LDAP Auth - CentOS 7 - SSH RSA - Group Restrictions - Sudo Access

Install

```
yum -y install openldap-clients nss-pam-ldapd git
```

Basic Configuration

```
authconfig --enableldap \
--enableldapauth \
--ldapserver={ldap.domain.com,192.168.1.255} \
--ldapbasedn="dc=domain,dc=com" \
--enablemkhomedir \
--update
```

Restrict to Group Access ServerAdmins

```
cat << 'EOL' >/etc/ldap.restrictions
root
wheel
ServerAdmins
EOL
```

```
nano /etc/pam.d/system-auth
```

Insert @ top of File

```
auth required pam_listfile.so onerr=fail item=group sense=allow file=/etc/ldap.restrictions
```

```
systemctl restart nslcd
```

Enable Home Directory Creation

```
cat << EOL >mkhomedir.te
# create new
module mkhomedir 1.0;
require {
type unconfined_t;
type oddjob_mkhomedir_exec_t;
class file entrypoint;
}
#============= unconfined_t ==============
allow unconfined_t oddjob_mkhomedir_exec_t:file entrypoint;
EOL
```

```
checkmodule -m -M -o mkhomedir.mod mkhomedir.te
semodule_package --outfile mkhomedir.pp --module mkhomedir.mod
semodule -i mkhomedir.pp
```

Enable RSA SSH Key Authentication

(Don't have RSA Key Auth setup on Server? >> Install LDAP + PHPLDAPAdmin - Ubuntu 14)

```
rpm -iUvh http://dl.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm
yum install -y epel-release
yum install -y python-pip python-ldap python-devel openldap-devel gcc
pip install ssh-ldap-pubkey
sh -c 'echo "AuthorizedKeysCommand /usr/bin/ssh-ldap-pubkey-wrapper" >> /etc/ssh/sshd_config'
sh -c 'echo "AuthorizedKeysCommandUser nobody" >> /etc/ssh/sshd_config'
```