Laboratorio di Amministrazione di Sistemi T

Prova pratica del 5 settembre 2016

Descrizione del problema

Si vuole realizzare un sistema di monitoraggio e diagnostica per una rete di calcolatori. Ogni calcolatore della rete 10.1.1.0/24 può registrare sul sistema di controllo 10.1.1.254 un elenco di processi da monitorare e un elenco di porte TCP consentite, sotto forma di entry LDAP, come nell'esempio illustrato a fianco:

```
dn: ip=10.1.1.1,dc=labammsis
objectClass: monitor
ip: 10.1.1.1
proc: dosomething.sh
proc: beuseful.sh
port: 22
port: 80
```

Il sistema di controllo configura in modo appropriato gli agenti snmp (che per ipotesi sono usati solo per questo compito) dei calcolatori da monitorare per poter successivamente verificare su ognuno se i processi sono in esecuzione.

Script da realizzare

(CAL) = installato su calcolatore ; (SDC) = installato su sistema di controllo

mon.schema.ldif (SDC) – Schema LDAP che permette l'inserimento di entry come da esempio.

add.sh (CAL) – Opera sulla entry LDAP relativa al calcolatore su cui viene lanciato. Accetta tre parametri. Il primo è una stringa, *add* o *del*, che indica se aggiungere o togliere un elemento alla entry. Il secondo è il tipo di elemento, *proc* o *port*. Il terzo è il valore. Ogni volta che viene invocato, realizza l'operazione richiesta, e logga l'IP della macchina e i tre parametri via syslog.

Esempio: `add.sh add proc dosomething.sh`

Indicare nelle note come configurare rsyslog su calcolatori e sistema di controllo perché tutti i messaggi prodotti vengano scritti sul file `/var/log/updates` del sistema di controllo

net.sh (CAL) – Accetta un numero di porta TCP come parametro, e stampa la stringa OPEN se rileva che sulla macchina è attiva almeno una connessione verso tale porta di un'altra macchina

update.sh (SDC) – Osserva continuamente il file `/var/log/updates`; ogni volta che rileva un nuovo messaggio rigenera il file `snmpd.conf` per il calcolatore che l'ha prodotto, come dettagliato di seguito, utilizzando i dati della relativa entry LDAP, per poi installarvelo.

Il file `snmpd.conf` deve contenere una riga per ogni attributo *proc* della entry LDAP, che consenta di verificare se il processo è in esecuzione sul calcolatore, e una riga per ogni attributo *port* della entry LDAP, che utilizzando *net.sh* consenta di verificare se ci sono connessioni attive sul calcolatore verso la relativa porta.

Indicare nelle note come vanno predisposti tutti i sistemi per consentire l'installazione del file `snmpd.conf` sui calcolatori da parte del sistema di controllo

procmon.sh (SDC) – Accetta come parametri un indirizzo IP di un calcolatore e un elenco di nomi di programmi (senza path) più eventuali altri che possano essere utili alla soluzione. Controlla via SNMP se sul calcolatore sono in esecuzione tutti i processi corrispondenti. Per ogni processo non trovato, si collega al calcolatore e prova a rilanciare il programma. Pianifica il controllo perché venga rieseguito dopo cinque minuti, per un massimo di tre tentativi. Si ipotizzi che tutti i programmi siano installati in /usr/bin.

portmon.sh (SDC) – Accetta come parametri un indirizzo IP di un calcolatore e un elenco di porte. Controlla via SNMP se sul calcolatore sono attive connessioni verso le porte specificate, e qualora ne trovi configura il packet filter sul sistema di controllo (che è anche il default gateway dei calcolatori) in modo che il traffico non possa più essere inoltrato.

monitor.sh (SDC) – Individua tutti i calcolatori che hanno entry LDAP, e per ognuno lancia *procmon.sh* con l'elenco di tutti i processi da controllare e *portmon.sh* con l'elenco di tutte le porte da controllare.

Indicare nei commenti come far eseguire automaticamente lo script ogni ora