Mezzora d'amicizia

Una settimana di lavoro con SSH

SSH use cases

http://www.linuxvar.it

02/04/2008

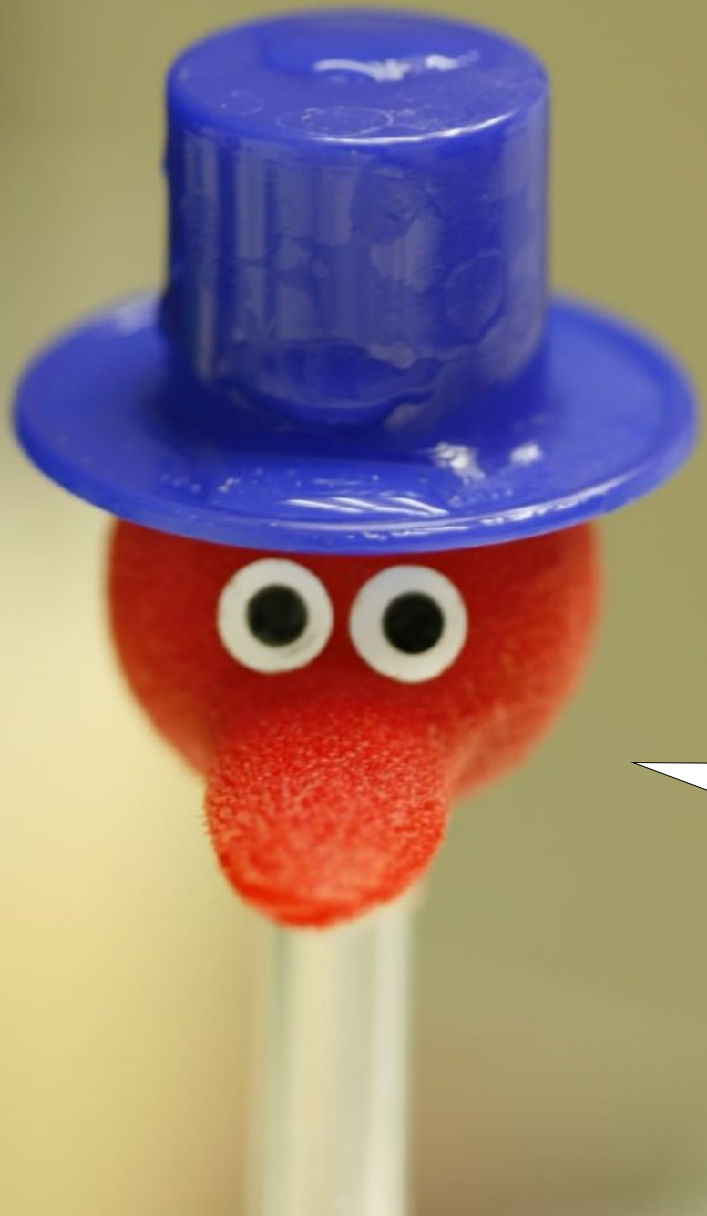
AndreA Ciancone

mail:
aciancone at **inscatolati** dot **net**

PICCHIO L'APPRENDISTA

Oggi e` il mio primo giorno di lavoro.

LUNEDÌ: AUTOMATIZZARE



OGNI 15 MINUTI...

AUTENTICAZIONE AL SERVER

AGGIORNAMENTO DATI

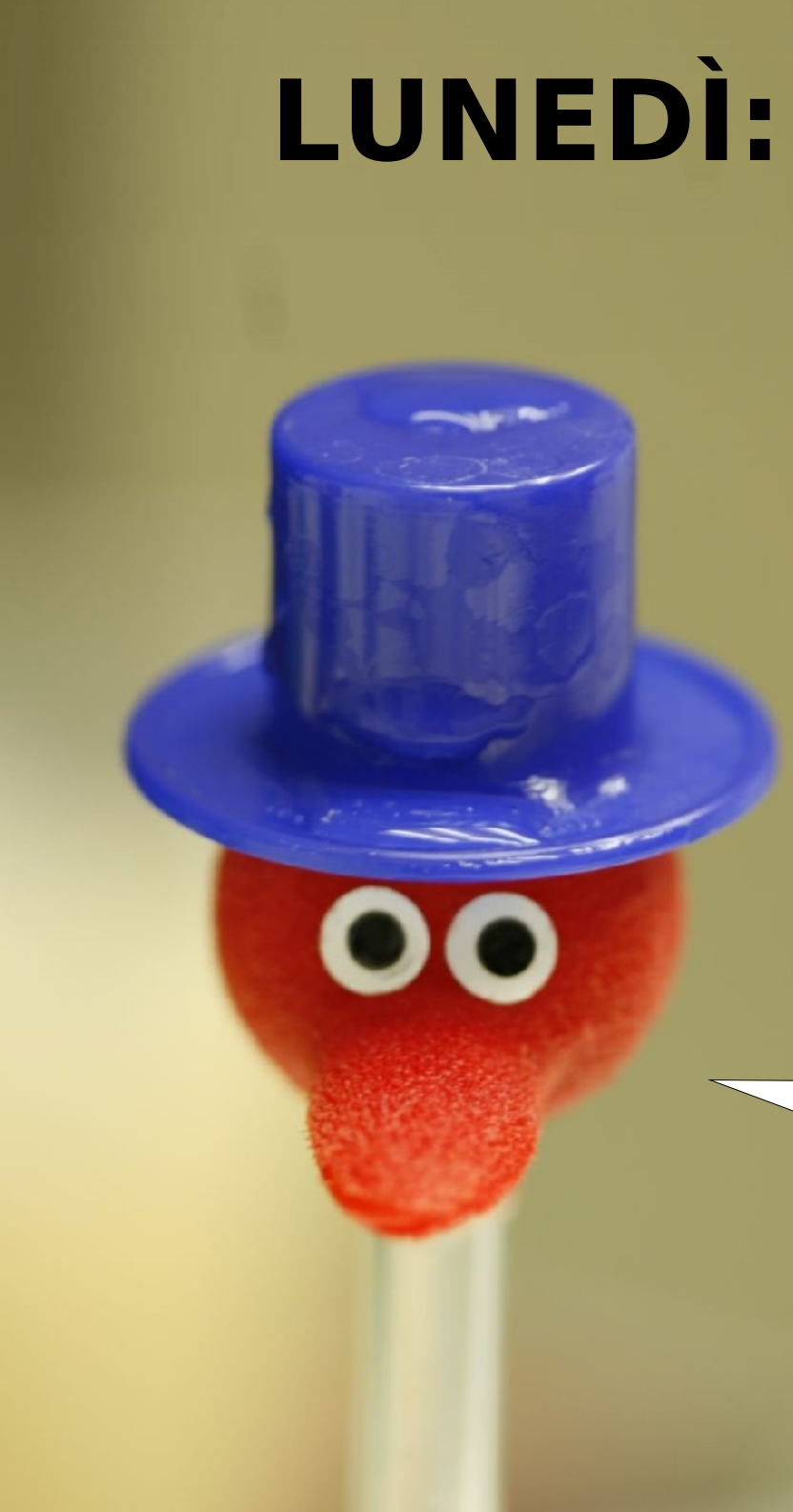
ANNOTARE I DATI SUL PC

Come posso automatizzare il processo?

COPIA DEL FILE

```
$ man 1 scp
scp copia file tra pc in
rete. Utilizza ssh(1) per
trasferire i dati e per
autenticarsi, fornendo la
stessa sicurezza di ssh(1).

$ scp picchio@server:~/file \
  ~/copia_file_locale
Password:
file        100% 1.6KB/s 00:00
```

LUNEDÌ: CHECKLIST 1/4



OGNI 15 MINUTI...

AUTENTICAZIONE AL SERVER

AGGIORNAMENTO DATI

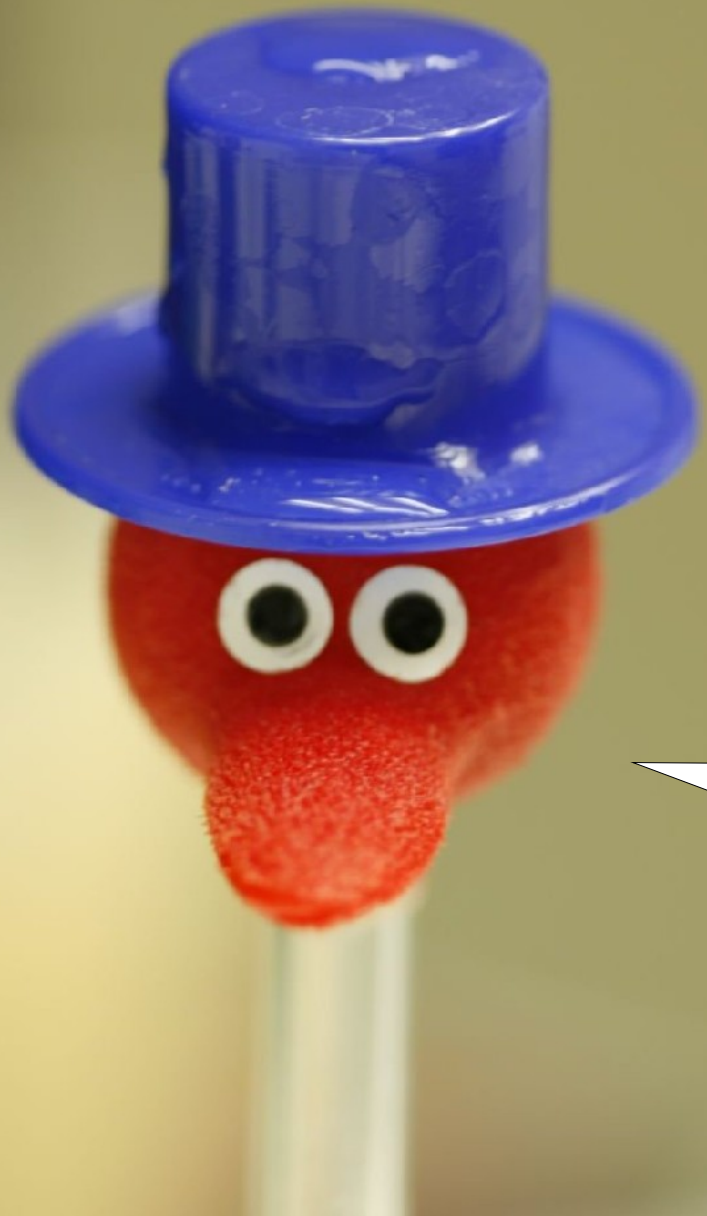
ANNOTARE I DATI SUL PC

Posso automatizzare il processo?

ESECUZIONE COMANDI

```
$ man 1 ssh
ssh [opzioni] host [comando]
se e` specificato il comando,
invece di ottenere una shell
viene eseguito il comando

$ ssh picchio@server ~/update
Password:
```

LUNEDÌ: CHECKLIST 2/4



OGNI 15 MINUTI...

AUTENTICAZIONE AL SERVER

- **AGGIORNAMENTO DATI**
- **ANNOTARE I DATI SUL PC**

Posso automatizzare il processo?

AUTENTICAZIONE

```
$ man 1 ssh
[...]
I metodi disponibili per
autenticarsi sono:
- password
- challenge-response
- public key
- host based
- GSSAPI based
```

GENERAZIONE CHIAVI

```
$ ssh-keygen -t rsa -b 4092
Generazione chiavi rsa.
Inserire password (nulla in
caso non la si voglia):

La chiave privata e`salvata in
~picchio/.ssh/id_rsa
La chiave pubblica e` salvata
in ~picchio/.ssh/id_rsa.pub.
Il fingerprint e`:
f1:da:6a:34:b3:43:d8:85:62:3b:
5c:71:49:8a:84:5f picchio@local
```

LUNGHEZZA CHIAVI

http://csrc.nist.gov/publications/PubsSPs.html

Recommendation for Key Management
SP 800-57 Review 2 (March 2007)

1024 bit sono considerati sicuri fino al 2010

2048 bit sono considerati sicuri fino al 2030

forse prima del 2030 ...

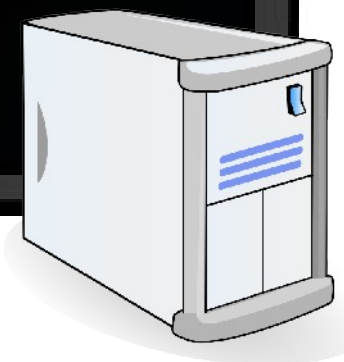
Algoritmo di Shor (quantico)

fattorizza interi N con tempo O((log N)^3) spazio O(log N)

SETUP CHIAVI

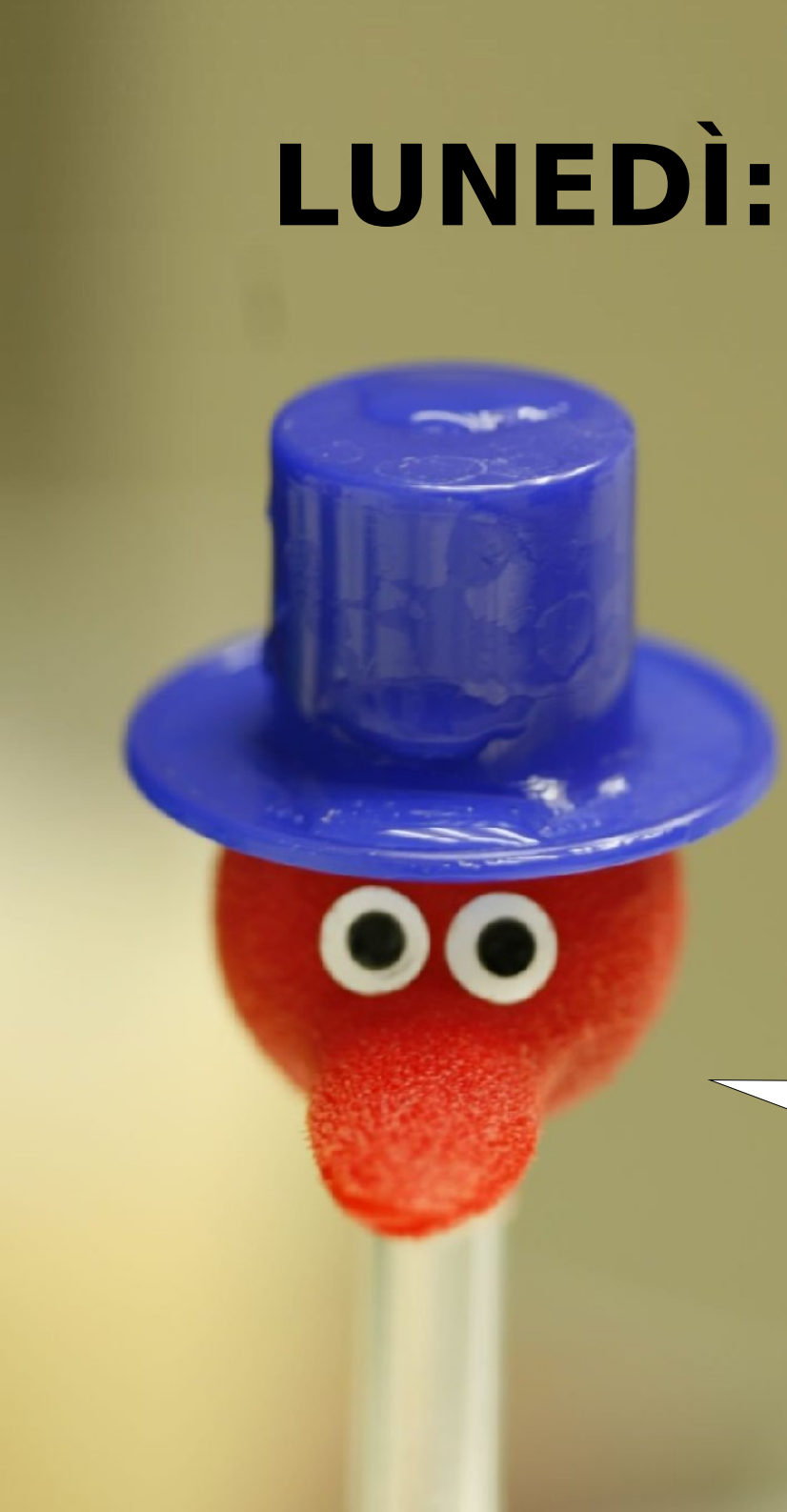
```
$ ls ~/.ssh/
id_rsa
id_rsa.pub
known_hosts

$ scp -u picchio \
~/.ssh/id_rsa.pub \
server:~/.ssh/key.pub
```

```
$ cd ~/.ssh/

$ cat picchio.pub \
  >> authorized_keys

$ ls ./
authorized_keys
known_hosts
```



SERVER

LUNEDÌ: CHECKLIST 3/4



OGNI 15 MINUTI...

- **AUTENTICAZIONE AL SERVER**
- **AGGIORNAMENTO DATI**
- **ANNOTARE I DATI SUL PC**

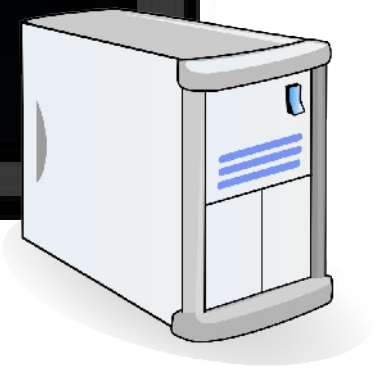
Posso automatizzare il processo?

SCRIPT AUTOMATICO

```
while true; do
  # set timeout to 15min
  timeout 900 bash <<< '
    echo "`date` Run script..."

    ssh picchio@server ~/update
    scp picchio@server:~/file \
        ~/file_`date +%s_%N`

    echo "done."
    # wait timeout syncronization
    sleep 900
  '
done 2>&1 | tee work.log
```

LIMITARE L'USO DI CHIAVI

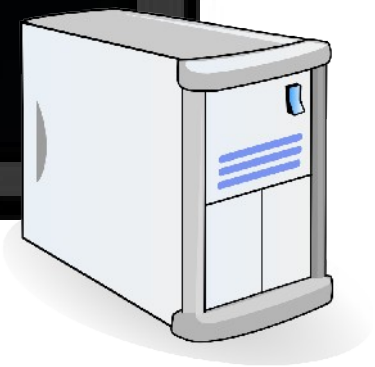
```
$ man sshd
Il formato di authorized_keys
prevede per ogni chiave i seguenti
campi: opzioni, tipo_chiave,
chiave base64-encoded, commento.
Le opzioni non sono obbligatorie.

Le opzioni (se presenti) sono
separate da virgola:
command="command"
enviromental="NAME=value"
from="pattern-list"
[...]
```



SERVER

L'OPZIONE COMMAND

```
$ vim ~/.ssh/authorized_keys

command="~/update &> /dev/null;
cat ~/file" ssh-rsa AAAAB3NzaC1yc
2EAAAABIwAAAQEAvl7c13YvGkOLMKfr14
GI07twaQOkFpUOu29KIOqs+yUsinZU9CY
[...]
jwjnQRSiA/w== picchio@local
```



SERVER

SCRIPT AUTOMATICO

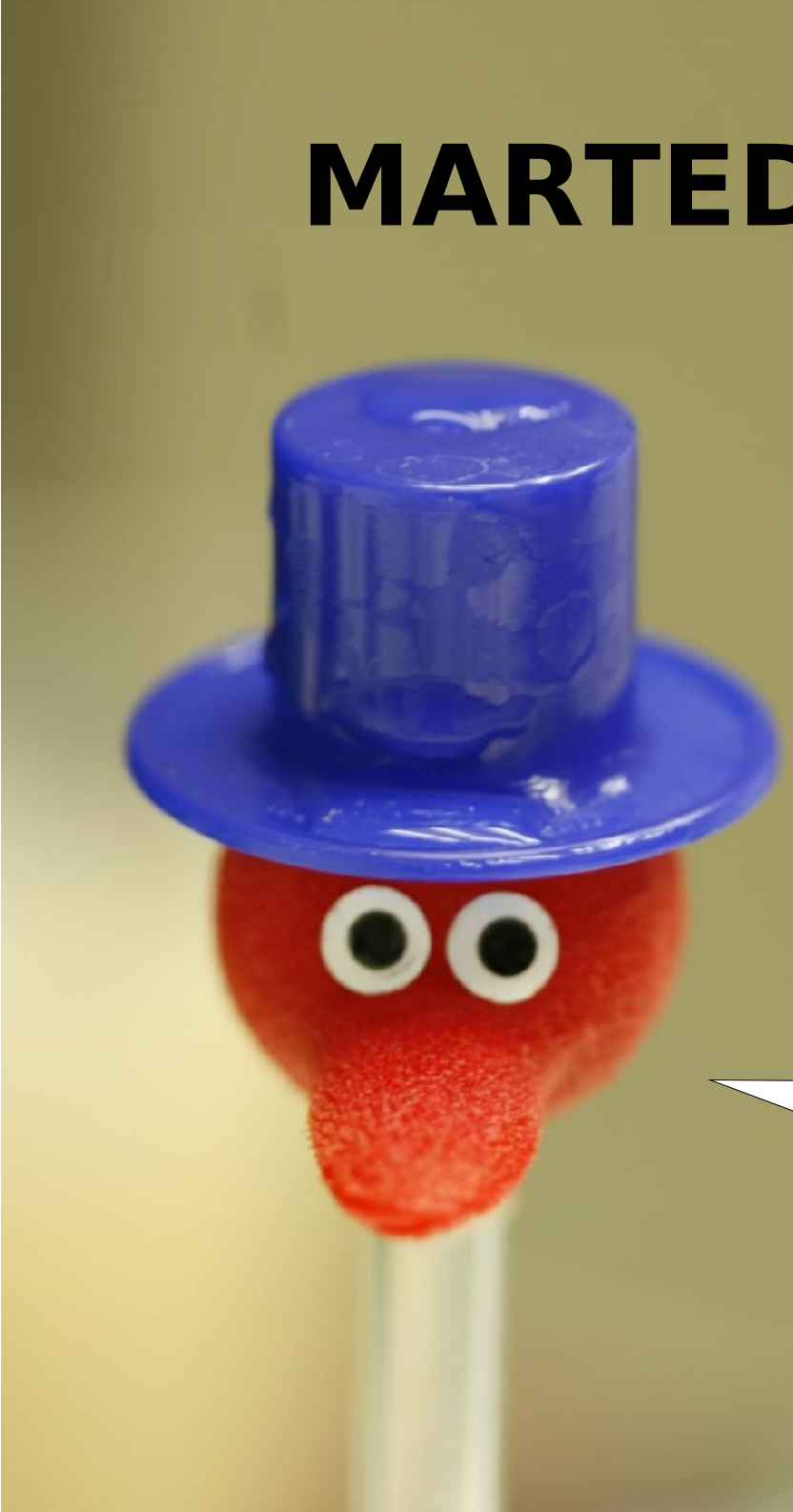
```
while true; do
  # set timeout to 15min
  timeout 900 bash <<< '
    echo "`date` Run script..."

    ssh picchio@server -i my_work \
        > ~/file_`date +%s_%N`

    echo "done."
    # wait timeout syncronization
    sleep 900
  '
done 2>&1 | tee work.log
```

AUTOMATIZZATO!

- OGNI 15 MINUTI...
- AUTENTICAZIONE AL SERVER
- AGGIORNAMENTO DATI
- ANNOTARE I DATI SUL PC

Posso automatizzare il processo?
SI

MARTEDÌ: STATISTICHE



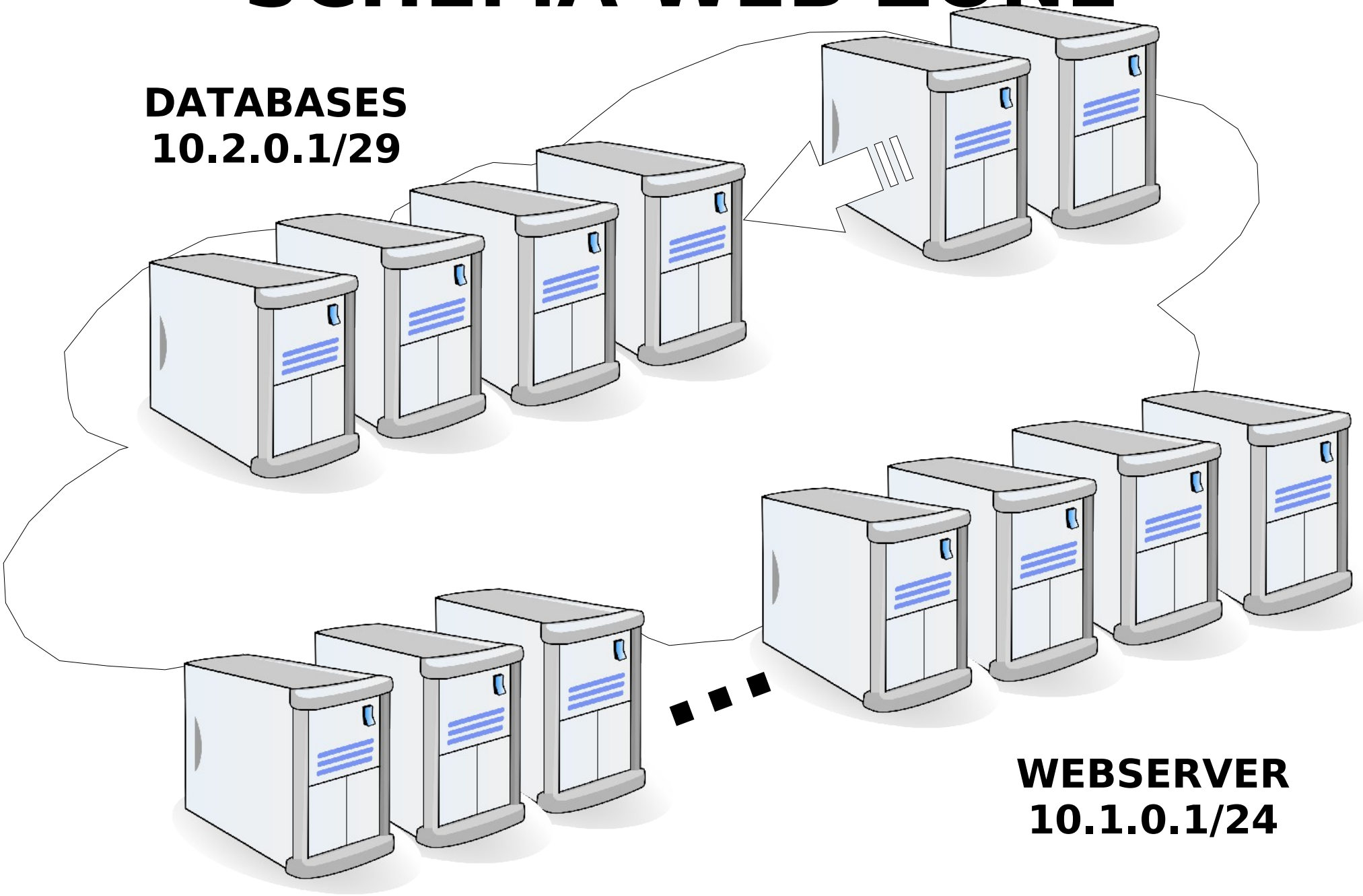
AUTENTICAZIONE AI SERVER

MULTIPLEXING

OTTENERE I LOG DEI SERVER

Posso multiplexare i comandi velocemente?

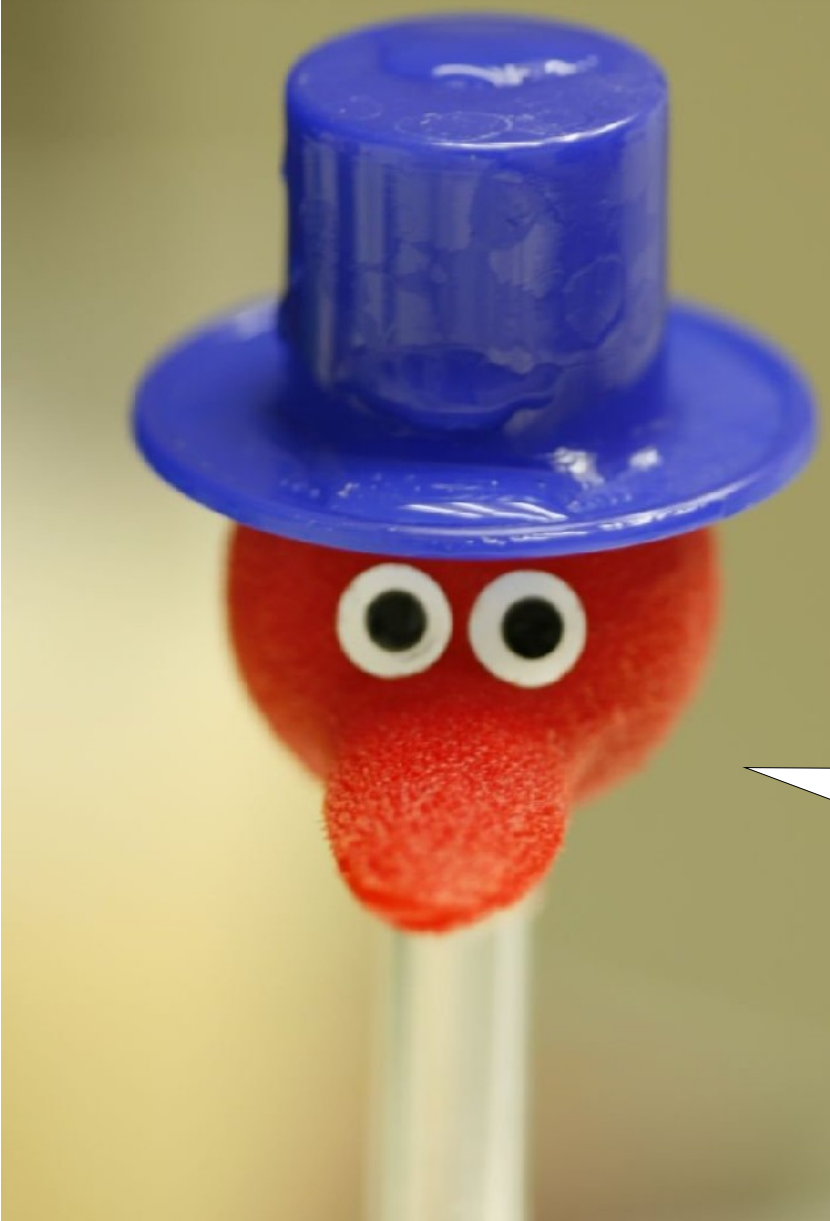
SCHEMA WEB ZONE



MULTIPLEXER

```
#!/bin/bash

list=`seq 1 30`

for num in $list; do

  echo "### `date` work on $num..."
  ssh root@10.1.0.$num "$*"
  echo "### done."

done
```

STATISTICHE!



AUTENTICAZIONE AI SERVER

MULTIPLEXING

OTTENERE I LOG DEI SERVER

Posso multiplexare i comandi velocemente?

SSH-AGENT

```
# man 1 ssh-agent
agent per l'autenticazione
[...]

mantiene caricate le chiavi
private, usate nella fase di
autenticazione con “public key”
[...]

ssh-agent e automaticamente
rilevato da ssh tramite variabili
d'ambiente e automaticamente usato
per autenticarsi su altre macchine
```

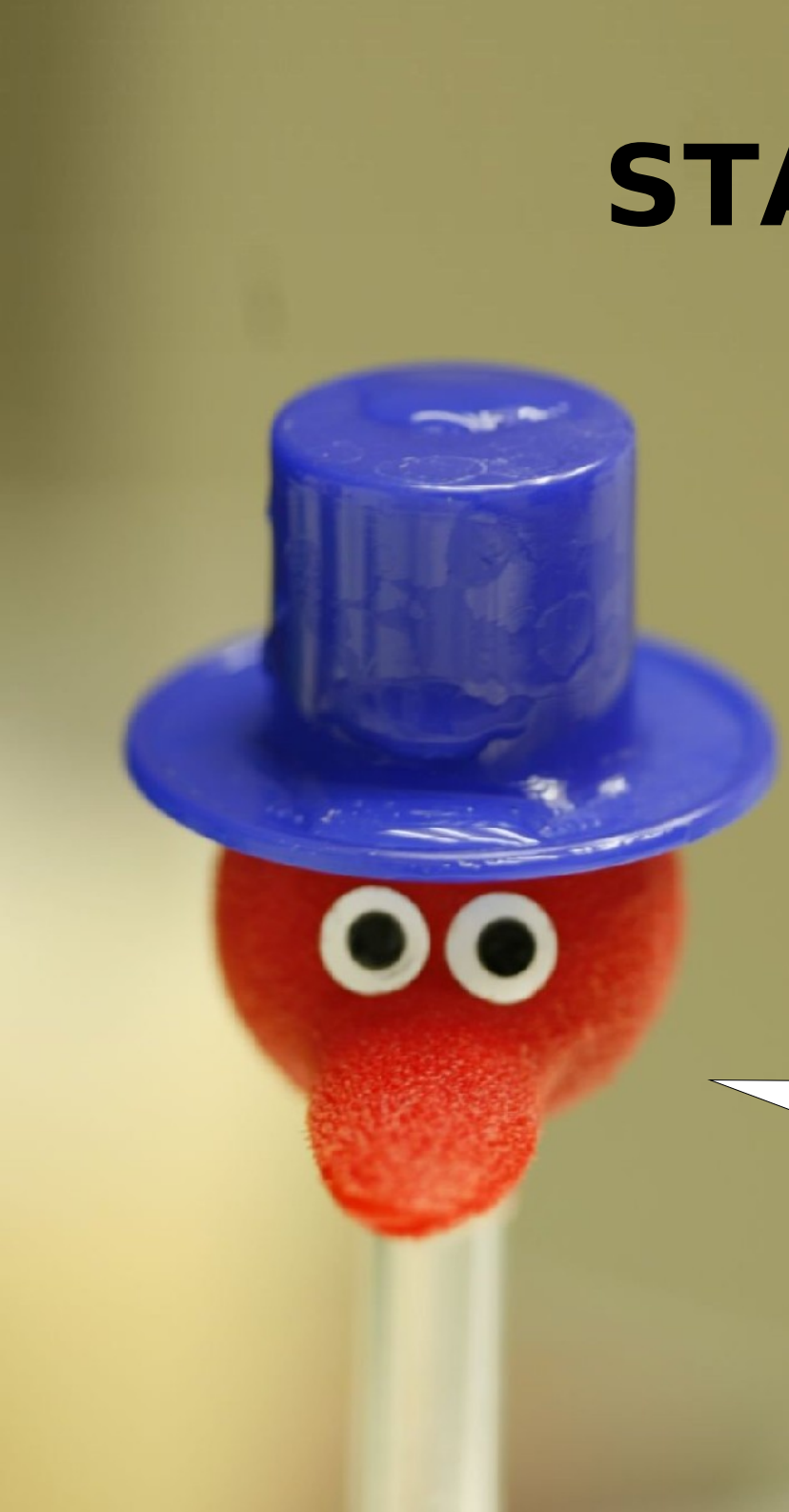
SSH-ADD

```
# man 1 ssh-add
aggiunge chiavi private all'agent
di autenticazione

Eseguito sensa argomenti aggiunge
i files ~/.ssh/id_rsa,
~/.ssh/id_dsa e ~/.ssh/identity.
[...]

OPZIONI
-d    rimuove tutte le chiavi dal
      agent
-l    mostra i fingerprint delle
      presenti nell'agent
[...]
```

PREPARE ENVIROMENT

```
# eval `ssh-agent`

Agent pid 10689

# ssh-add
Enter passphrase for
 /home/picchio/.ssh/id_dsa:

Identity added:
 /home/picchio/.ssh/id_dsa

# ssh-add -l
4096 01:23:45:67:89:.....:ca:cc:a0
/home/picchio/.ssh/id_dsa (DSA)
```

STATISTICHE!



- AUTENTICAZIONE AI SERVER
- MULTIPLEXING
- OTTENERE I LOG DEI SERVER

Posso multiplexare i comandi velocemente?

MULTIPLEXER IN USO

```
$ multiplexer.sh cat \
  /var/log/databases_access.log

#### Wed Apr  2 20:15:59 CEST 2008
     work on 1...
[...]
### done.
#### Wed Apr  2 20:15:59 CEST 2008
     work on 2...
[...]
### done.
[...]
#### Wed Apr  2 22:16:56 CEST 2008
     work on 30...
[...]
### done.
```

STATISTICHE!

- AUTENTICAZIONE AI SERVER
- MULTIPLEXING
- OTTENERE I LOG DEI SERVER

Posso multiplexare i comandi velocemente?
SI

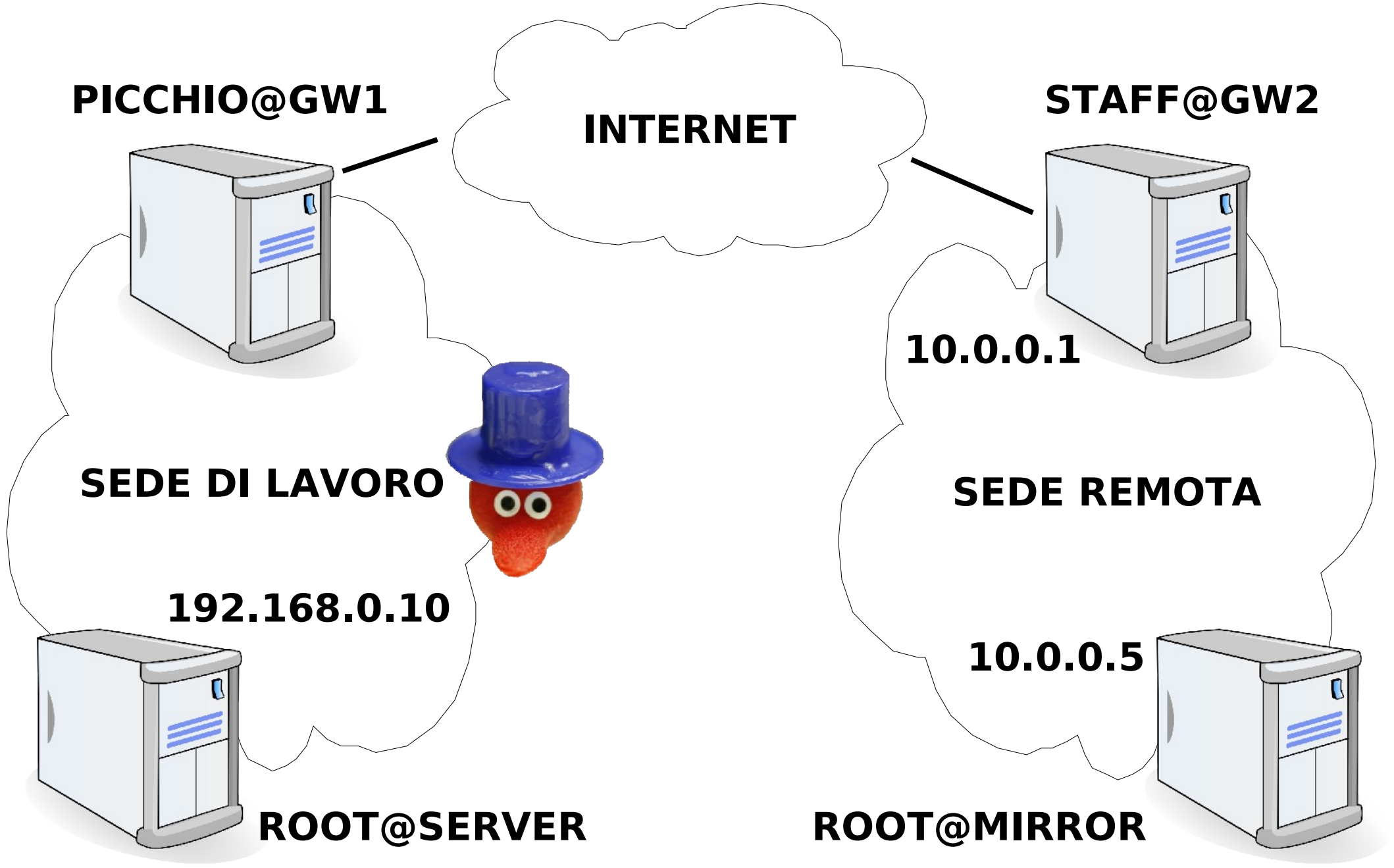
MERCOLEDÌ: BACKUP

COPIA DIRETTA TRA SISTEMI

LIMITARE L'USO DI BANDA

Posso migliorare il processo e l'uso delle risorse?

RETE AZIENDALE

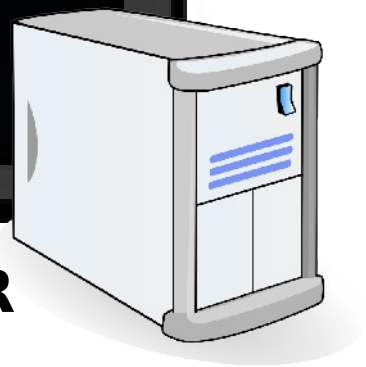


PROXY COMMAND

```
$ man 5 ssh_config

ProxyCommand specifica il
comando da usare per
connettesi al server. Il
comando deve leggere da stdin
e scrivere su stdout.
[...]
Esempio:
 ProxyCommand /usr/bin/nc -X \
 -connect 10.0.1.10:8080 %h %p
```

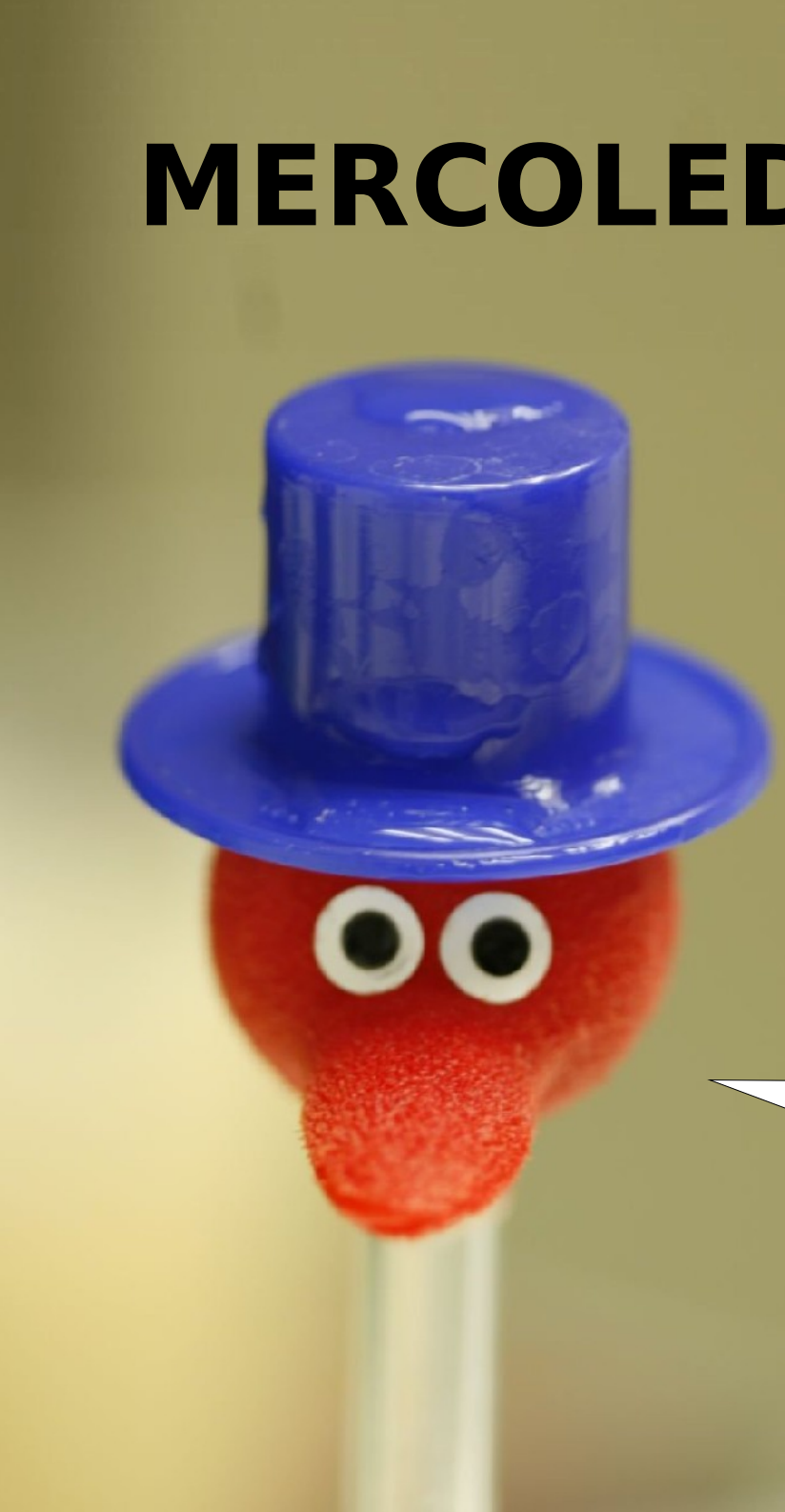
CONNESSIONE CON PROXY

```
# ssh -o ProxyCommand='ssh \
  staff@GW2 nc %h %p' \
  root@10.0.0.5
Password:
Password:

# tar -cjpsoh /opt/ | ssh -o \
  ProxyCommand='ssh staff@GW2 \
  nc %h %p' root@10.0.0.5 \
  'cat > /archive/`date +%s_%N`
Password:
Password:
```



ROOT@SERVER

MERCOLEDÌ: CHECKLIST 1/2



- **COPIA DIRETTA TRA SISTEMI**
- **LIMITARE L'USO DI BANDA**

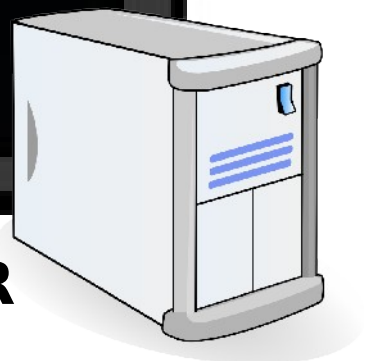
Posso migliorare il processo e l'uso delle risorse? SI

RSYNC

```
man 1 rsync
rsync e` un programma in grado di
velocizzare il trasferimento di
file quando i file di destinazione
sono solo da aggiornare.
[...]

Opzioni:
 -a                 archive mode
 -e                 specifica la shell
                    remota da usare
 --bwlimit=KBPS     limite di banda
                    usata. Espresso in
                    KBytes per secondo
```

CONNESSIONE CON RSYNC

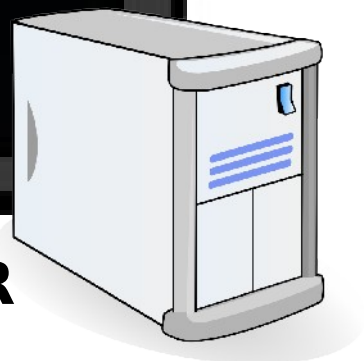
```
# ssh -o ProxyCommand='ssh \
  staff@GW2 nc %h %p' \
  root@10.0.0.5
Password:
Password:

# rsync --bwlimit=100 -a -e "ssh \
  -o ProxyCommand='ssh staff@GW2 \
  nc %h %p'" /opt/ \
  root@10.0.0.5:/opt/backup
Password:
Password:
```



ROOT@SERVER

FORWARD AGENT

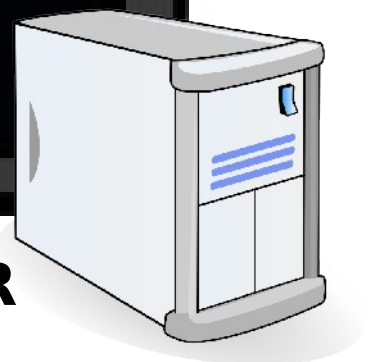
```
# man 1 ssh
Opzioni
-A Abilita il forwarding della
   connessione con l'agent ssh.
   Un utente privilegiato sul
   server remoto potrebbe usarlo
   per autenticarsi altrove ma non
   puo` ottenere la chiave.

# rsync --bwlimit=100 -a -e "ssh \
  - A -o ProxyCommand='ssh -A \
  staff@GW2 nc %h %p'" /opt/ \
  root@10.0.0.5:/opt/backup
```



ROOT@SERVER

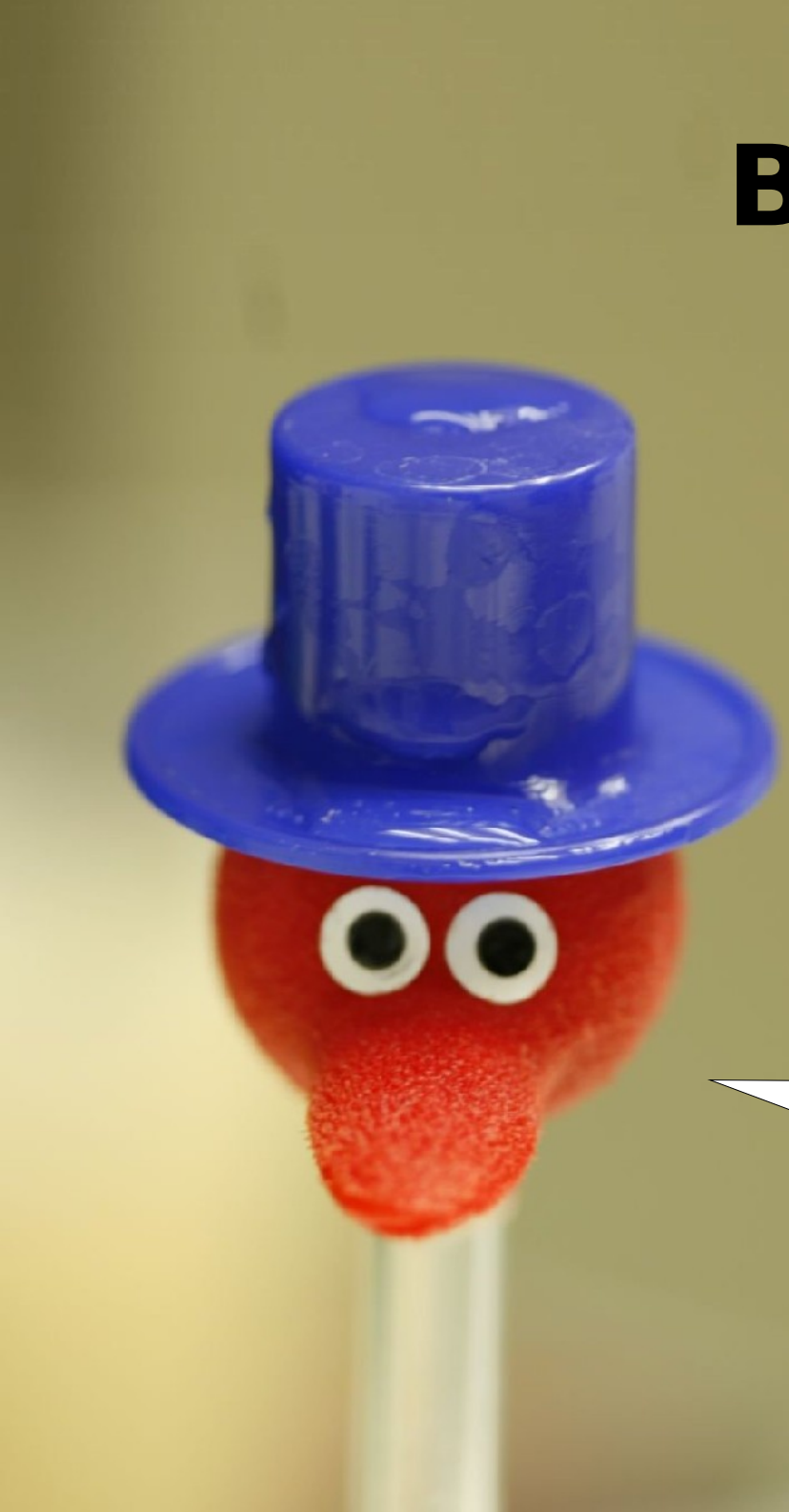
RIDUZIONE OVERHEAD DI SSH

```
# rsync --bwlimit=100 -a -e 'ssh \
  -A staff@GW2 -- ssh -A ' /opt/
  root@10.0.0.5:/opt/backup
```



ROOT@SERVER

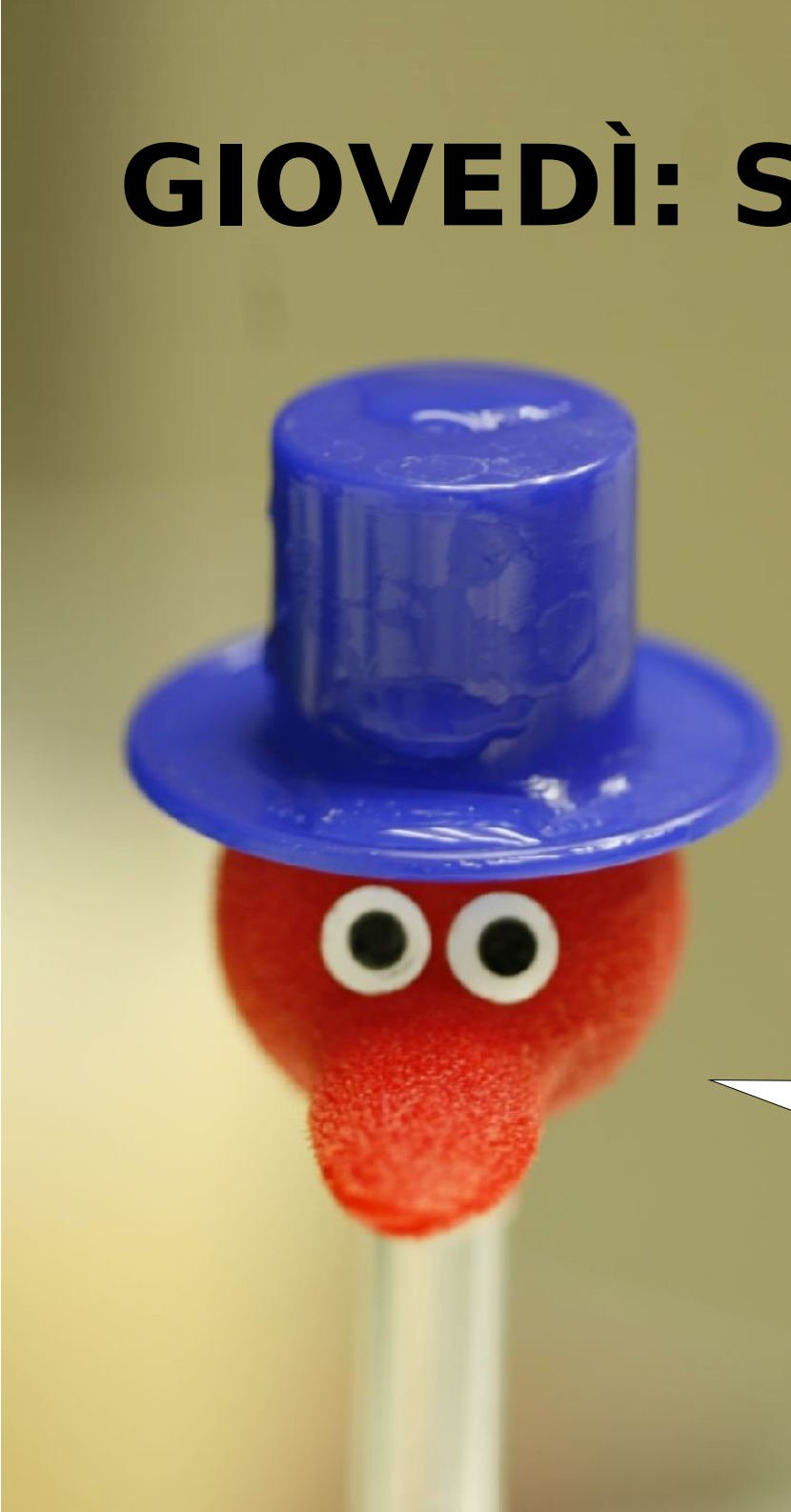
BACKUP!



- COPIA DIRETTA TRA SISTEMI
- LIMITARE L'USO DI BANDA

Posso migliorare il processo e l'uso delle risorse? SI

GIOVEDÌ: SERVIZIO REMOTO

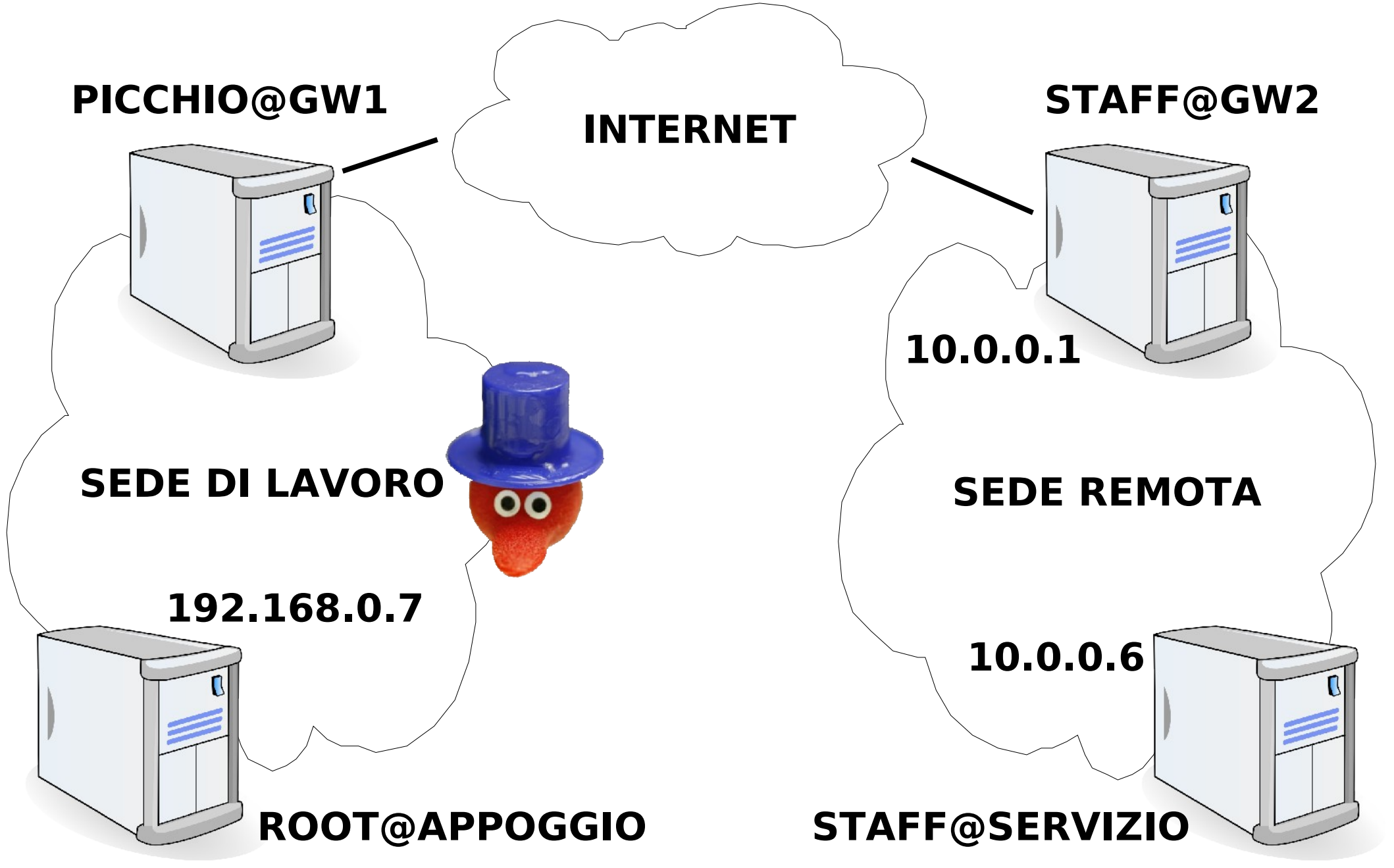


ESPORTAZIONE SERVIZIO

CONSOLIDAMENTO

Posso esportare un servizio dalla rete remota alla rete di lavoro?

RETE AZIENDALE

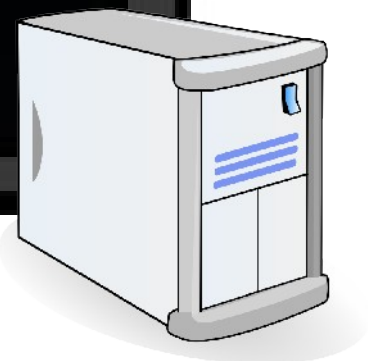


PORT FORWARDING

```
# man 1 ssh
Opzioni
 -L [bind_addr:]port:host:hostport
 ssh si mette in ascolto sulla
 porta port e` quando riceve una
 connessione la trasmette, tramite
 il canale ssh con il server,
 all'indirizzo host sulla porta
 hostport.
 Puo` essere indicato su quale
 inidirizzo ssh deve mettersi in
 ascolto (bind_addr), altrimenti
 ssh accetta connessioni solo dalla
 rete locale, localhost
```

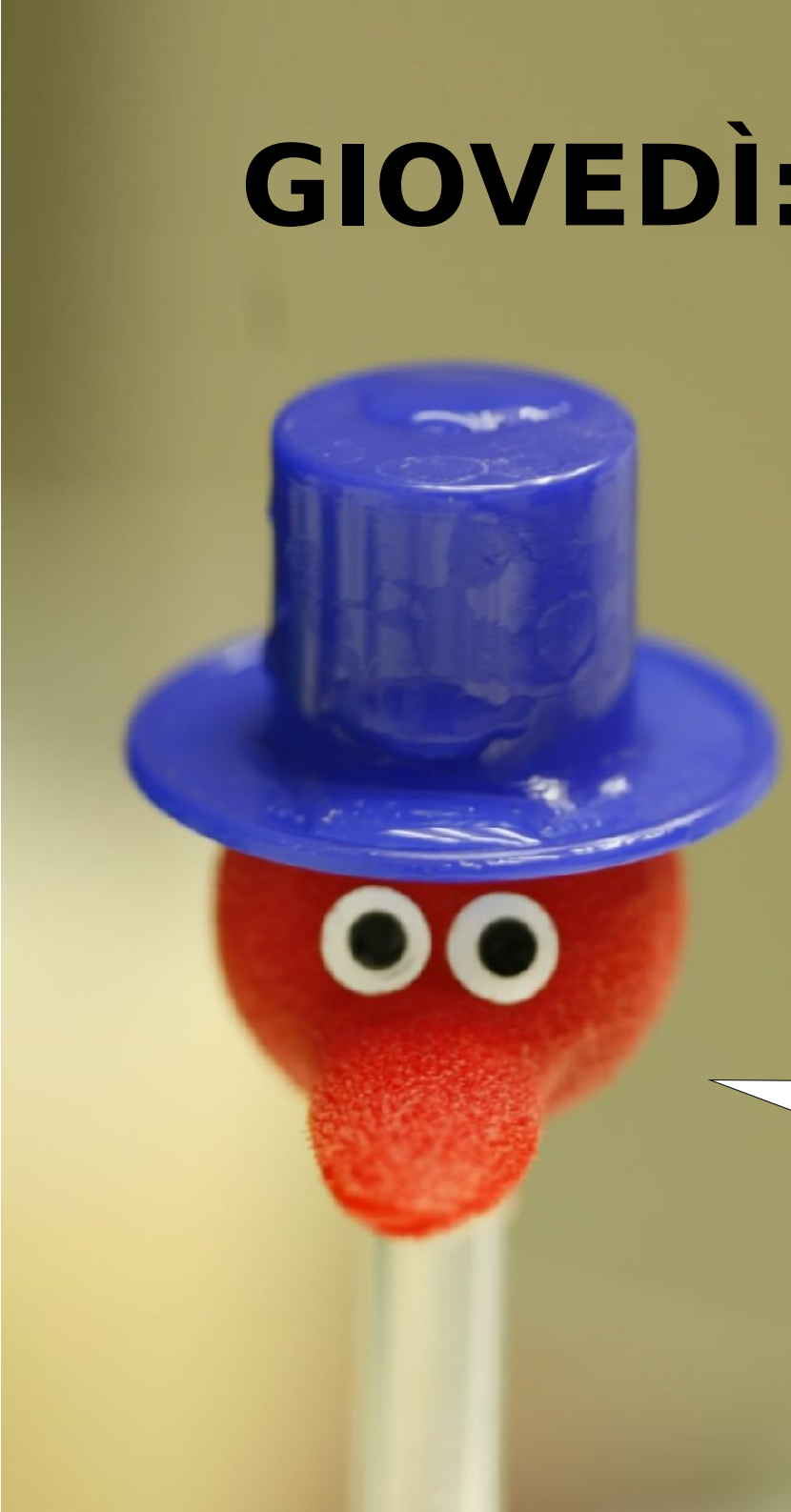
LOCAL FORWARDING

```
# ssh staff@GW2 \
  -L 192.168.0.7:80:SERVIZIO:80 \
  -o ExitOnForwardFailure=yes

# ~^Z [suspend ssh]
[1]+  Stopped       ssh ...

# netstat -polenta
Proto Local Addr      Progr State
tcp   192.168.0.7:80 ssh   LISTEN
[...]
```



ROOT@GW2

GIOVEDÌ: CHECKLIST 1/2

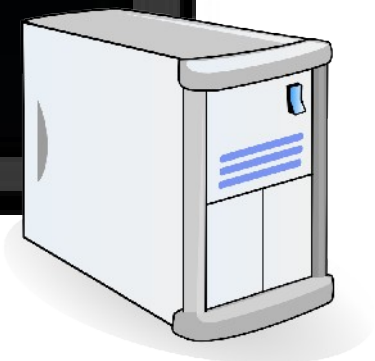


- **ESPORTAZIONE SERVIZIO**
- **CONSOLIDAMENTO**

Posso esportare un servizio dalla rete remota alla rete di lavoro?

USO CONFIGURAZIONI

```
# vim /root/.ssh_config
  Host servizio_fw
   LocalForward \
        192.168.0.7:80:SERVIZIO:80
   Hostname GW2
   User staff
   ExitOnForwardFailure=yes

# ssh servizio_fw
  Password:
```



ROOT@SERVIZIO

SERVIZIO REMOTIZZATO!

- ESPORTAZIONE SERVIZIO
- CONSOLIDAMENTO

Posso esportare un servizio dalla rete remota alla rete di lavoro?
SI

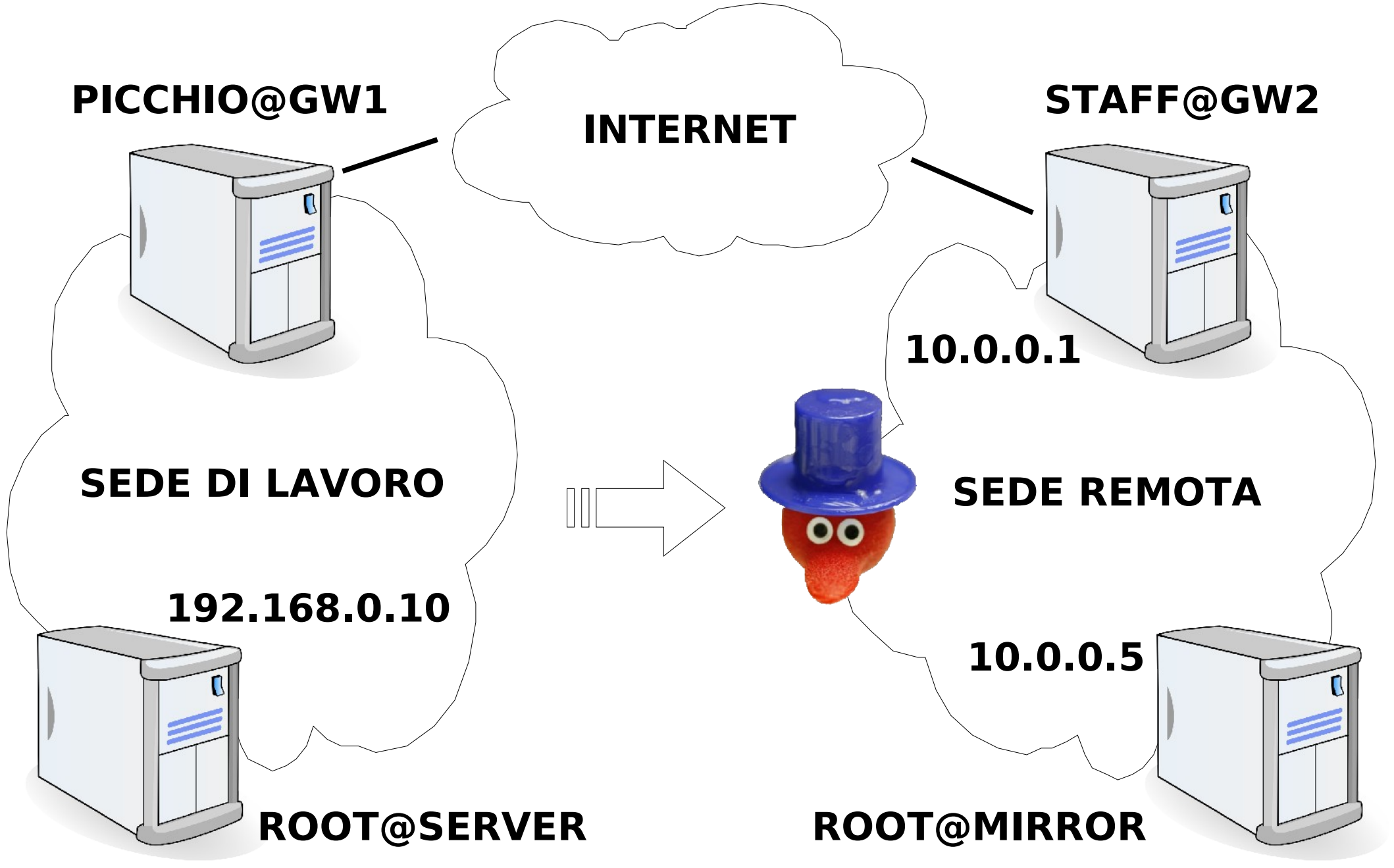
VENERDÌ: VPN FUORI SEDE

SETUP RETE

LIMITARE L'USO

Posso creare una vpn con ssh?

DALL'ALTRA RETE

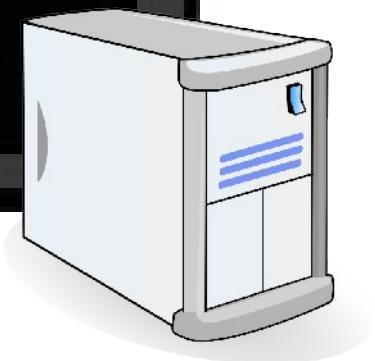


TUNNEL SSH

```
$ man ssh
[...]
VPN basate su ssh.
 ssh ha il supporto per i tunnel
 VPN usando la pseudo interfaccia
 tun(4)

Puo` essere configurato tramite
sshd_conf(5), nel quale si puo`
indicare a chi consentire l'uso
del tunnel e le sue caratteristiche
[...]
```

ABILITARE IL TUNNEL

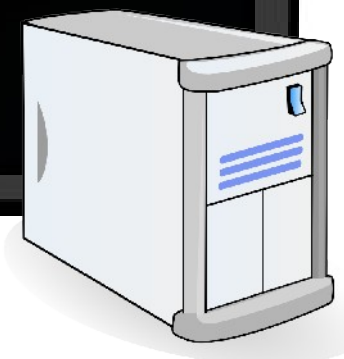
```
$ man sshd_config
[...]
PermitTunnel
 Permette di specificare il tunnel
 da usare:
 - point-to-point (layer 3)
 - ethernet (layer 2)
 - yes (entrambi)
 - no

il default e` “no”
```



SETUP VPN

```
# ssh -f -w 0:1 \
 picchio@GW1 true

# ifconfig tun0 \
 192.9.1.1 192.9.1.2 \
 netmask 255.255.255.255

# route add
192.168.0.0/24 192.9.1.2
```

```
# ifconfig tun1 \
 192.9.1.2 192.9.1.1 \
 netmask 255.255.255.252

# route add \
 192.9.1.1/32 192.9.1.1
```



GW1

VENERDÌ: VPN FUORI SEDE

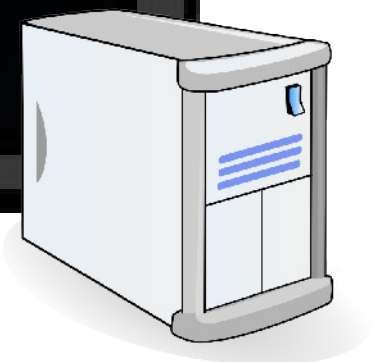
SETUP RETE

LIMITARE L'USO

Posso creare una vpn con ssh?

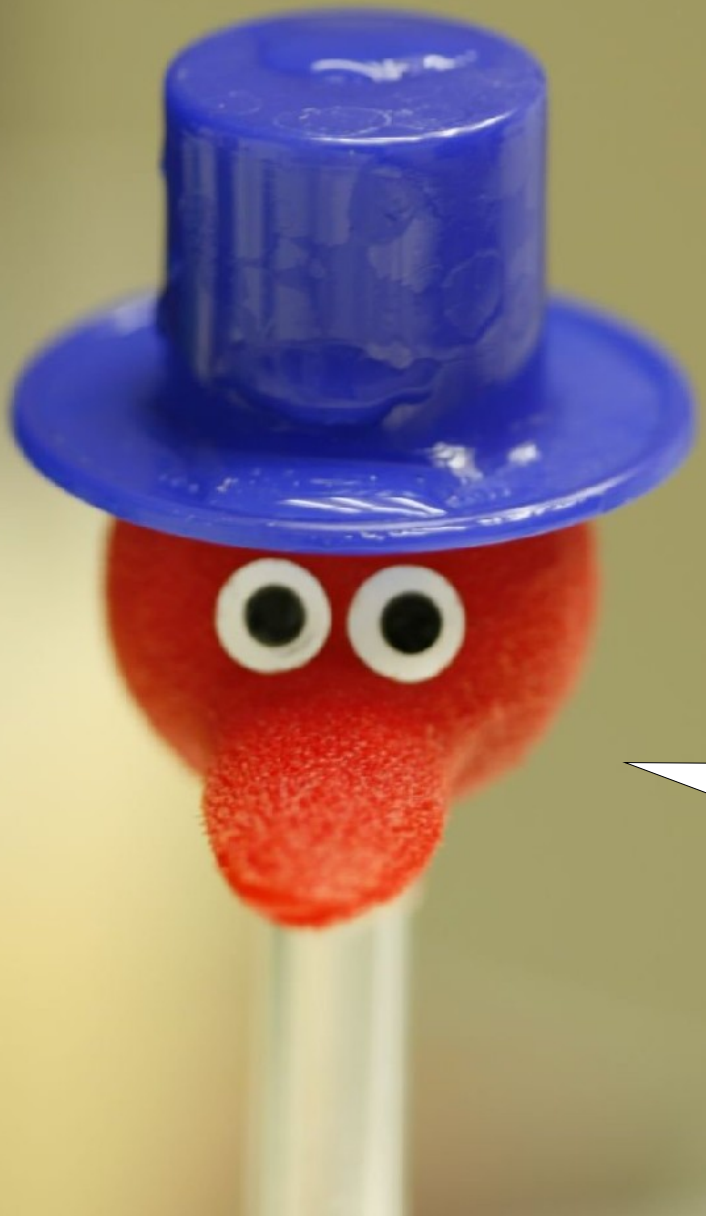
LIMITARE L'USO DI VPN

```
vim ~/.ssh/authorized_keys

tunnel="1",command="~/netstart" \
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAA
QEAvl7c13YvGkOLMKfr14GI07twaQOkFp
[...]
jwjnQRSiA/w== picchio@local
```



SERVER

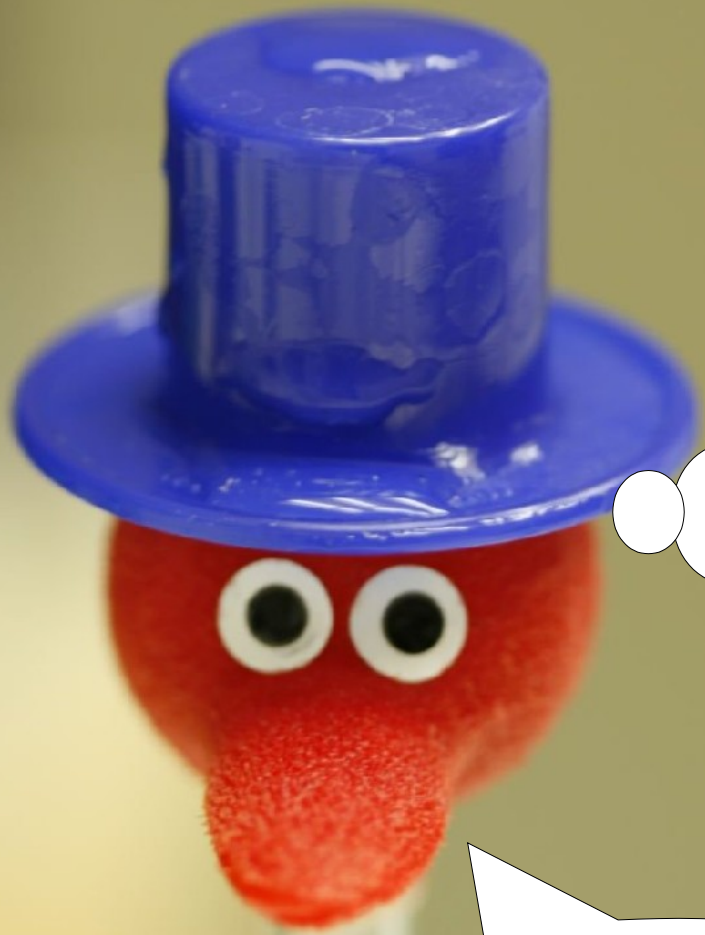
VPN FUORI SEDE!



- SETUP RETE
- LIMITARE L'USO

Posso creare una vpn con ssh?
SI

WEEKEND: DIVERTIMENTO!



Dopo tanto lavoro ci si diverte!

CONCETTI CHIAVE

- COPIA DI FILE CON SCP
- AUTENTICAZIONE CON CHIAVI
- LIMITARE SULL'USO DELLE CHIAVI
- ESECUZIONE COMANDI REMOTI
- PROXY COMMAND
- SALTI SSH MULTIPLI
- SSH-AGENT
- PORT FORWARDING
- SSH TUNNEL