Fileserver con SAMBA e Windows

Integrazione con *Microsoft Active Directory*

Emiliano Vavassori

BGlug — Bergamo Linux User Group
Circoscrizione n° 2, Largo Röntgen n° 3
24128 Bergamo

23 ottobre 2010 — LinuxDay 2010

Premessa

Tutto il materiale qui riportato è disponibile a questo indirizzo:

http://tinyurl.com/ld10-samba

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk 0:-)

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto. Ci vorrebbe una giornata intera.

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk 0:-)

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto. Ci vorrebbe una giornata intera.

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk `0:-)`

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto.
Ci vorrebbe una giornata intera.

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk 0:-)

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto.
Ci vorrebbe una giornata intera.

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk 0:-)

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto.
Ci vorrebbe una giornata intera.

Lightning Talk?

- Richiesta «passiva» sul sito del BGlug
- Limitazione nell'obiettivo
- Livello tecnico abbastanza alto
- Procedura di setup di meno di mezz'ora (compresi test)
- Poco tempo per la preparazione del talk 0:-)

Un piccolo dubbio mi assale… Esaustivo?

Non si può fare un *lightning talk* su *Active Directory* in senso stretto. Ci vorrebbe una giornata intera.

Obiettivo

Creare un *file server* integrato con una struttura *Active Directory* preesistente.

Obiettivo

Creare un *file server* integrato con una struttura *Active Directory* preesistente.

Integrato con *Active Directory*

Gli utenti saranno in grado di accedere ai documenti condivisi senza ulteriori autenticazioni da macchine di dominio con utenze di dominio.

0.0 — Struttura della rete

Domain Controller — *Windows 2003 Server*

```
10.0.0.1    testdc.domain.local
```

File Server — *Debian 5.0 «Lenny»*

```
10.0.0.100  linuxfs.domain.local
```

0.1 — Indirizzi del fileserver

Prima di partire, conviene verificare l'indirizzo di rete:

```
# ip address show eth0
```

Verificare il *Fully Qualified Domain Name* (FQDN):

Estratto: `/etc/hosts`

```
10.0.0.100 linuxfs.domain.local linuxfs \
  localhost.localdomain localhost
```

0.1 — Indirizzi del fileserver

Prima di partire, conviene verificare l'indirizzo di rete:

```
# ip address show eth0
```

Verificare il *Fully Qualified Domain Name* (FQDN):

Estratto: `/etc/hosts`

```
10.0.0.100 linuxfs.domain.local linuxfs \
  localhost.localdomain localhost
```

0.2 — Indirizzi del domain controller

Verificare DNS primario e dominio:

Estratto: `/etc/resolv.conf`

```
nameserver 10.0.0.1
search domain.local
domain domain.local
```

Verificare comunicazione e risoluzione nomi:

```
$ ping 10.0.0.1
```

```
$ ping testdc.domain.local
```

```
$ ping testdc
```

0.2 — Indirizzi del domain controller

Verificare DNS primario e dominio:

Estratto: `/etc/resolv.conf`

```
nameserver 10.0.0.1
search domain.local
domain domain.local
```

Verificare comunicazione e risoluzione nomi:

```
$ ping 10.0.0.1
```

```
$ ping testdc.domain.local
```

```
$ ping testdc
```

1 — Installazione pacchetti necessari

```
# aptitude install openntpd ntpdate krb5-user samba
winbind smbclient
```

Opzionalmente:

```
# aptitude install smbfs
```

1 — Installazione pacchetti necessari

```
# aptitude install openntpd ntpdate krb5-user samba
winbind smbclient
```

Opzionalmente:

```
# aptitude install smbfs
```

Fermiamo il servizio:

```
# /etc/init.d/openntpd stop
```

Estratto: `/etc/openntpd/ntpd.conf`

```
server testdc.domain.local
```

Impostiamo l'ora…

```
# ntpdate testdc.domain.local
```

…e riavviamo il servizio:

```
# /etc/init.d/openntpd start
```

Fermiamo il servizio:

```
# /etc/init.d/openntpd stop
```

Estratto: `/etc/openntpd/ntpd.conf`

```
server testdc.domain.local
```

Impostiamo l'ora…

```
# ntpdate testdc.domain.local
```

…e riavviamo il servizio:

```
# /etc/init.d/openntpd start
```

Fermiamo il servizio:

```
# /etc/init.d/openntpd stop
```

Estratto: `/etc/openntpd/ntpd.conf`

```
server testdc.domain.local
```

Impostiamo l'ora…

```
# ntpdate testdc.domain.local
```

…e riavviamo il servizio:

```
# /etc/init.d/openntpd start
```

Fermiamo il servizio:

```
# /etc/init.d/openntpd stop
```

Estratto: `/etc/openntpd/ntpd.conf`

```
server testdc.domain.local
```

Impostiamo l'ora…

```
# ntpdate testdc.domain.local
```

…e riavviamo il servizio:

```
# /etc/init.d/openntpd start
```

Estratto: /etc/krb5.conf

```
[libdefaults]
default_realm = DOMAIN.LOCAL
…
[realms]
DOMAIN.LOCAL = {
  kdc = testdc.domain.local
  admin_server = testdc.domain.local
}
…
[domain_realm]
.domain.local = DOMAIN.LOCAL
domain.local = DOMAIN.LOCAL
```

4.0 — Configurazione SAMBA: generale

Estratto: /etc/samba/smb.conf

```
[global]
workgroup = DOMAIN
realm = DOMAIN.LOCAL
wins server = 10.0.0.1
security = ads
password server = testdc.domain.local
obey pam restrictions = yes
unix password sync = yes
winbind separator = +
winbind use default domain = yes
```

4.0 — Configurazione SAMBA: generale

Estratto: /etc/samba/smb.conf

```
[global]
workgroup = DOMAIN
realm = DOMAIN.LOCAL
wins server = 10.0.0.1
security = ads
password server = testdc.domain.local
obey pam restrictions = yes
unix password sync = yes
winbind separator = +
winbind use default domain = yes
```

Estratto: `/etc/samba/smb.conf`

```
[shared]
comment = …
path = /var/local/shared
valid users = %U
browseable = yes
writable = yes
guest ok = no
read only = no
create mask = 0664
directory mask = 0775
```

Infine testiamo il file:

```
# testparm
```

4.1 — Configurazione SAMBA: condivisioni

Estratto: /etc/samba/smb.conf

```
[shared]
comment = …
path = /var/local/shared
valid users = %U
browseable = yes
writable = yes
guest ok = no
read only = no
create mask = 0664
directory mask = 0775
```

Infine testiamo il file:

```
# testparm
```

4.1 — Configurazione SAMBA: condivisioni

Estratto: /etc/samba/smb.conf

```
[shared]
comment = …
path = /var/local/shared
valid users = %U
browseable = yes
writable = yes
guest ok = no
read only = no
create mask = 0664
directory mask = 0775
```

Infine testiamo il file:

```
# testparm
```

Estratto: `/etc/samba/smb.conf`

```
[shared]
comment = …
path = /var/local/shared
valid users = %U
browseable = yes
writable = yes
guest ok = no
read only = no
create mask = 0664
directory mask = 0775
```

Infine testiamo il file:

```
# testparm
```

Riavviamo i servizi:

```
# /etc/init.d/samba restart
```

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

Verifichiamo che Kerberos funzioni:

```
# kinit -a administrator
```

Messa in dominio:

```
# net ads join -U Administrator
```

Verifichiamo che si riesca ad accedere alle informazioni di dominio:

```
# wbinfo -u
```

Riavviamo i servizi:

```
# /etc/init.d/samba restart
```

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

Verifichiamo che Kerberos funzioni:

```
# kinit -a administrator
```

Messa in dominio:

```
# net ads join -U Administrator
```

Verifichiamo che si riesca ad accedere alle informazioni di dominio:

```
# wbinfo -u
```

5 — Messa in dominio

Riavviamo i servizi:

```
# /etc/init.d/samba restart
```

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

Verifichiamo che Kerberos funzioni:

```
# kinit -a administrator
```

Messa in dominio:

```
# net ads join -U Administrator
```

Verifichiamo che si riesca ad accedere alle informazioni di dominio:

```
# wbinfo -u
```

Riavviamo i servizi:

```
# /etc/init.d/samba restart
```

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

Verifichiamo che Kerberos funzioni:

```
# kinit -a administrator
```

Messa in dominio:

```
# net ads join -U Administrator
```

Verifichiamo che si riesca ad accedere alle informazioni di dominio:

```
# wbinfo -u
```

Difetti d'implementazione

- Non utilizza Heimdal Kerberos (se necessario LDAP, da preferire)
- Incompatibilità con sistemi *Microsoft* più moderni: Windows 7, Windows 2008 Server.
- L'implementazione attuale non permette il login sul file server di utenze di dominio (necessario configurare PAM)

Difetti d'implementazione

- Non utilizza Heimdal Kerberos (se necessario LDAP, da preferire)
- Incompatibilità con sistemi *Microsoft* più moderni: Windows 7, Windows 2008 Server.

- L'implementazione attuale non permette il login sul file server di utenze di dominio (necessario configurare PAM)

Difetti d'implementazione

- Non utilizza Heimdal Kerberos (se necessario LDAP, da preferire)
- Incompatibilità con sistemi *Microsoft* più moderni: Windows 7, Windows 2008 Server.
  Soluzione — Samba 3.4 da *Lenny Backports*
- L'implementazione attuale non permette il login sul file server di utenze di dominio (necessario configurare PAM)

Difetti d'implementazione

- Non utilizza Heimdal Kerberos (se necessario LDAP, da preferire)
- Incompatibilità con sistemi *Microsoft* più moderni: Windows 7, Windows 2008 Server.
  Soluzione — Samba 3.4 da *Lenny Backports*
- L'implementazione attuale non permette il login sul file server di utenze di dominio (necessario configurare PAM)

Un *cadeau*

Possiamo «importare» magicamente gruppi e utenze all'interno della macchina Linux aggiungendo:

Estratto: `/etc/nsswitch.conf`

```
passwd: compat winbind
passwd_compat: winbind
group: compat winbind
group_compat: winbind
shadow: compat winbind
```

Un *cadeau*

Possiamo «importare» magicamente gruppi e utenze all'interno della macchina Linux aggiungendo:

Estratto: `/etc/nsswitch.conf`

```
passwd: compat winbind
passwd_compat: winbind
group: compat winbind
group_compat: winbind
shadow: compat winbind
```

Sarà ora possibile attribuire i permessi a intere cartelle come:

```
# chown -R root:'domain users' /var/local/shared
```

Cosa possiamo fare ora?

A partire da quanto messo a punto ora possiamo implementare:

- un proxy autenticato (Squid + `auth_ntlm`)
- un *domain controller* Linux-based (LDAP)

Cosa possiamo fare ora?

A partire da quanto messo a punto ora possiamo implementare:

- un proxy autenticato (Squid + `auth_ntlm`)
- un *domain controller* Linux-based (LDAP)

Sitografia

- The SAMBA Team
  The Official Samba 3.5.x HOWTO and Reference Guide
  http://tinyurl.com/samba-howto
- Blog di Jake Surly
  Post: *Join Debian Lenny to Active Directory using Samba*
  http://tinyurl.com/samba-adjoin
- Guide Debianizzati
  Samba e OpenLDAP: creare un controller di dominio con Debian Lenny
  http://tinyurl.com/deb-dc
- Guide Debianizzati
  Samba, OpenLDAP, Kerberos: creare un controller di dominio sicuro con Debian Lenny
  http://tinyurl.com/deb-secure-dc