Amministrazione di Sistemi - Parte II (pratica) - 14 giugno 2021

Modalità di consegna

Per ogni esercizio, consegnare un archivio compresso che contenga 4 directory (una per ogni host menzionato nell'esercizio 1). In tali directory inserire tutti i file creati o modificati nelle rispettive macchine, includendo sempre i file .bash_history di tutti gli utenti impiegati.

Esempio di struttura del file da consegnare (non esaustivo dei file da includere):

esercizio1.tgz

```
Client/etc/nsswitch.conf
Client/root/.bash_history
Router/etc/dnsmasq.conf
Router/root/.bash_history
Server1/etc/network/interfaces
Server1/root/.bash_history
Server2/etc/network/interfaces
Server2/root/.bash_history
```

VALUTAZIONE:

1 punto per aver tentato in qualsiasi modo di consegnare gli archivi,

2 punti per tutti i nomi e i formati corretti dei file archivio

2 punti per struttura interna corretta

esercizio1

Configurare 4 macchine virtuali: Client, Router, Server1, Server2

Router deve avere su eth1 l'indirizzo 10.10.10.254 e su eth2 l'indirizzo 10.20.20.254.

Router deve erogare via DHCP

- ai Client indirizzi nel range 1-10 della rete 10.10.10.0/24,
- ai Server indirizzi nel range 1-10 della rete 10.20.20.0/24,
- a tutti le rotte appropriate perché i Client possano comunicare coi Server attraverso Router

Su tutte le macchine Client e Server deve essere abilitata l'autenticazione centralizzata degli utenti, configurata per interrogare una directory LDAP all'indirizzo 10.20.20.20

SOLUZIONE

- tutti i file .bash_history [1 punto]
- file /etc/nsswitch.conf identico per le VM Client, Server1, Server2 [1 punto]

  aggiungere `ldap` alle righe `passwd, shadow, group, gshadow`

- file /etc/ldap/ldap.conf identico per le VM Client, Server1, Server2 [1 punto]

```
BASE dc=labammsis
URI ldap://10.20.20.20/
```

- file /etc/network/interfaces di Router [2 punt1]

```
auto eth1
iface eth1 inet static
      address 10.10.10.254
      netmask 255.255.255.0
auto eth2
iface eth2 inet static
      address 10.20.20.254
      netmask 255.255.255.0
```

- file /etc/network/interfaces di Client [1 punto]

```
auto eth1
      iface eth1 inet dhcp
```

- file /etc/network/interfaces di Server1 e Server2 [1 punto]

```
auto eth2
      iface eth2 inet dhcp
```

- file /etc/dnsmasq.conf di Router [3 punti]

```
interface=eth1
interface=eth2
dhcp-range=10.10.10.1,10.10.10.10,12h
dhcp-range=10.20.20.1,10.20.20.10,12h
dhcp-option=3
dhcp-option=121,20.20.20.0/24,10.10.10.254,10.10.10.0/24,10.20.20.254
```

esercizio2

Su ognuno di due Server (idealmente quelli configurati all'esercizio 1, o se non si è svolto questo, sul server preconfigurato durante il corso e su di un suo clone),

- Installare una directory LDAP per l'autenticazione centralizzata
- Realizzare uno script **ldap.sh** che svolga queste operazioni:

a) Se è presente un parametro di valore "**new**", devono essere cancellate dalla directory locale tutte le entry sotto **ou=People,dc=labammsis**, e devono essere sostituite col contenuto del file **/tmp/dir.backup** del Router, prelevato via SSH/SCP

b) Se non è presente alcun parametro, deve essere fatto un dump in formato LDIF di tutte le entry sotto **ou=People,dc=labammsis**, e trasferito via SSH/SCP nel file **/tmp/dir.backup** del Router

c) Se è presente un parametro ma di valore diverso, o più parametri, devono essere loggati via syslog sul file **/var/log/ldap.errors** del Router

Nota: i trasferimenti via SSH devono essere automatizzati, e non richiedere password

SOLUZIONE

- tutti i file .bash_history [1 punto]

  (si deve vedere l'aggiunta delle OU a LDAP su Router)

- ldap.sh [9 punti]

```
#!/bin/bash
if [[ "$1" = "new" && -z "$2" ]] ; then
      ldapsearch –x –LLL –D cn=admin,dc=labammsis –b  ou=People,dc=labammsis -s one –w gennaio.marzo –H ldapi:/// |
            egrep ^dn: | ldapdelete -x -D cn=admin,dc=labammsis –b dc=labammsis –w gennaio.marzo –H ldapi:///
      # NOTA: si può usare anche un ldapdelete -r, ricordando però di ricreare il nodo ou=People,dc=labammsis
      ssh 10.20.20.254 "cat /tmp/dir.backup | ldapadd -x -D cn=admin,dc=labammsis –b dc=labammsis –w gennaio.marzo
–H ldapi:///
elif [ -z "$1" ] ; then
      ldapsearch –x –LLL –D cn=admin,dc=labammsis –b ou=People,dc=labammsis -s one –w gennaio.marzo –H ldapi:/// |
            ssh 10.20.20.254 "cat > /tmp/dir.backup"
else
      logger -p local1.notice -t parametri "$@"
fi
```

- file /etc/rsyslog.d/ldaperr.conf dei Server [1 punto]

```
local1.=notice    @10.20.20.254
```

  # Nota: equivalente anche non usare questo file e mettere invece -n 10.20.20.254 nel comando logger

- file /etc/rsyslog.d/ldaperr.conf di Router [1 punto]

```
local1.=notice    /var/log/ldap.errors
```

- file /root/.ssh/id_rsa e /root/.ssh/id_rsa.pub dei Server [1 punto]

  come generati da ssh-keygen

- file /root/.ssh/authorized_keys di Router [1 punto]

  contiene le due chiavi pubbliche dei Server

esercizio3

Su ognuno di due Server (idealmente quelli configurati all'esercizio 1, o se non si è svolto questo, sul server preconfigurato durante il corso e su di un suo clone) realizzare uno script **failback.sh** che svolga queste operazioni:

a) Interroga via SNMP il Router, che deve rispondere col contenuto del proprio file **/tmp/server.attivo**. Il contenuto di tale file consiste nel nome di un server (Server1 o Server2) seguito eventualmente da uno spazio e dalla parola "new"

NOTA: l'agent SNMP di Router chiaramente deve essere configurato appositamente per erogare il file quando viene richiesto uno specifico OID; la configurazione dell'agent deve essere consegnata.

b) Se il risultato ottenuto contiene il nome del server su cui è in esecuzione lo script (Server1 o Server2), lo script assegna all'interfaccia eth2 l'indirizzo aggiuntivo 10.20.20.20, altrimenti lo script si assicura che l'interfaccia eth2 non detenga l'indirizzo 10.20.20.20, deconfigurandolo se necessario.

c) Lancia lo script ldap.sh, passando come parametro la parola "new" se è presente nella risposta SNMP

Configurare Server1 per eseguire failback.sh a ogni minuto dispari, e Server2 per eseguirlo a ogni minuto pari.

SOLUZIONE

- file /etc/snmp/snmpd.conf di Router [2 punti]

  # configurazione porta ascolto, view, community
  ```
  extend failback /bin/cat /tmp/server.attivo
  ```

- failback.sh [8 punti]

  ```
  #!/bin/bash
  snmpget -v 1 -c public 10.20.20.254 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"failback\" |
        awk -F 'STRING: ' '{ print $2 }' | (
              read NAME PARAM
              if [ "$NAME" = "$(hostname)" ] ; then
                    ip a | grep -qw 10.20.20.20/24 || ip a add 10.20.20.20/24 dev eth2
              else
                    ip a | grep -qw 10.20.20.20/24 && ip a del 10.20.20.20/24 dev eth2
              fi
              test "$PARAM = "new" || PARAM=""
              /root/ldap.sh $PARAM
        )
  ```

- crontab di root o equivalente [2 punti ognuno]

  per Server1: `1-59/2 * * * * /root/failback.sh`

  per server2: `0-58/2 * * * * /root/failback.sh`