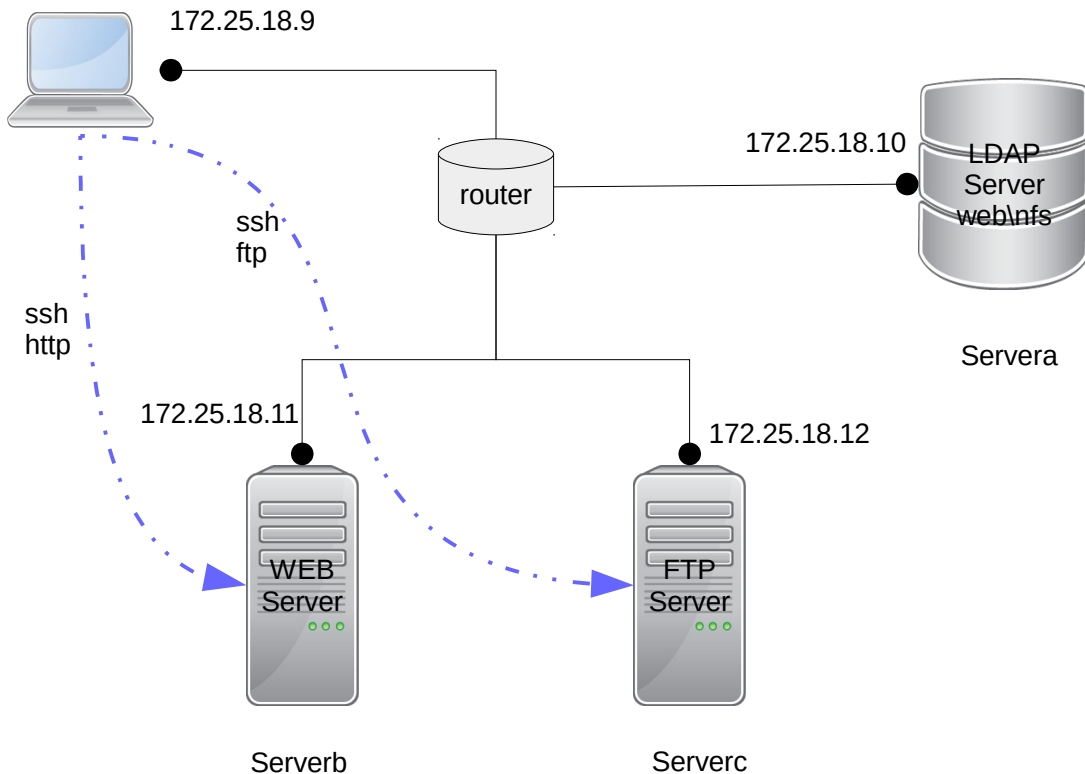


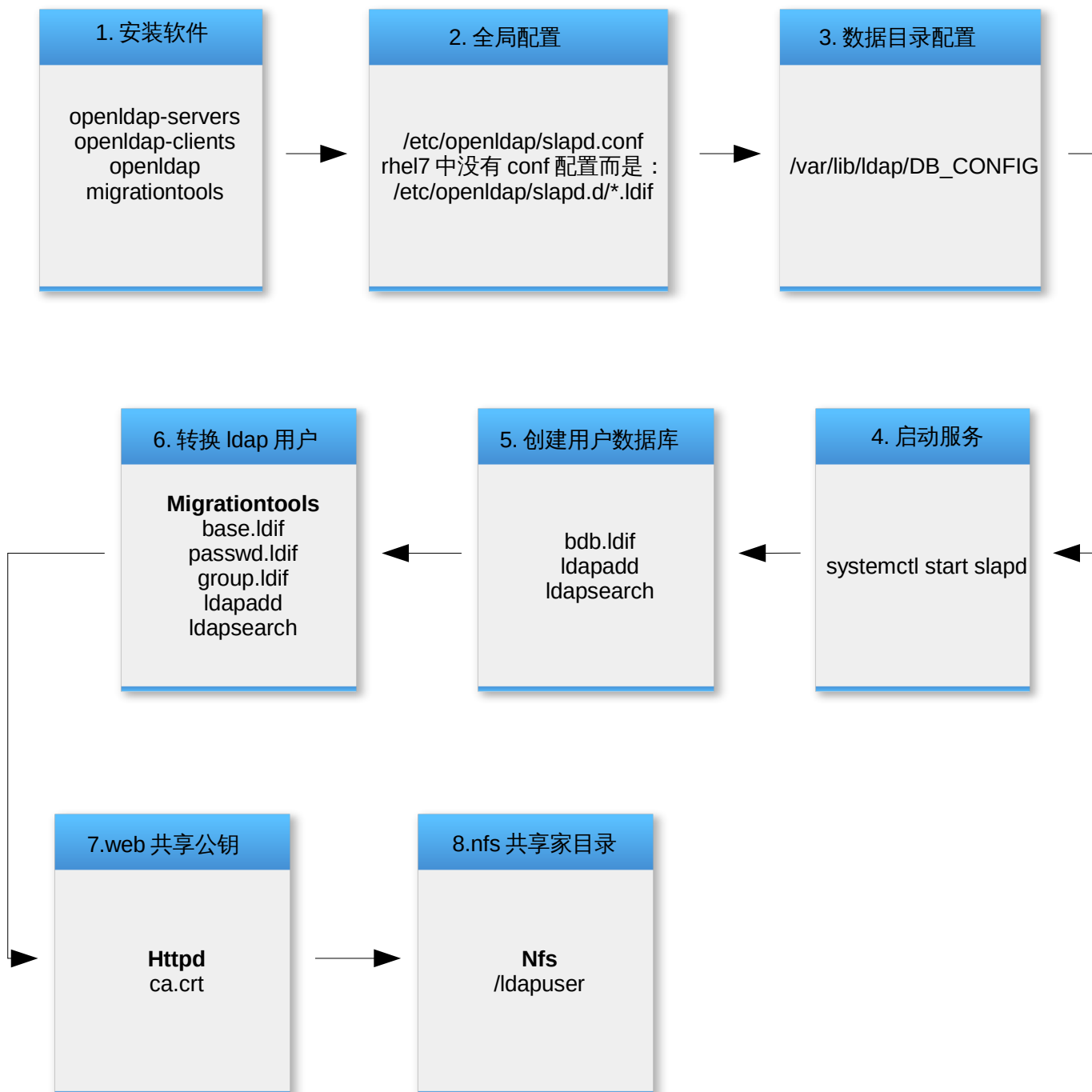
OPENLDAP 认证系统实验



server	ip	software	role
servera	172.25.18.10	openldap-servers openldap-clients openldap migrationtools	ldap 服务端
serverb	172.25.18.11	httpd lmod_ldap openldap-clients openldap nss-pam-ldapd autofs	web 服务器 ldap 客户端
serverc	172.25.18.12	Vsftpd openldap-clients openldap nss-pam-ldapd autofs	ftp 服务器 ldap 客户端
workstation	172.25.18.9	firefox	web 和 ftp 服务的客户端



OPENLDAP Server 端配置概览



OPENLDAP Client 端配置概览



1. 软件安装

```
openldap-clients
openldap
nss-pam-ldapd
autofs
```

2. 添加 ldap 认证

```
authconfig --enableldap --enableldapauth
--ldapserver=servera.pod18.example.com
--ldapbasedn='dc=example,dc=org'
--enableldaptls
--ldaploadcacert=http://servera.pod18.example.com/ca/ca.crt
--update
```

3. autofs 自动挂接 ldap 用户家目录

```
* -rw,soft,intr servera.pod18.example.com:/ldapuser/&
```



1. 软件安装

```
Httpd
mod_ldap
```

2. 修改认证配置

```
LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/ca.crt
<VirtualHost *:80>
    servername www.ldapuser.com
    Documentroot /var/www/ldapuser.com
</VirtualHost>

<Directory /var/www/ldapuser.com>
    authname ldap
    authtype basic
    authbasicprovider ldap
    authldapurl
    "ldap://servera.pod18.example.com/dc=example,dc=org"
    TLS
    require valid-user
</Directory>
```

3. 启动 httpd 服务