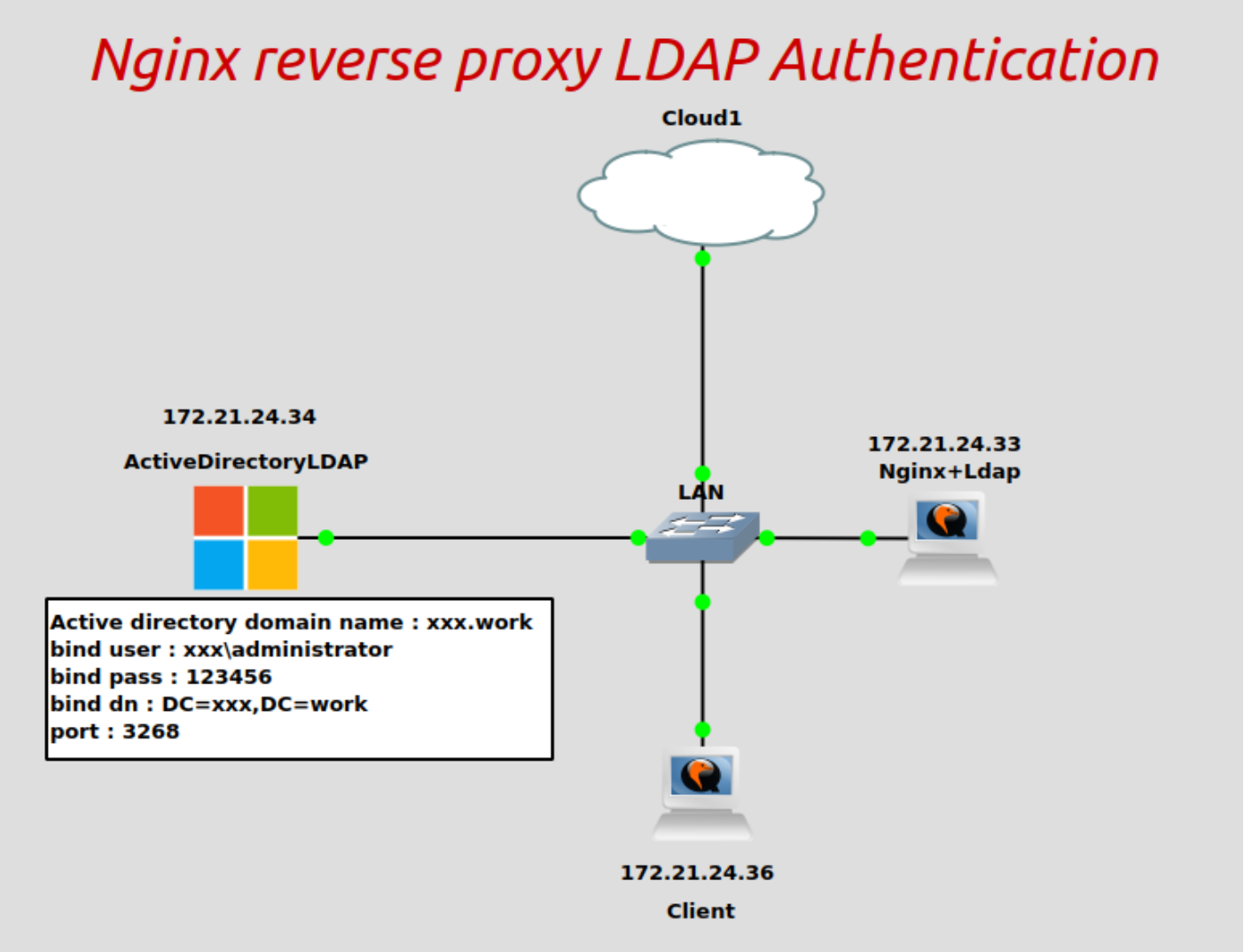
Nginx http load balance ve ldap authentication



Bu dökümanı takip edebilmek için admin seviyesinde linux tecrübesi gereklidir. Bu seviyede tecrübeniz eksik ise teknik destek ekibimizden yardım alabilirsiniz.

Bir müşterimizde kibana önüne koymak üzere active directory ldap entegrasyonu ile birlikte nginx reverse proxy çalıştırmamız gerekiyordu

Malum ngnix plus içerisinde gerekli modül pre-install şeklinde bulunyor fakat opensource olan versiyonda bu modülü bulamıyoruz.

Ancak,

```
https://github.com/kvspb/nginx-auth-ldap
```

Adresinden, opensource versiyon ile de kullanılabilen bir modülü indirebiliriz. modülü kullanabilmek için bir kaç ön şart var bunlar aşağıdaki gibi ;

- Ubuntu/Debian repolarındaki nginx bu modülü içermiyor bu sebeple source code kullanarak compile etmemiz gerekiyor
- Compile etmeden önce birkaç paket var bunları kurmak gerekiyor.
- kurduktan sonra da nginx.conf ve reverse proxy konfigürasyon içeriğinde bu modülü ve ayarlarını yapmak gerekiyor.

Kuruluma devam etmeden önce ;

```
a. Bu install şekli internete açılacak şekilde kullanılmamalıdır.
b. Brute force gibi tekniklere açıktır.
c. Ldap bind için kullanılan hesabın şifresi cleartext saklanır dolayısı ile bu servisin çalıştığı makina harden edilmelidir
d. örnekte protokol olarak ldap kullandım işiniz bitince ldaps ve port değişikliğini yapmayı kesinlikle unutmayınız.
```

Yukarıdaki uyarıları anladığınıza emin olduktan sonra sırasıyla ;

1. Nginx compile edebilmek için gerekli paketleri kuruyoruz
   bu detayda, repositoryleri enable ettikten sonra compile edebilmek için gerekli kütüphaneleri yüklüyoruz

   ```
   $ sudo -i #<-- sudo yapbilen bir kullanıcının şifresini girelim
   $ sudo add-apt-repository universe
   $ sudo add-apt-repository multiverse
   $ sudo apt update
   $ sudo apt upgrade
   $ sudo apt install ldap-utils zlib1g build-essential gcc make libldap2-dev libssl-dev libpcre3-dev
   ```

   kurulumlar bittikten sonra reboot ediyoruz
2. Git kullanarak modülü indiriyoruz

   ```
   $ cd ~/Downloads
   $ git clone https://github.com/kvspb/nginx-auth-ldap
   $ cd nginx-auth-ldap
   $ git pull
   ```

3. Nginx source code indiriyor ve deflate ediyoruz
   Ben bu denemem de nginx-1.21.6 versiyonunu kullandım

```
$ cd ~/
$ wget -c http://nginx.org/download/nginx-1.21.6.tar.gz
$ tar zxvf nginx-1.21.6.tar.gz
$ cd nginx-1.21.6
```

4. ./configure, make, sudo make instal Bu aşamada nginx i compile edeceğiz bunun için aşağıdaki komutu kullanacağız

```
./configure --user=nginx --group=nginx --prefix=/etc/nginx --sbin-path=/usr/sbin/nginx --conf-path=/etc/nginx/nginx.conf --pid-path=/var/run/nginx.pid --lock-path=/var/run/nginx.lock --error-log-path=/var/log/nginx/error.log --http-log-path=/var/log/nginx/access.log --with-http_gzip_static_module --with-http_stub_status_module --with-http_ssl_module --with-pcre --with-file-aio --with-http_realip_module --add-module=/root/nginx-auth-ldap/ --with-ipv6 --with-debug
```

   Bütün compile işi sorunsuz tamamlandıktan sonra ;

```
$ make
$ sudo make install
```

5. systemd değişiklikleri
   nginx compile edilerek kurulduğunda, systemd service unit dosyası olmadan kuruluyor bunu maalesef elimizle yapmak zorunda kalıyoruz. Bunun için yukarıdaki compile metoduna göre aşağıdaki unit içeriğini kopyalayabilirsiniz

```
[Unit]
Description=A high performance web server and a reverse proxy server
Documentation=man:nginx(8)
After=network.target nss-lookup.target

[Service]
Type=forking
PIDFile=/var/run/nginx.pid
ExecStartPre=/usr/sbin/nginx -t -q -g 'daemon on; master_process on;'
ExecStart=/usr/sbin/nginx -g 'daemon on; master_process on;'
ExecReload=/usr/sbin/nginx -g 'daemon on; master_process on;' -s reload
ExecStop=-/sbin/start-stop-daemon --quiet --stop --retry QUIT/5 --pidfile /run/nginx.pid
TimeoutStopSec=5
KillMode=mixed

[Install]
WantedBy=multi-user.target
```

yukarıdaki içeriği /lib/systemd/system/nginx dosyasına yapıştırıp kaydedip çıkın

```
$sudo nano /lib/systemd/system/nginx
```

6. Ldap-auth modülünün çalışabilmesi için gerekli nginx.conf değişiklikleri
   Bu adımda ldap-auth modülünü nginx'e eklemek için

```
/etc/nginx/nginx.conf
```

Dosyasını nano ile açıp aşağıdaki içeriği http protokolüne ekliyoruz

```
http {
    include /etc/nginx/conf.d/*.conf;
    auth_ldap_cache_enabled on;
    auth_ldap_cache_expiration_time 1000;
    auth_ldap_cache_size 1000;
    ldap_server adds {
    url "ldap://172.21.24.34:3268/DC=xxx,DC=work?sAMAccountName?sub?(ObjectClass=user)";
        binddn "XXX\administrator";
        bind_passwd "12qwasZX";
        require_valid_user;
        ssl_check_cert off;
```

Bu işlem tamamlandıktan sonra default konfig olan ve yine nginx.conf dosyası içindeki server { başlığını comment out ediyoruz

```
#    server {
#        listen       80;
#        server_name  localhost;

        #charset koi8-r;

        #access_log  logs/host.access.log  main;

#       location / {
#            root   html;
#            index  index.html index.htm;
#        }

        #error_page  404              /404.html;

        # redirect server error pages to the static page /50x.html
        #
#        error_page   500 502 503 504  /50x.html;
#        location = /50x.html {
#            root   html;
#        }

        # proxy the PHP scripts to Apache listening on 127.0.0.1:80
        #
        #location ~ \.php$ {
        #    proxy_pass   http://127.0.0.1;
        #}

        # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
        #
        #location ~ \.php$ {
        #    root           html;
        #    fastcgi_pass   127.0.0.1:9000;
        #    fastcgi_index  index.php;
```

6. Reverse proxy tanımı /etc/nginx/conf.d içerisine

```
$sudo nano /etc/nginx/conf.d/kibana.conf
```

aşağıdaki detayları kendinize göre değiştirerek yapıştırabilirisiniz

```
upstream kibana {
    server kibana_ip_adresi:port_numarası;
    }
server {
    listen 80;
    server_name default_server;
    location / {
        auth_ldap "Enter AD credentials like 'mesut.bayrak@xxx.work'";
            auth_ldap_servers adds;
```

```
        proxy_set_header Host $host;
        proxy_pass http://kibana;
        }
    }
```

7. Testler
   Yukarıdaki tanımlar bittikten sonra

   ```
   $sudo nginx -t
   ```

   hata görmezseniz,

   ```
   $sudo nginx restart
   ```

   yazarak ldap authentication modüllü bu çözümü kullanabilirsiniz.

Bu konuda mesut[at]netdev.com.tr den, destek alabilirsiniz

Revision #2
Created 9 November 2022 12:07:21 by Mesut Bayrak
Updated 11 November 2022 08:29:51 by Mesut Bayrak