

# Autenticazione Apache/Unix via Kerberos SPNEGO verso Windows AD 2003

Matteo Redaelli  
01/09/2005

## Obiettivo

Autenticazione integrata (senza inserire la password) degli utenti intranet in un'applicazione web Unix/Apache. Nel caso che l'utente non fosse autenticato sul pc con l'utenza di rete, comparirà una form in cui sarà comunque possibile inserire l'utente/password di rete.

## Introduzione

Come si può leggere sul sito

<http://www.microsoft.com/windows2000/techinfo/howitworks/security/kerberos.asp>

Microsoft dalla versione di Windows 2000 utilizza di default Kerberos per l'autenticazione degli utenti in luogo di protocolli proprietari. Con la modalità SPNEGO è possibile avere l'autenticazione integrata analogamente al vecchio e insicuro NTLM tipico dei sistemi NT4-

## Scenario

Dominio win2003: REDAELLI

DomainController: dc.REDAELLI.ORG

Server unix Apache: Linux Debian (SARGE) di nome sarge con Apache/2.0.54 (Debian GNU/Linux)

mod\_auth\_kerb/5.0-rc6 mod\_python/3.1.3 Python/2.3.5 PHP/4.3.10-15 mod\_perl/1.999.21

Perl/v5.8.4 Server at sarge Port 80

## Riferimenti

- 1) <http://modauthkerb.sourceforge.net/>
- 2) <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/http-sso-1.asp>

Altre info su

- 3) <http://www.grolmsnet.de/kerbtut/>
- 4) <http://support.microsoft.com/default.aspx?scid=kb;en-us;555092>
- 5) [http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Intran\\_4.msp](http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/P3Intran_4.msp)
- 6) <http://www.onlamp.com/lpt/a/4171>

## Installazione

Installare il sw necessario sul server sarge

```
apt-get install krb5-config
Default realm: REDAELLI.ORG
Enter the hostnames of Kerberos servers: dc.REDAELLI.ORG
```

```
apt-get install krb5-clients krb5-config krb5-user
apt-get install ntpdate
apt-get install libapache2-mod-auth-kerb
```

# Configurazione

## *Sul Domain Controller*

Creato sull'AD l'utente di servizio (non interattivo) "myuser" con password "XXX". Non è necessario creare invece un'entry per l'hostname "sarge".

```
ktpass -princ HTTP/sarge@REDAELLI.ORG -pass XXX -mapuser myuser -out c:\sarge.keytab
```

## *Sul server unix/apache*

### Configurazione ntpdate

Occorre sincronizzare la data tra il server kerberos e il client unix. Su debian occorre modificare il file /etc/default/ntpdate o inserire gli hostname dei server ntp durante l'installazione del pacchetto ntpdate

```
# servers to check. (Separate multiple servers with spaces.)
NTPSERVERS="ntp.redaelli.org"
#
# additional options for ntpdate
#NTPOPTIONS="-v"
NTPOPTIONS="-u"
```

### Configurazione Kerberos

File /etc/krb5.conf, in nero le modifiche apportate da me:

```
[libdefaults]
    default_realm = REDAELLI.ORG
# The following krb5.conf variables are only for MIT Kerberos.
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
dns_lookup_realm = true
dns_lookup_kdc = true
# The following encryption type specification will be used by MIT Kerberos
# if uncommented. In general, the defaults in the MIT Kerberos code
# are correct and overriding these specifications only serves to disable
# new encryption types as they are added, creating interoperability problems.
#    default_tgs_etypes = aes256-cts arcfour-hmac-md5 des3-hmac-sha1 des-cbc-crc des-
cbc-md5
#    default_tkt_etypes = aes256-cts arcfour-hmac-md5 des3-hmac-sha1 des-cbc-crc des-
cbc-md5
#permitted_etypes = aes256-cts arcfour-hmac-md5 des3-hmac-sha1 des-cbc-crc des-cbc-md5
# The following libdefaults parameters are only for Heimdal Kerberos.
v4_instance_resolve = false
v4_name_convert = {
    host = {
        rcmd = host
        ftp = ftp
    }
    plain = {
        something = something-else
    }
}

[realms]
REDAELLI.ORG = {
    kdc = dc.REDAELLI.ORG:88
    admin_server = dc.REDAELLI.ORG:464
}
```

```

ATHENA.MIT.EDU = {
    kdc = kerberos.mit.edu:88
    kdc = kerberos-1.mit.edu:88
    kdc = kerberos-2.mit.edu:88
    kdc = kerberos-3.mit.edu:88
    admin_server = kerberos.mit.edu
    default_domain = mit.edu
}
MEDIA-LAB.MIT.EDU = {
    kdc = kerberos.media.mit.edu
    admin_server = kerberos.media.mit.edu
}
ZONE.MIT.EDU = {
    kdc = casio.mit.edu
    kdc = seiko.mit.edu
    admin_server = casio.mit.edu
}
MOOF.MIT.EDU = {
    kdc = three-headed-dogcow.mit.edu:88
    kdc = three-headed-dogcow-1.mit.edu:88
    admin_server = three-headed-dogcow.mit.edu
}
CYGNUS.COM = {
    kdc = KERBEROS.CYGNUS.COM
    kdc = KERBEROS-1.CYGNUS.COM
    admin_server = KERBEROS.CYGNUS.COM
}
GREY17.ORG = {
    kdc = kerberos.grey17.org
    admin_server = kerberos.grey17.org
}
IHTFP.ORG = {
    kdc = kerberos.ihtfp.org
    admin_server = kerberos.ihtfp.org
}
GNU.ORG = {
    kdc = kerberos.gnu.org
    kdc = kerberos-2.gnu.org
    kdc = kerberos-3.gnu.org
    admin_server = kerberos.gnu.org
}
1TS.ORG = {
    kdc = kerberos.1ts.org
    admin_server = kerberos.1ts.org
}
GRATUITOUS.ORG = {
    kdc = kerberos.gratuitous.org
    admin_server = kerberos.gratuitous.org
}
DOOMCOM.ORG = {
    kdc = kerberos.doomcom.org
    admin_server = kerberos.doomcom.org
}

ANDREW.CMU.EDU = {
    kdc = vice28.fs.andrew.cmu.edu
    kdc = vice2.fs.andrew.cmu.edu
    kdc = vice11.fs.andrew.cmu.edu
    kdc = vice12.fs.andrew.cmu.edu
    admin_server = vice28.fs.andrew.cmu.edu
    default_domain = andrew.cmu.edu
}
CS.CMU.EDU = {
    kdc = kerberos.cs.cmu.edu
    kdc = kerberos-2.srv.cs.cmu.edu
    admin_server = kerberos.cs.cmu.edu
}
DEMENTIA.ORG = {
    kdc = kerberos.dementia.org
    kdc = kerberos2.dementia.org
    admin_server = kerberos.dementia.org
}

[domain_realm]
.mit.edu = ATHENA.MIT.EDU

```

```

mit.edu = ATHENA.MIT.EDU
.media.mit.edu = MEDIA-LAB.MIT.EDU
media.mit.edu = MEDIA-LAB.MIT.EDU
.who1.edu = ATHENA.MIT.EDU
who1.edu = ATHENA.MIT.EDU
.stanford.edu = stanford.edu
.REDAELLI.ORG = .REDAELLI.ORG
REDAELLI.ORG = REDAELLI.ORG

[login]
krb4_convert = true
krb4_get_tickets = true

```

A questo punto si può testare l'autenticazione Kerberos con il comando

```
kinit myuser@REDAELLI.ORG
```

## Configurazione Apache

Eeguire i seguenti passi:

- Creare la (virtual) directory /var/www/kerberos/
- Verificare nel file di configurazione di apache (/etc/apache2/sites-enabled/000-default) la possibilità di usare i file .htaccess (stringa "AllowOverride All").
- Copiare il file "sarge.keytab" creato nel paragrafo precedente sotto /etc/apache2
- Creare il file /var/www/kerberos/.htaccess coem segue:

```

AuthName "Kerberos Login"
AuthType Kerberos
Krb5Keytab /etc/apache2/sarge.keytab
KrbAuthRealm REDAELLI.ORG
KrbMethodNegotiate on
KrbMethodK5Passwd on
KrbSaveCredentials off
KrbVerifyKDC off
Require valid-user

```

## Configurazione dei client

Occorre usare una versione recente di Mozilla o di Internet Explorer impostando l'autenticazione integrata come indicato nel secondo link del paragrafo "Riferimenti".

## Esempio1 (semplice test php)

A questo punto dovrebbe essere tutto ok e per fare un test si crei un file index.php come segue

```

<?php
echo "<p>Hello {$_SERVER['REMOTE_USER']}</p>";
?>

```

e si acceda col browser all'url

<http://sarge/kerberos/>

## Esempio2 (con applicazione RT)

Per info sull'installazione del prodotto si veda <http://www.bestpractical.com/rt/>

Oppure per Debian

```
apt-get install request-tracker3.4
```

File di configurazione di apache (/etc/request-tracker3.4/apache2-modperl2.conf su linux debian):

```
<Directory /usr/share/request-tracker3.4/html>
  SetHandler perl-script
  PerlHandler RT::Mason
AuthName "REDAELLI account"
AuthType Kerberos
Krb5Keytab /etc/apache2/sarge.keytab
KrbAuthRealm REDAELLI.ORG
KrbMethodNegotiate on
KrbMethodK5Passwd on
KrbSaveCredentials off
KrbVerifyKDC off
Require valid-user
</Directory>
```

File di configurazione RT\_SiteConfig.pm (sotto /etc/request-tracker3.4 su linux debian):

```
# http://wiki.bestpractical.com/index.cgi?WebExternalAuth
Set($WebExternalAuth , 1);
Set($WebExternalAuto , 1);
Set($WebFallbackToInternalAuth , true);
```

Occorrerebbe dare pero' all'utente la possibilità di collegarsi con l'utente "root" amministratore dell'applicazione. Forse il link <http://sial.org/howto/rt/> può essere utile.