SQUID - Installation und Konfiguration

Im ersten Schritt installieren wir den Proxy-Server **Squid**.

Installation

Wie soll es anders sein, funktioniert die Installation der benötigten Programme im gewohnten Rahmen via **yum**, welches wir als User **root** ausführen.

```
# su -
```

```
# yum install squid
```

Was uns das Paket **squid** alles mitbringt offenbart eine Blick, nach erfolgter Installation des Paketes, in das **RPM**.

```
# rpm -iql squid
Name        : squid                         Relocations: (not relocatable)
Version     : 2.6.STABLE21                       Vendor: CentOS
Release     : 3.el5                          Build Date: Mi 21 Jan 2009
05:15:13 CET
Install Date: Do 10 Dez 2009 14:00:30 CET      Build Host:
builder16.centos.org
Group       : System Environment/Daemons    Source RPM:
squid-2.6.STABLE21-3.el5.src.rpm
Size        : 3690075                          License: GPL
Signature   : DSA/SHA1, Mo 09 Mär 2009 02:49:14 CET, Key ID a8a447dce8562897
Summary     : Der Proxy-Cache-Server Squid.
Description :
Squid is a high-performance proxy caching server for Web clients,
supporting FTP, gopher, and HTTP data objects. Unlike traditional
caching software, Squid handles all requests in a single,
non-blocking, I/O-driven process. Squid keeps meta data and especially
hot objects cached in RAM, caches DNS lookups, supports non-blocking
DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System
lookup program (dnsserver), a program for retrieving FTP data
(ftpget), and some management and client tools.
/etc/httpd/conf.d/squid.conf
/etc/logrotate.d/squid
/etc/pam.d/squid
```

```
/etc/rc.d/init.d/squid
/etc/squid
/etc/squid/cachemgr.conf
/etc/squid/errors
/etc/squid/icons
/etc/squid/mib.txt
/etc/squid/mime.conf
/etc/squid/mime.conf.default
/etc/squid/msntauth.conf
/etc/squid/msntauth.conf.default
/etc/squid/squid.conf
/etc/squid/squid.conf.default
/etc/sysconfig/squid
/usr/lib/squid
/usr/lib/squid/cachemgr.cgi
/usr/lib/squid/digest_pw_auth
/usr/lib/squid/diskd-daemon
/usr/lib/squid/fakeauth_auth
/usr/lib/squid/getpwname_auth
/usr/lib/squid/ip_user_check
/usr/lib/squid/msnt_auth
/usr/lib/squid/ncsa_auth
/usr/lib/squid/ntlm_auth
/usr/lib/squid/pam_auth
/usr/lib/squid/sasl_auth
/usr/lib/squid/smb_auth
/usr/lib/squid/smb_auth.pl
/usr/lib/squid/smb_auth.sh
/usr/lib/squid/squid_ldap_auth
/usr/lib/squid/squid_ldap_group
/usr/lib/squid/squid_unix_group
/usr/lib/squid/unlinkd
/usr/lib/squid/wbinfo_group.pl
/usr/lib/squid/yp_auth
/usr/sbin/cossdump
/usr/sbin/squid
/usr/sbin/squidclient
/usr/share/doc/squid-2.6.STABLE21
...

...
/var/log/squid
/var/spool/squid
```

Konfiguration des Proxy's

Die Konfiguration des Proxyservers erfolgt über die zentrale Konfigurationsdatei ***/etc/squid/squid.conf***. Mit dem Editor unserer Wahl z.B. **vim** bearbeiten wir nun die Konfigurationsdatei des squid's:

```
 # vim /etc/squid/squid.conf
```

Authentifizierung mit NCSA-AUTH

Damit sich jeder Nutzer an jedem Rechner setzen und Verbindungen zum Internet aufbauen kann, aktivieren wir die ***NCSA-style Username und Passwort Authentifizierung***. Somit haben wir später die Möglichkeit zur Überprüfung der besuchten Seiten.

Zu erst überprüfen wir, ob der entsprechende Authentification-Helper vorhanden und installiert ist.

```
 # rpm -ql squid | grep ncsa_auth
```

```
/usr/lib/squid/ncsa_auth
/usr/share/man/man8/ncsa_auth.8.gz
```

Dann legen wir uns ein entsprechendes Passwortfile (mit dem User bofh) an:

```
htpasswd -c /etc/squid/passwd bofh
```

Die Option **-c** verwenden wir, da das File noch nicht existiert und wir ein entsprechendes anlegen wollen. Alle weiteren User werden dann mit

```
htpasswd /etc/squid/passwd django
```

angelegt.

Zu guter Letzt konfigurieren wir nun **nsca_auth** für die Squid Autentifizierung in der Konfigurationsdatei **/etc/squid/squid.conf** des Proxyservers. Aktivierung der NSCA_Authentifizierung:

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
auth_param basic children 4
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

Aktivierung einer ACL für den Zugriff:

```
acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users
```

Somit beschränkt sich das gesamte Konfigurationsfile auf folgende Einträge:

```
# egrep -v '(^#|^$)' /etc/squid/squid.conf
http_port 3128
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
acl apache rep_header Server ^Apache
```

```
broken_vary_encoding allow apache
logformat common %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st %Ss:%Sh
access_log /var/log/squid/access.log squid
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
auth_param basic children 4
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
http_reply_access allow all
icp_access allow all
coredump_dir /var/spool/squid
```

Authentifizierung mit LDAP-AUTH

Weitaus komfortabler, da der zentrale LDAP-Verzeichnisdienst genutzt wird, läuft die Authentifizierung gegen unseren LDAP-Server (open_ldap_server), den wir hoffentlich schon eingerichtet haben. Auch hier haben wir später die Möglichkeit zur Überprüfung der besuchten Seiten.

Zu erst überprüfen wir, ob der entsprechende Authentification-Helper vorhanden und funktionsfähig ist.

```
 # /usr/lib/squid/squid_ldap_auth -b "dc=domain,dc=de" -f "uid=%s" -h
ldap.domain.de -D "cn=System_User,dc=domain,dc=de" -W
```

```
"/etc/squid/ldap_system_user_passwd"
```

Anschließende geben wir folgende Werte ein: **User-ID [Leerzeichen] Passwort** also z.B.

```
500 klausi-is-a-geek
```

In der Logdatei unseres LDAP-server wird dann der Erfolg entsprechend quittiert:

```
Feb  4 19:43:05 nss slapd[21642]: conn=58 fd=12 ACCEPT from
IP=192.168.100.1:45681 (IP=0.0.0.0:389)
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=0 BIND
dn="cn=System_User,dc=domain,dc=de" method=128
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=0 BIND
dn="cn=System_user,dc=domain,dc=de" mech=SIMPLE ssf=0
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=0 RESULT tag=97 err=0 text=
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=1 SRCH base="dc=domain,dc=de"
scope=2 deref=0 filter="(uid=500)"
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=1 SRCH attr=1.1
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=1 SEARCH RESULT tag=101 err=0
nentries=0 text=
Feb  4 19:43:05 nss slapd[21642]: conn=58 op=2 UNBIND
Feb  4 19:43:05 nss slapd[21642]: conn=58 fd=12 closed
```

Mit **err=0** wird uns der erfolgreiche Test quittiert.

Im Gegensatz zur vorhergenannten Variante authentifizierung_mit_ncsa-auth brauchen wir keine eigene Nutzer-/Passwortdatei anlegen, da ja die zentrale LDAP-Datenbank genutzt wird.

Anschließend konfigurieren wir nun **ldap_auth** für die Squid Autentifizierung in der Konfigurationsdatei **/etc/squid/squid.conf** des Proxyservers. Aktivierung der LDAP_Authentifizierung:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b "dc=domain,dc=de"
-f "uid=%s" -h ldap.domain.de -D "cn=System_User,dc=domain,dc=de" -W
/etc/squid/ldap_system_user_passwd
auth_param basic children 5
auth_param basic realm Squid-Proxyserver im SOHO-LAN bei nausch.org
auth_param basic credentialsttl 15 minutes
auth_param basic casesensitive off
```

Aktivierung einer ACL für den Zugriff:

```
acl ldapauth proxy_auth REQUIRED
http_access allow ldapauth
```

Somit beschränkt sich das gesamte Konfigurationsfile auf folgende Einträge:

```
# egrep -v '(^#|^$)' /etc/squid/squid.conf
http_port 3128
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
```

```
cache deny QUERY
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
logformat common %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st %Ss:%Sh
access_log /var/log/squid/access.log squid
auth_param basic program /usr/lib/squid/squid_ldap_auth -b "dc=domain,dc=de"
-f "uid=%s" -h ldap.domain.de -D "cn=System_User,dc=domain,dc=de" -W
/etc/squid/ldap_system_user_passwd
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl ldapauth proxy_auth REQUIRED
http_access allow ldapauth
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
http_reply_access allow all
icp_access allow all
coredump_dir /var/spool/squid
```

Nach erfolgtem Start des squid (**service squid start**) sehen wir bei den Benutzeranmeldungen im squid.log (**/var/log/squid.log**) die erfolgreichen Authentifizierungen:

```
Aug  6 22:44:45 nss slapd[5821]: conn=38 fd=21 ACCEPT from
IP=192.168.1.1:52671 (IP=0.0.0.0:389)
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=0 SRCH base="dc=domain,dc=de"
scope=2 deref=0 filter="(uid=django)"
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=0 SRCH attr=1.1
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=0 SEARCH RESULT tag=101 err=0
nentries=1 text=
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=1 BIND
dn="uid=django,ou=People,dc=domain,dc=de" method=128
```

```
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=1 BIND
dn="uid=django,ou=People,dc=domain,dc=de" mech=SIMPLE ssf=0
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=1 RESULT tag=97 err=0 text=
Aug  6 22:44:45 nss slapd[5821]: conn=38 op=2 UNBIND
Aug  6 22:44:45 nss slapd[5821]: conn=38 fd=21 closed
Aug  6 22:44:45 nss slapd[5821]: connection_read(21): no connection!
```

Starten des Squid-Proxys

Nun starten wir das erste mal unsere neuen Dienste und zwar zuerst den **squid**:

```
# service squid start
init_cache_dir /var/spool/squid... squid starten: .        [  OK  ]
```

automatisches Starten der Dienste beim Systemstart

Damit der squid-Daemon automatisch bei jedem Systemstart startet, kann die Einrichtung der Start-Scripte über folgende Befehle erreicht werden:

```
# chkconfig squid on
```

Die Überprüfungung ob der Dienst (Daemon) squid auch wirklich bei jedem Systemstart automatisch mit gestartet werden, kann durch folgenden Befehle erreicht werden:

```
# chkconfig --list | grep squid
squid           0:Aus   1:Aus   2:Ein   3:Ein   4:Ein   5:Ein   6:Aus
```

Wichtig sind jeweils die Schalter **on** bzw. **Ein** bei den Runleveln - **2 3 4 5**.

Content- und Virenfilter mit Dansguardian und ClamAV

Die Konfiguration des Content- und Virenfilters mit Hilfe von Dansguardian und ClamAV ist auf den folgenden Seiten beschrieben.

From:
https://dokuwiki.nausch.org/ - **Linux - Wissensdatenbank**

Permanent link:
https://dokuwiki.nausch.org/doku.php/centos:squid

Last update: **20.04.2018 09:08.**