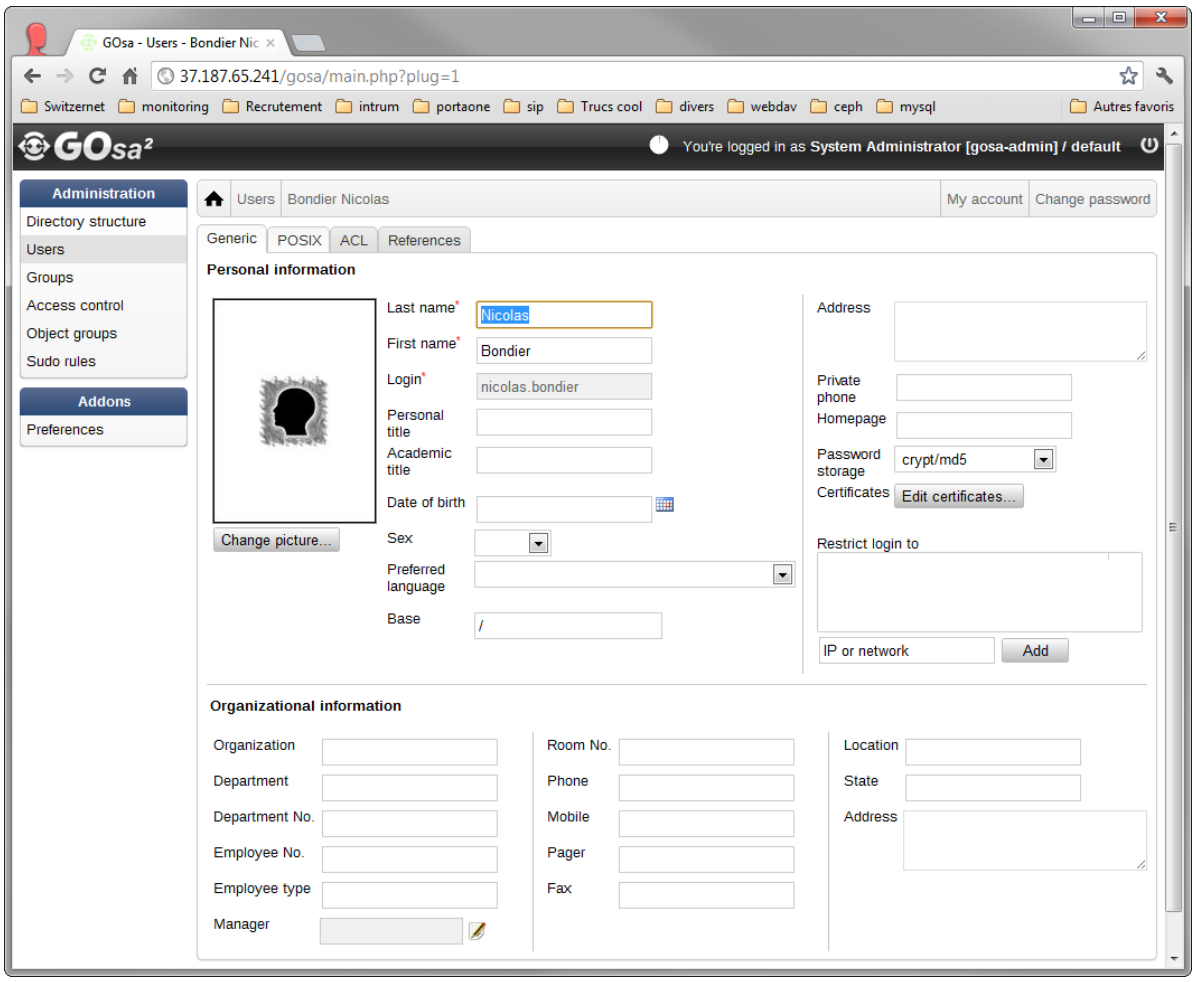
```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
netgroup:       nis
```

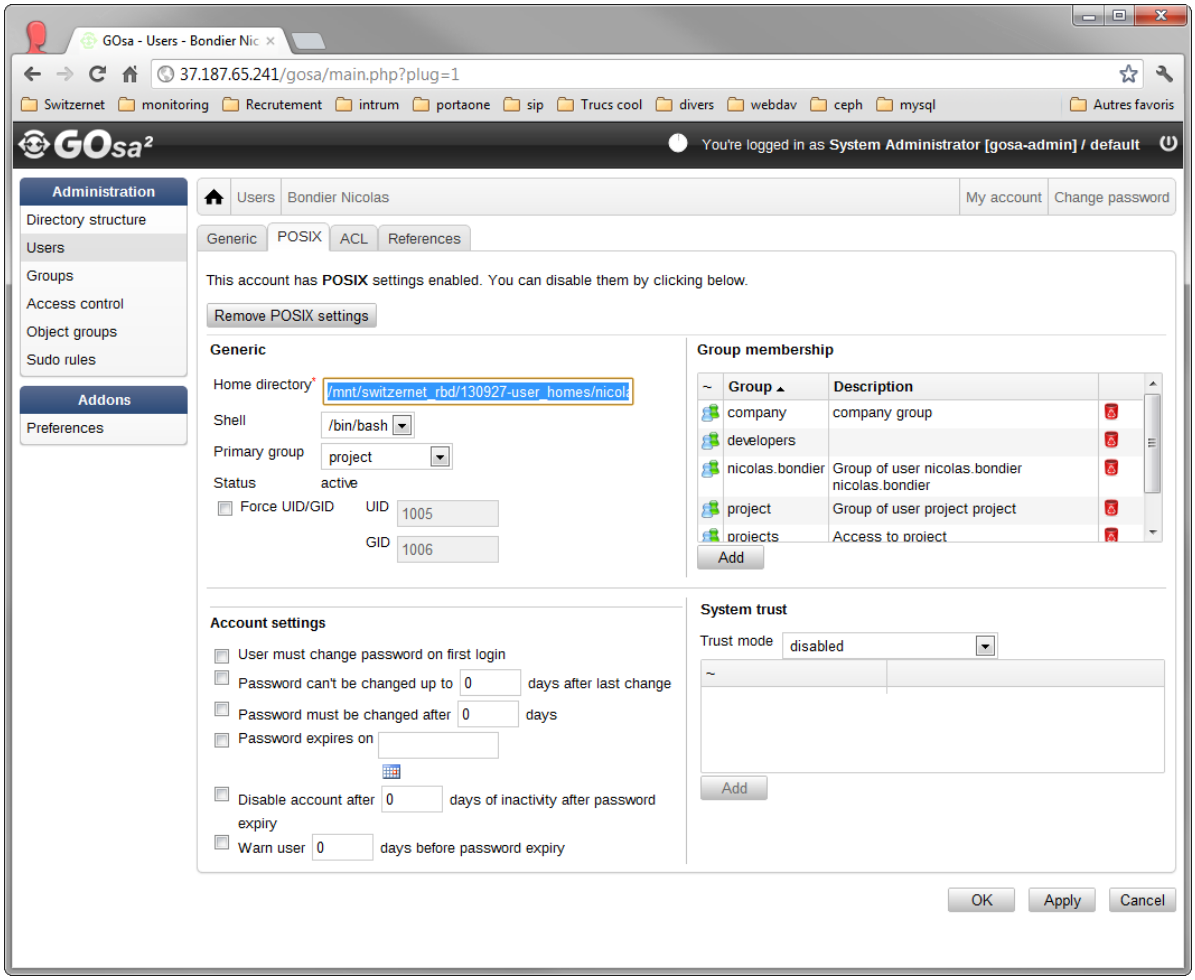
/etc/pam_ldap.conf

```
base dc=switzernet,dc=com
uri ldap://37.187.65.241/
ldap_version 3
pam_password crypt
```

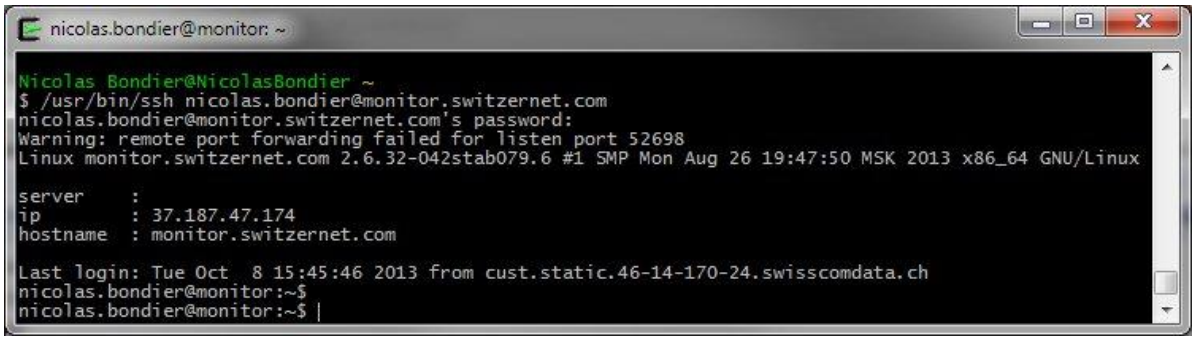
Connect with SSH

Create a user in Gosa and give him POSIX settings:





If everything worked, you should be able to login with your LDAP account.



Links

This document: http://switzernet.com/3/public/131007-ldap-gosa-unix/

Debian LDAP PAM: https://wiki.debian.org/fr/LDAP/PAM

Gosa: https://oss.gonicus.de/labs/gosa

OpenLDAP: http://www.openldap.org/

This document is related to the project including:

Ceph cluster: http://switzernet.com/3/public/130925-ceph-cluster/

Dovecot + Ceph: http://switzernet.com/3/public/130910-ceph-dovecot/

* * *