

MS AD (legacy)

LDAP-

1.

WNAM , WNAM, Linux- .

Samba, :

```
apt-get install samba winbind
```

/etc/samba/smb.conf:

```
[global]
workgroup = <__>
server string = %h server (Samba, Ubuntu)
dns proxy = no
security = ads
password server = <__>
realm = <__>
log file = /var/log/samba/log.%m
max log size = 1000
syslog = 0
panic action = /usr/share/samba/panic-action %d
server role = standalone server
passdb backend = tdbsam
obey pam restrictions = yes
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
pam password change = yes
map to guest = bad user
usershare allow guests = yes
```

:

```
testparm
```

Samba:

```
systemctl unmask samba
systemctl enable samba
systemctl restart samba

/etc/init.d/nmbd restart
/etc/init.d/smbd restart
```

Samba , :

```
net ads join -U <__>
```

```
/etc/init.d/winbind restart
```

(: wifitest, : wifitest) Samba :

```
ntlm_auth --request-nt-key --domain=<__> --username=wifitest --password=wifitest
```

-, WNAM . nginx (WNAM) /etc/nginx/sites-available/wnam :

```

server {
    listen 80 default_server;

    root /var/www/html;

    server_name _;

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_read_timeout 120;
        proxy_connect_timeout 120;
    }

    location ~ ^/cgi {

        root /home/wnam/cgi;
        rewrite ^/cgi/(.*) /$1 break;

        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/var/run/fcgiwrap.socket;
        fastcgi_param SCRIPT_FILENAME /home/wnam/cgi$fastcgi_script_name;
    }
}

```

FastCGI:

```

apt install fcgiwrap
systemctl restart nginx

```

ntlmauth.cgi . **/usr/bin/ntlm_auth.** **/home/wnam/cgi/ () " ":**

```

mkdir /home/wnam/cgi
cd /home/wnam/cgi
wget -O ntlmauth.cgi https://netams.com/files/wnam/misc/ntlmauth.cgi
chmod +x ntlmauth.cgi

```

FastCGI- :

```

chmod a+x /home/wnam && chmod a+x /home/wnam/cgi

```

nginx (www-data) winbindd_priv, , winbindd:

```

usermod -a -G winbindd_priv www-data
chown root:www-data /var/lib/samba/winbindd_privileged/

```

- :

```

/usr/bin/ntlm_auth --request-nt-key --username=wifitest --challenge=89b2cc47d4571192 --nt-
response=7413e0e319aa658f2214baadb65c131da88b767ab7771f17
wget -O - 'http://localhost/cgi/ntlmauth.cgi?username=wifitest&challenge=89b2cc47d4571192&nt-
response=7413e0e319aa658f2214baadb65c131da88b767ab7771f17'

```

:

```

NT_KEY: 535A15A134F3555A8089A772D0591D4C

```

Active Directory WNAM. , ():


```

chmod a+s /usr/bin/ntlm_auth

```

"" : support@netams.com.

2.

 WNAM , (), samba+nginx+ntlmauth.

WNAM, "" "" " Active Directory".

Имя домена

main

Имя контроллера домена

dcb1

Учётная запись

Пароль

URL для NTLM проверки

http://localhost/cgi/ntlmauth.cgi

Обновить список групп

Удалить

Сохранить

FQDN , (,), (, -). URL - NTLM-, . () - : <http://localhost/cgi/ntlmauth.cgi> , "".

" " , .

 .

. ().

#	Имя группы	Путь группы в AD
<input type="checkbox"/>	Exchange Servers	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	Exchange Organization Administrators	CN=Exchange Organization Administrators,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	Exchange Recipient Administrators	CN=Exchange Recipient Administrators,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	Exchange View-Only Administrators	CN=Exchange View-Only Administrators,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	Exchange Public Folder Administrators	CN=Exchange Public Folder Administrators,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	ExchangeLegacyInterop	CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=main,DC=example,DC=com
<input type="checkbox"/>	Domain Computers	CN=Domain Computers,CN=Users,DC=main,DC=example,DC=com
<input type="checkbox"/>	Group Policy Creator Owners	CN=Group Policy Creator Owners,CN=Users,DC=main,DC=example,DC=com
<input type="checkbox"/>	Users	CN=Users,CN=Builtin,DC=main,DC=example,DC=com
<input checked="" type="checkbox"/>	Domain Users	CN=Domain Users,CN=Users,DC=main,DC=example,DC=com

"" . WNAM MS AD . WNAM EAP-PEAP/MSCHAPv2 .