**Unix + PAM + LDAP**

Document created on 2013-10-09  
Nicolas Bondier

[[pdf](index.pdf)][[doc](index.docx)][[htm](index.htm)]

Contents

[Introduction 3](#_Toc369012287)

[Prerequisites 3](#_Toc369012288)

[Install OpenLDAP server 3](#_Toc369012289)

[Install ldap client 12](#_Toc369012290)

[Connect with SSH 17](#_Toc369012291)

[Links 19](#_Toc369012292)

# 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

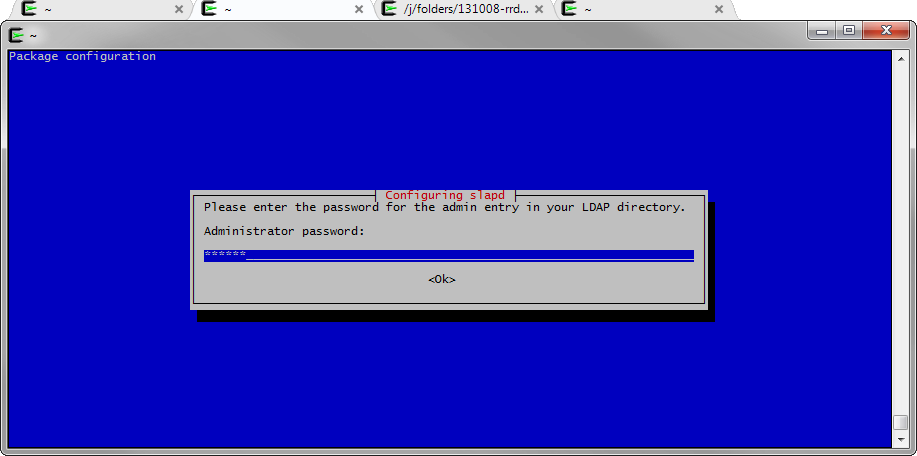
No prerequisites. We need one server for LDAP and a second one for the authentication.

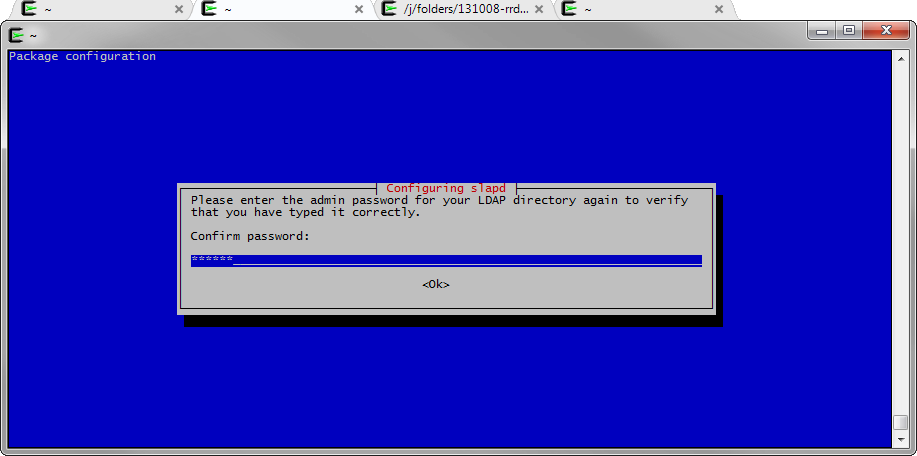
# Install OpenLDAP server

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

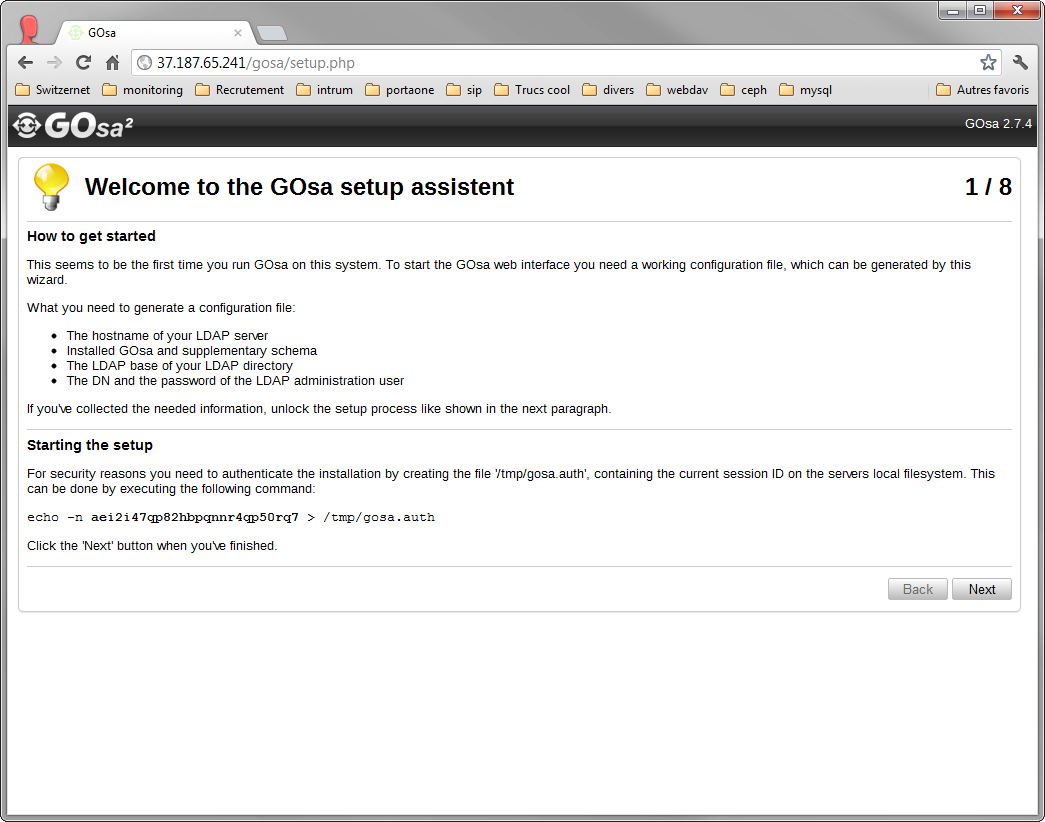
/etc/dyngroup.ldif;

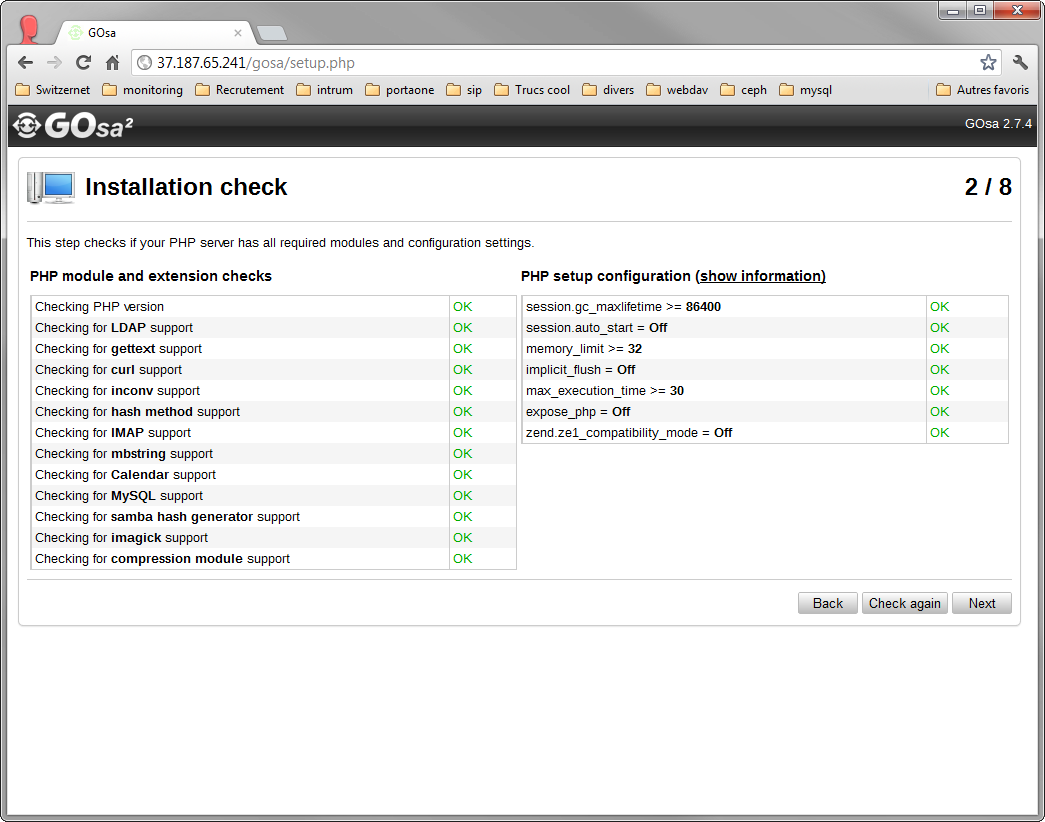
do ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/$schema || exit 1; done

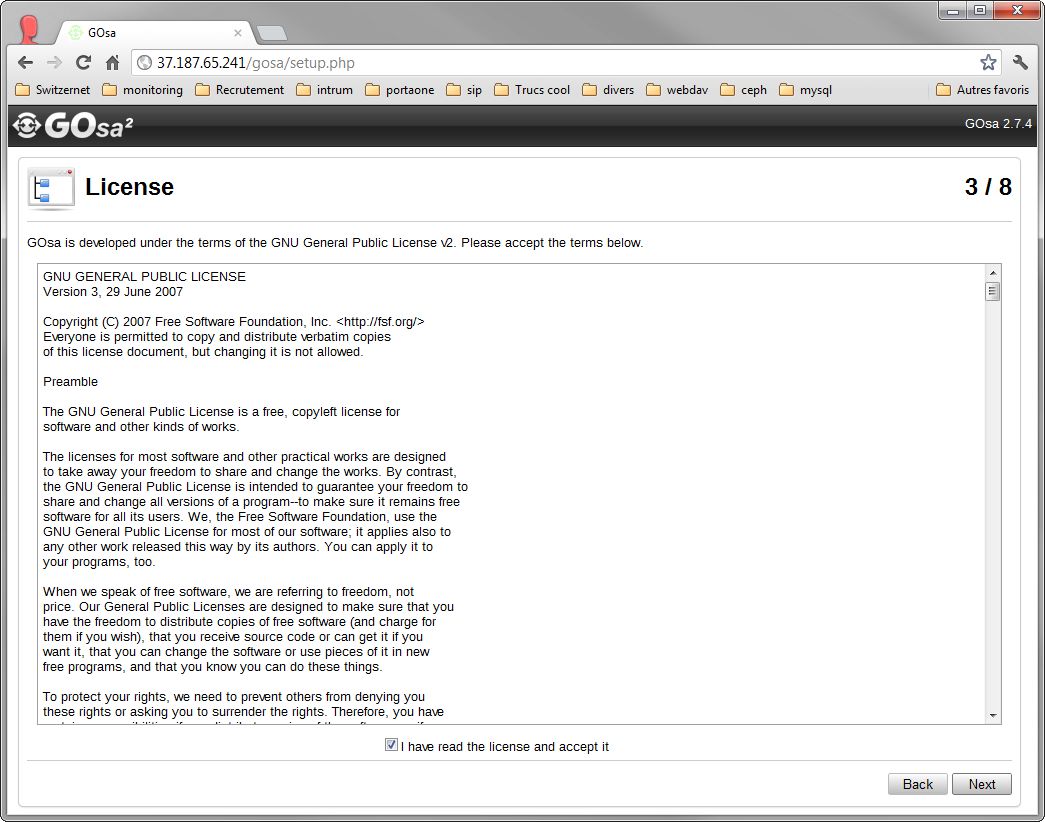
Restart your ldap:

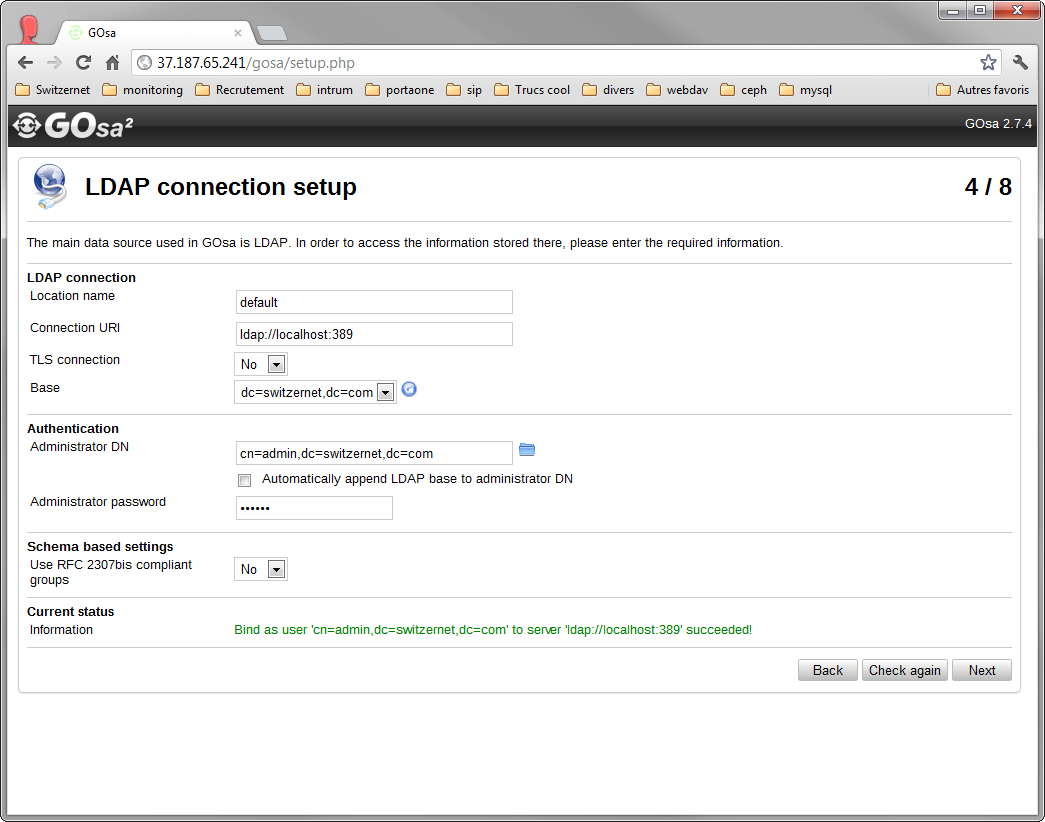
root@ldap:~# /etc/init.d/slapd start

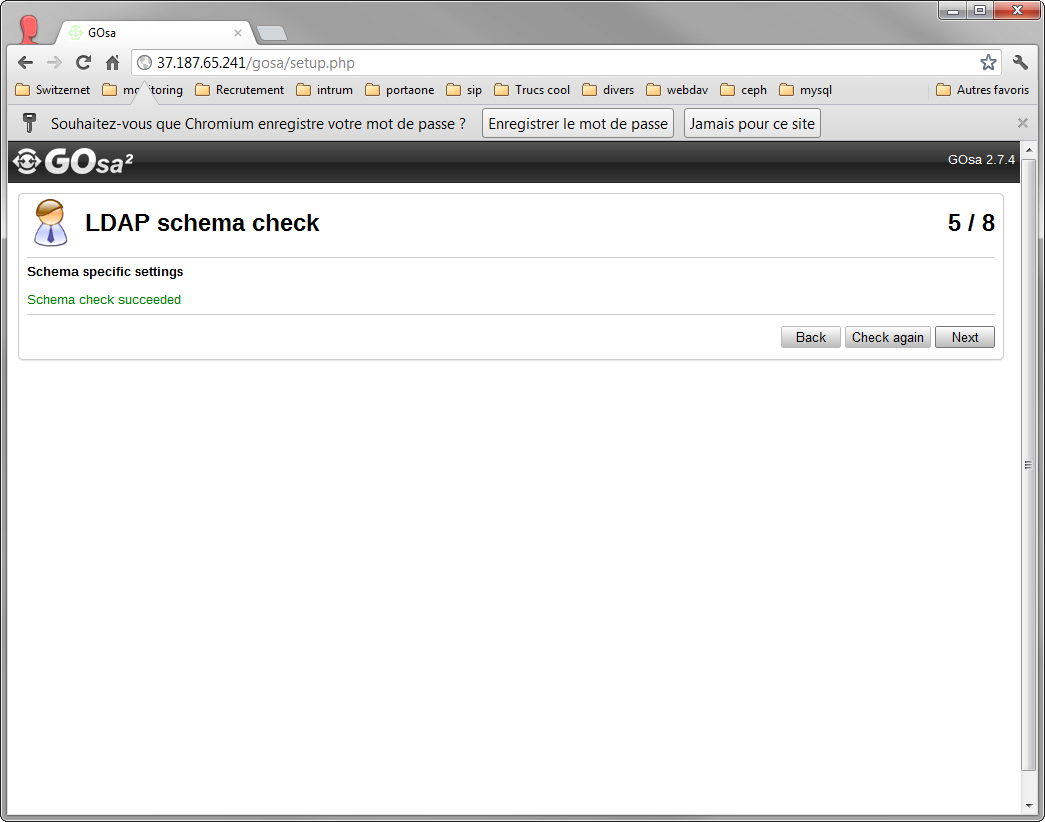
Go to the Gosa configuration interface (http://ldap-server/gosa/), and follow the instructions for configuring Gosa:

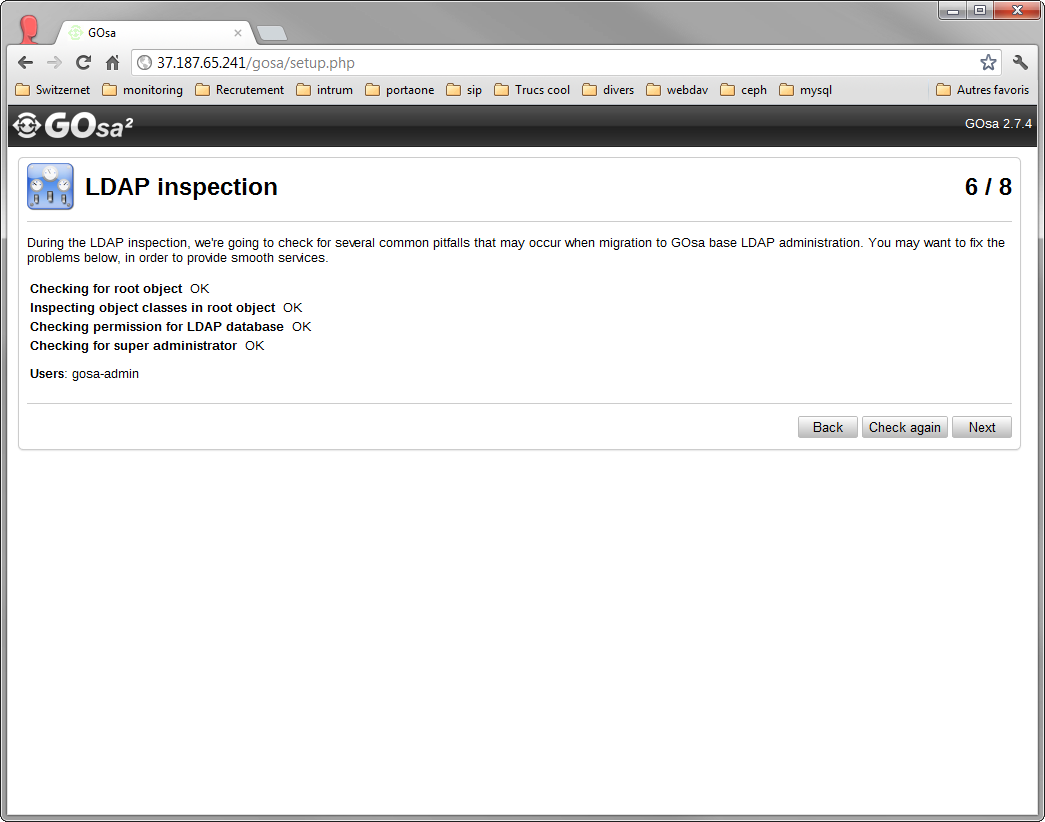


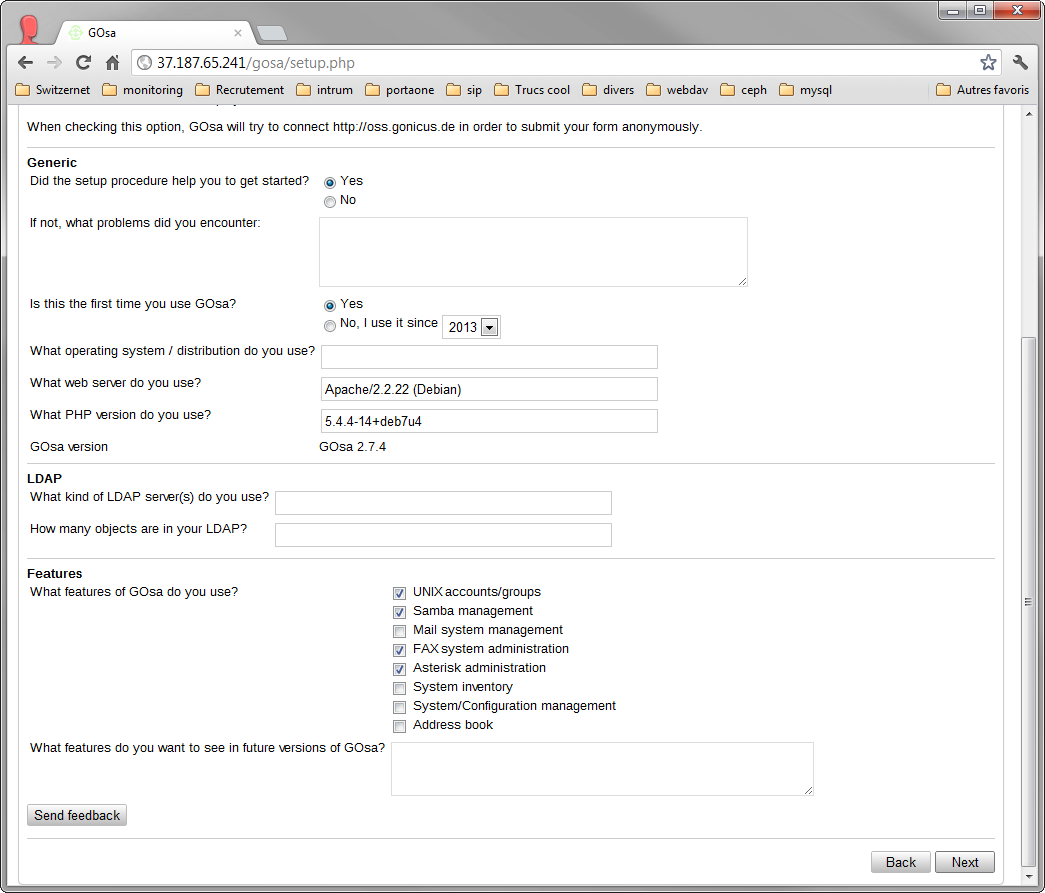


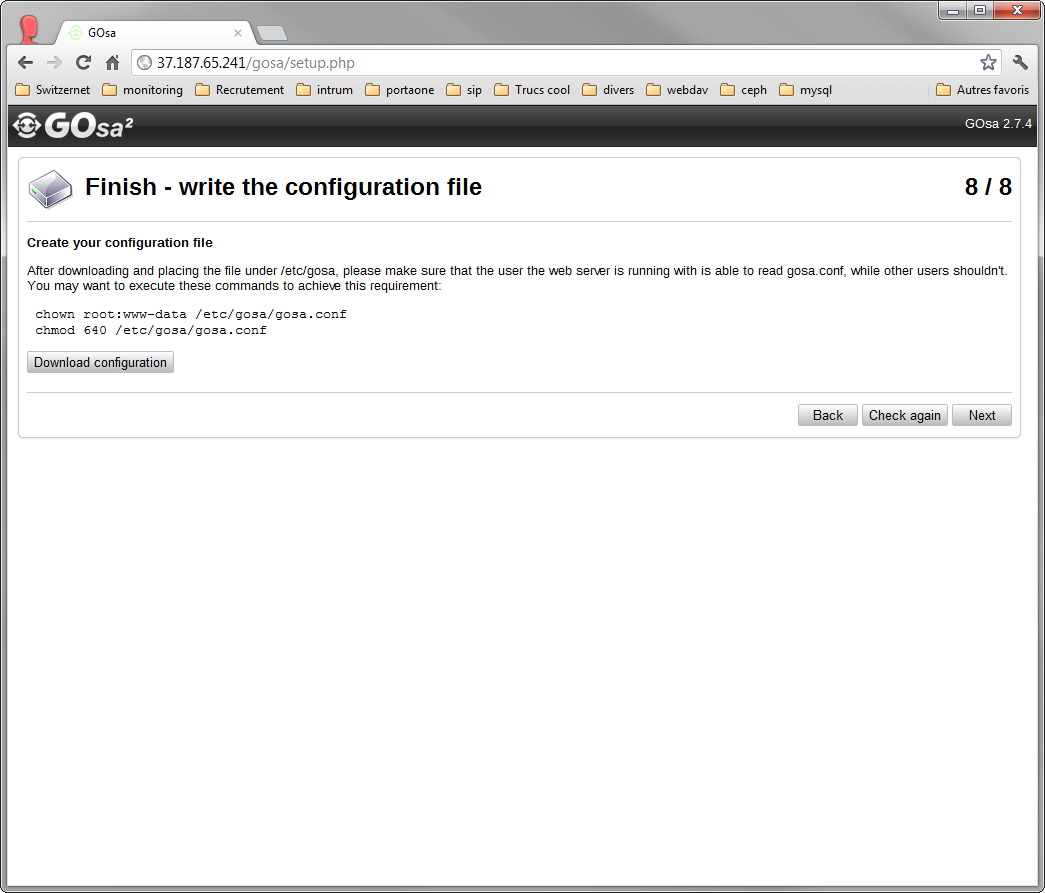








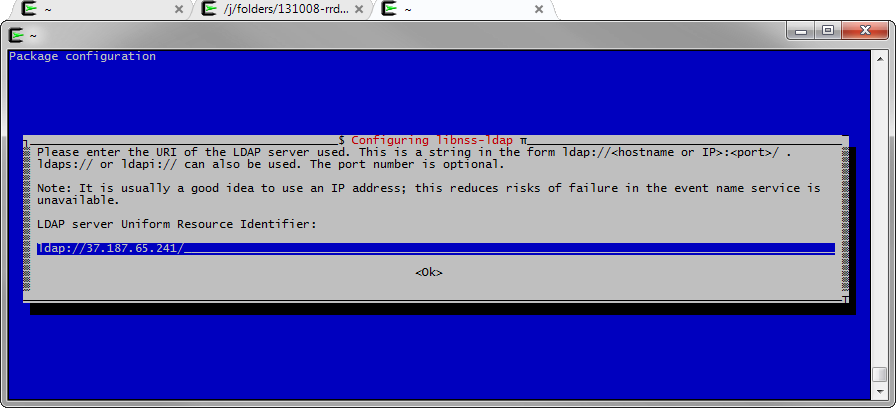


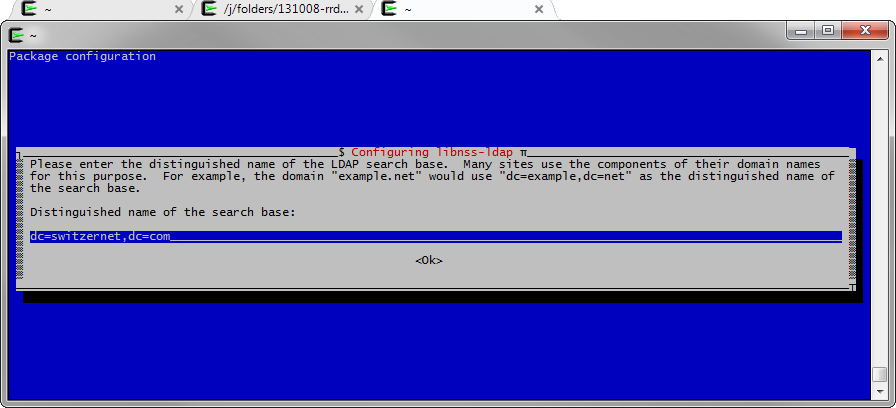


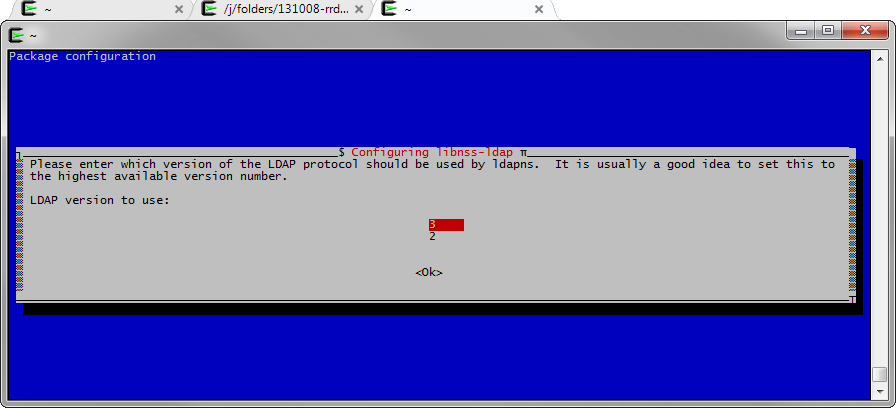
# Install ldap client

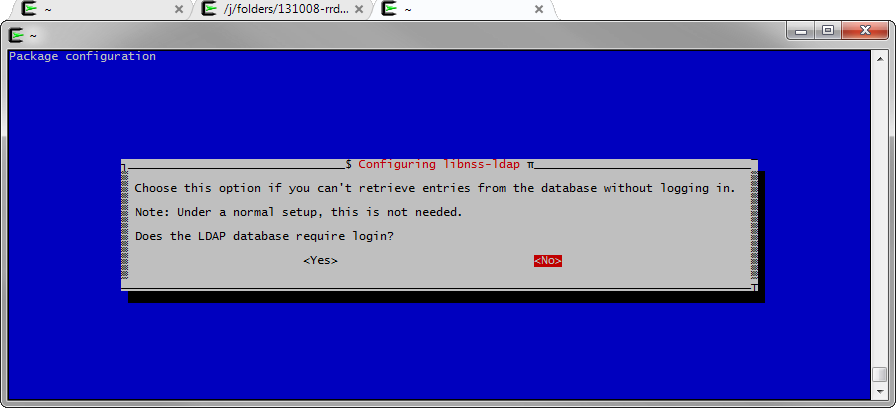
root@client:~# aptitude install libnss-ldap

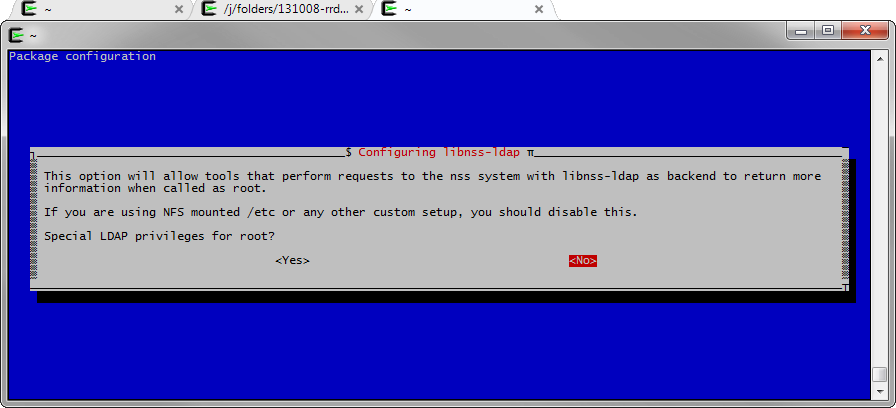
And complete the required fields:

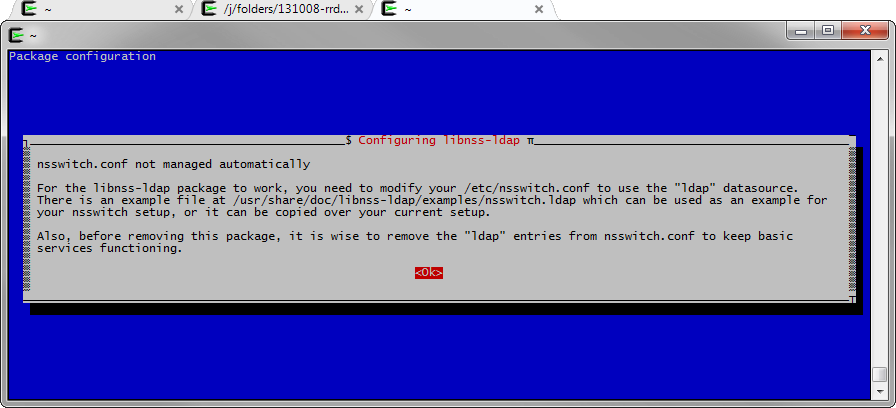


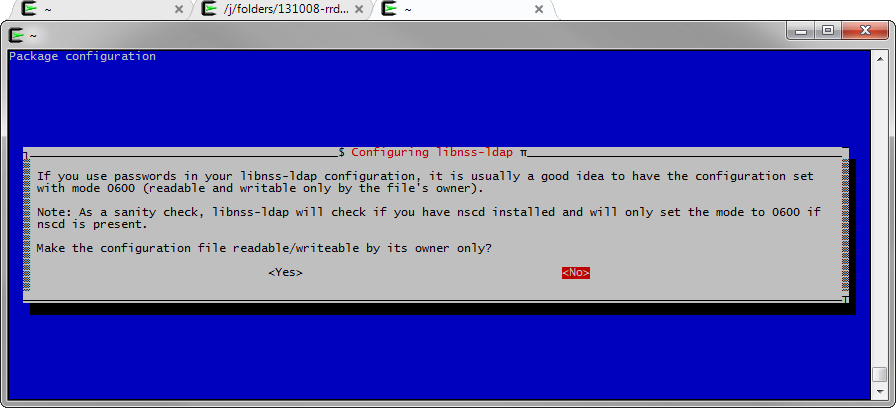












Below are the pam.d configuration files without the comments (‘egrep -v "^#|^[ ]\*$" file’ command). Add the missing lines and verify the values:

/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

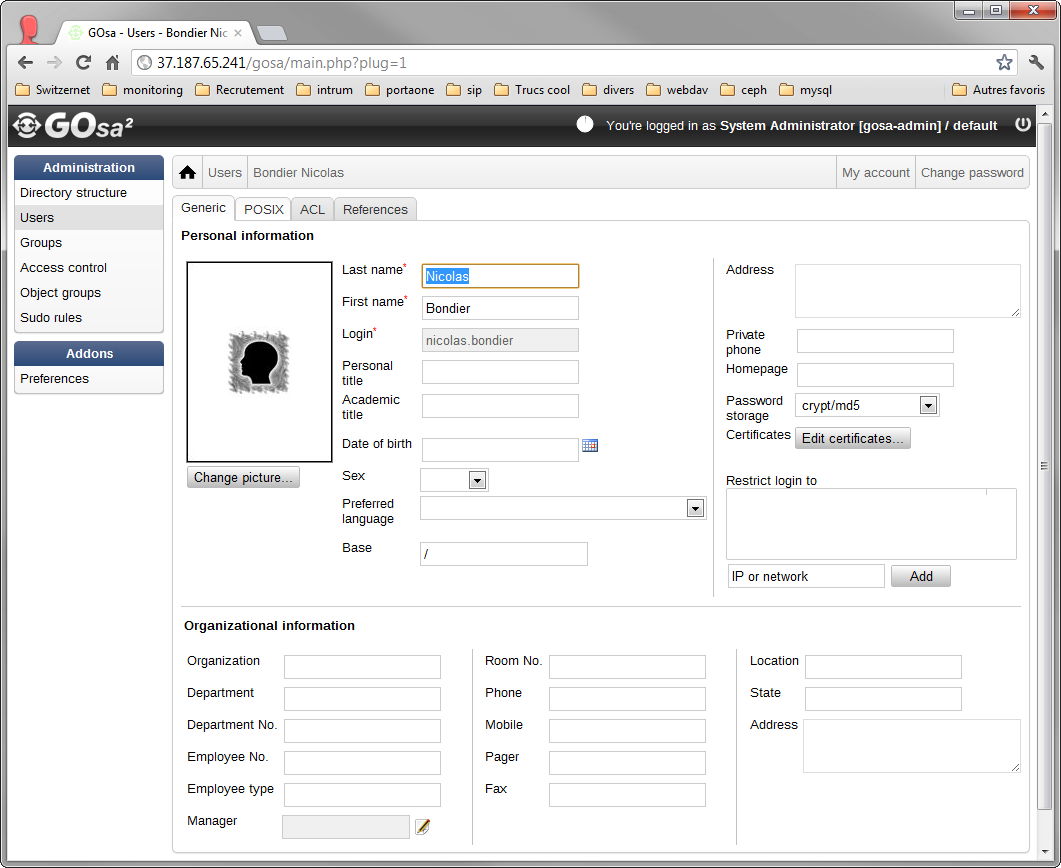
uri ldap://37.187.65.241/

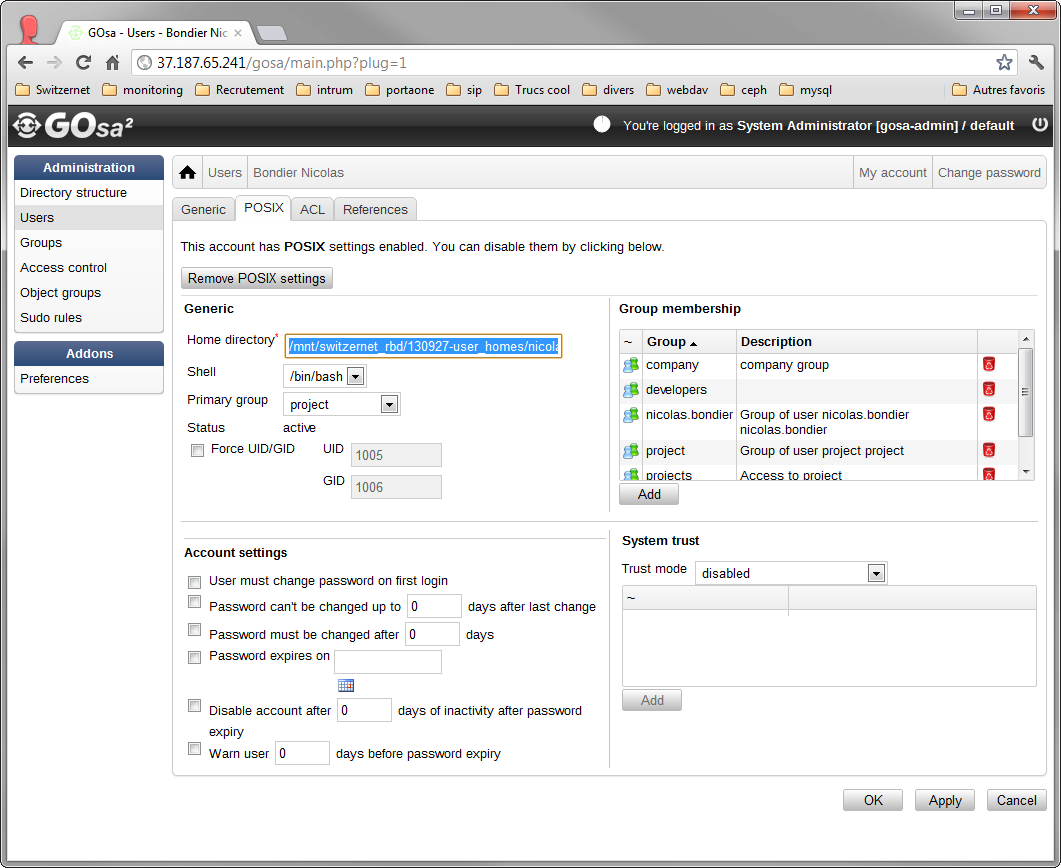
ldap\_version 3

pam\_password crypt

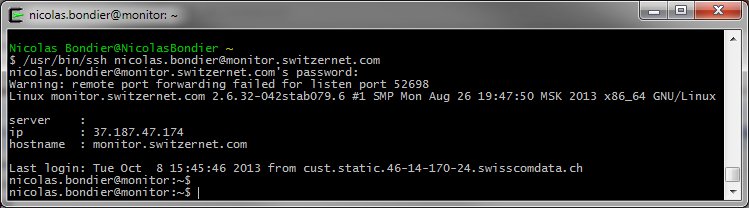
# Connect with SSH

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/>

\* \* \*



Copyright © 2013 by Switzernet