Amministrazione di Sistemi 6 CFU

Parte II - Pratica - 2021-09-06

NOTE PRELIMINARI

La prova prevede lo svolgimento di una serie di attività. Qualsiasi file venga creato o modificato deve essere incluso in un archivio da comporre come specificato qui di seguito.

Laddove si svolgano operazioni di configurazione attraverso strumenti, e non modificando direttamente uno o più file, le si descrivano in un file di testo con nome **note.txt** inserito nella directory associata all'attività svolta.

Consegnare solo le linee significative dei file di configurazione, eliminando tutti i commenti.

Nell'archivio devono essere inclusi anche i file **.bash_history** di tutti gli utenti utilizzati durante lo svolgimento della prova.

L'archivio deve avere nome **ammsis.tar.gz** (e formato coerente con l'estensione) e il contenuto deve essere strutturato come da esempio qui di seguito (i nomi dei file sono solo per dare un esempio della struttura, si ribadisce che devono essere inclusi tutti i file creati o modificati). Usare solo lettere minuscole e senza accenti, e non utilizzare spazi nei nomi delle directory relative ai vari host e alle attività.

attivita0/client/root/.bash_history

attivita0/router/home/las/.bash_history

attivita0/maketar.sh

attivita1/client1/etc/network/interfaces

attivita1/server1/etc/network/interfaces

attivita2/router/etc/dnsmasq.conf

attivita3/note.txt

Solo questo archivio deve essere consegnato via EOL. La struttura e la correttezza dei nomi sarà valutata.

Attività 0 - automazione della consegna

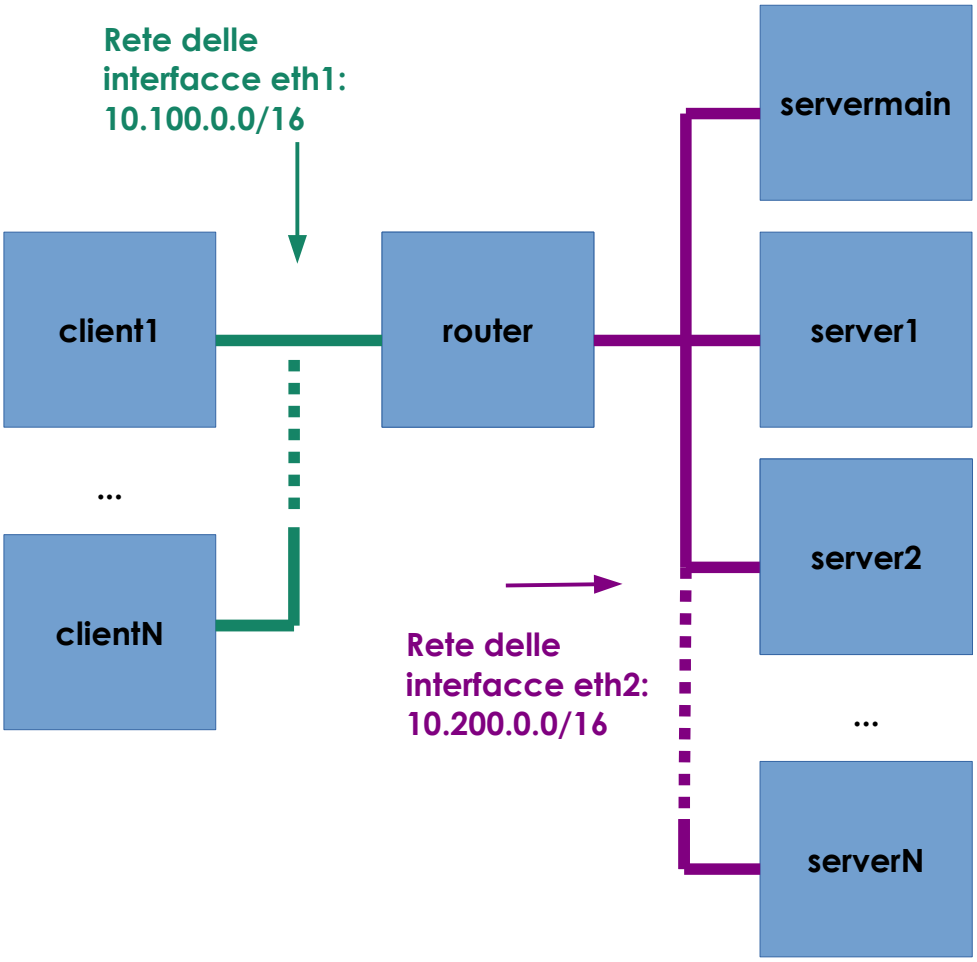
Predisporre su di una macchina a piacere (l'host o una delle VM) uno script **maketar.sh** che crei automaticamente l'archivio da consegnare, prelevando i file necessari da tutte le VM (si considerino parte di questa attività i file .bash_history). Lo script sarà oggetto di valutazione, va esso stesso incluso nell'archivio, come da esempio sopra fornito.

```
maketar.sh
# su host Linux
# dopo aver installato la chiave pubblica dell'utente dell'host
# negli account root delle varie VM

mkdir esame
cd esame

# per ogni file da consegnare...
scp 192.168.56.202:/etc/dnsmasq.conf  attivita2/router/etc/dnsmasq.conf
# ...

tar czf ../ammsis.tar.gz *
cd ..
```

Contesto dell'esercizio

Si immagini un'infrastruttura in cui client pubblici siano disponibili per accedere a un pool di risorse di calcolo. Sui client qualunque utente può effettuare il login come utente *las*, password *las* (in ogni istante su ogni client può essere presente un solo utente), per collegarsi poi via SSH a un server, utilizzando credenziali personali. Il collegamento è mediato da un router che guida la connessione verso il server più scarico tra quelli disponibili.

Attività 1 - rete



Considarando lo schema di rete fornito, configurare 5 macchine virtuali: **client1**, **router**, **servermain**, **server1**, **server2** (il sistema deve essere immaginato e predisposto per scalare a un numero arbitrario di client e di server, ma per i test si possono considerare solo gli host indicati)

router deve avere su eth1 l'indirizzo 10.100.0.1 e su eth2 l'indirizzo 10.200.0.1.

Router deve erogare via DHCP

- ai **client1/...** indirizzi nel range 10.100.1.1 - 10.100.9.254
- ai **server1/2/...** indirizzi nel range10.200.1.1 - 10.200.1.254
- al server **servermain**, sulla base del MAC address, rigidamente l'indirizzo 10.200.2.1
- a tutti gli host le rotte appropriate perché i client possano comunicare coi server attraverso router

client1:/etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet dhcp

# per funzionamento script consegna
auto eth3
iface eth3 inet static
  address 192.168.56.201
  netmask 255.255.255.0
```

server1:/etc/network/interfaces

server2:/etc/network/interfaces

servermain:/etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth2
iface eth2 inet dhcp

# per funzionamento script consegna
auto eth3
iface eth3 inet static
  address 192.168.56.203 / 204 / 205
  netmask 255.255.255.0
```

router:/etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
  address 10.100.0.1
  netmask 255.255.0.0

auto eth2
iface eth2 inet static
  address 10.200.0.1
  netmask 255.255.0.0

# per funzionamento script consegna
auto eth3
iface eth3 inet static
  address 192.168.56.202
  netmask 255.255.255.0
```

router:/etc/dnsmasq.conf

```
interface=eth1
interface=eth2
dhcp-range=10.100.1.1,10.100.9.254,12h
dhcp-range=10.200.1.1,10.200.1.254,12h
# dopo aver scoperto il MAC di servermain
dhcp-host=aa:bb.cc:dd:ee:ff,10.200.2.1
dhcp-option=3
dhcp-
option=121,10.100.0.0/16,10.200.0.1,10.200.0.0/16,10.100.0.1
```

router:/etc/sysctl.conf

```
net.ipv4.ip_forward=1
```

Attività 2 - autenticazione e storage

Su tutti gli host deve essere abilitata l'autenticazione centralizzata degli utenti, configurata per interrogare la directory installata e configurata su **servermain**.

servermain deve esportare verso gli altri server, via NFS, la directory **/home**, e i server la devono montare automaticamente nella stessa posizione.

attivita2/note.txt	su servermain si creano le entry ou=People,dc=labammsis e ou=Groups,dc=labammsis su tutte le macchine si installano i pacchetti libpam−ldap e libnss−ldap e quando richiesto si fornisce come server da usare ldapi://10.200.2.1/
per ogni macchina: /etc/ldap/ldap.conf	BASE dc=labammsis URI ldapi://10.200.2.1/
per ogni macchina: /etc/nsswitch.conf	aggiungere *ldap* tra le fonti passwd e group
servermain:/etc/exports	/home 10.200.1.0/24(rw,no_subtree_check)
server1 e server2: /etc/fstab	10.200.2.1:/home /home nfs defaults 0 0

Attività 3 - Stima del carico

Realizzare su **server1** (sarà poi disponibile su tutti i server) uno script **/home/count.sh** che resti continuamente in ascolto di pacchetti in arrivo dalla rete dei client che richiedono l'apertura di una nuova connessione sulla porta *ssh*. L'indirizzo sorgente deve essere scritto, attraverso rsyslog, sul file **/var/log/conn.log**

Lo script deve essere automaticamente avviato al boot e riavviato in caso di terminazione anomala.

server1: /home/count.sh	`#!/bin/bash`
	
	`tcpdump -i eth2 -nlp src net 10.100.0.0/16 and dst port 22 and 'tcp[tcpflags] && tcp-syn != 0' | while read T IP SIP RESTO ; do`
	`    echo $SIP | cut -f1-4 -d. | logger -p local1.info`
	`done`

server1 e server 2: /etc/rsyslog.d/ count.conf	local1.=info /var/log/conn.log
server1 e server 2: /etc/systemd/system/count.service	[Service] Type=simple ExecStart=/home/count.sh Restart=on-failure [Install] Wanted-by=basic.target

Attività 4 - Rilevazione del carico

Realizzare su **router** uno script **/root/poll.sh** che esplori l'intervallo di indirizzi assegnabili ai server, ricavando via SNMP il carico di ogni server attivo (si noti che nell'intervallo di indirizzi solo alcuni server possono essere attivi e quindi rispondere alla query).

Il carico è definito come il numero di linee presenti nel file **/var/log/conn.log** di un server. Lo script deve memorizzare nel file **/tmp/bestserver** l'indirizzo del server col carico più basso.

Lo script deve essere eseguito automaticamente ogni 3 minuti; l'esplorazione deve quindi essere svolta in modo da concludersi in un tempo molto più breve, indipendentemente da quanti server siano raggiungibili nell'intervallo di indirizzi considerato.

router:
/root/poll.sh
	function getLoad() {
	  snmpget -Ovq -v 1 -c public $1 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"poll\"
	}
	
	for S in 10.200.1.{1..254} ; do
	  getLoad $S > /tmp/$S &
	done
	
	wait
	
	for S in 10.200.1.{1..254} ; do
	  echo $(cat /tmp/$S) $S
	done | sort -n | head -1 | awk '{ print $2 }' > /tmp/bestserver

server1 e server2: /etc/snmp/ snmpd.conf	# aggiungere extend-sh poll /bin/wc -l /var/log/conn.log | /bin/cut -f1 -d' '

Attività 5 - utilizzo dei server

Realizzare su **client1** uno script **/home/las/connect.sh** con queste specifiche:

- Richiede come parametro sulla riga di comando un nome utente, ed eventualmente uno o più altri parametri che rappresentano nell'insieme una riga di comando da eseguire in remoto
- Ricava l'indirizzo del server più scarico con una query SNMP rivolta a **router** (che, si ricordi, conserva queste informazione nel file /tmp/bestserver)
- Avvia una connessione *ssh* verso tale server a nome dell'utente indicato come primo parametro, (eseguendo in remoto il comando specificato dagli altri parametri, se presenti). La password verrà quindi richiesta direttamente dal comando ssh.

client1: /home/las/connect.sh	test "$1" \|\| exit 1 IP=$(snmpget -Ovq -v 1 -c public 10.100.0.1 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"connect\") U="$1" shift ssh "$U"@"$IP" "$@"
router: /etc/snmp/snmpd.conf	extend-sh connect /bin/cat /tmp/bestserver