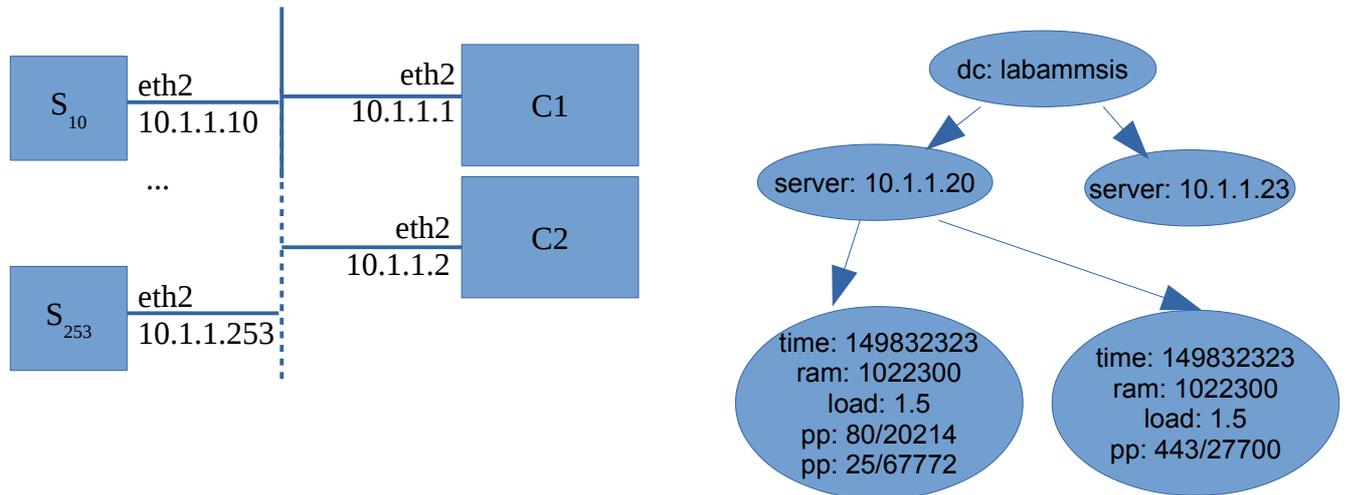


# Laboratorio di Amministrazione di Sistemi T

## Prova pratica del 17 luglio 2017

### Descrizione generale del problema



Un sistema di monitoraggio ad alta disponibilità è costituito da una coppia di macchine “controller” (C1 e C2).

In condizioni normali C1 effettua la rilevazione periodica di alcuni parametri di funzionamento dei server di un pool che può contenere fino a 244 macchine numerate da 10 a 253, non necessariamente tutte presenti o sempre accese. I dati vengono memorizzati sulla directory LDAP locale e su quella di C2, costruendo un DIT esemplificato in figura.

Se C2 rileva un’assenza prolungata di aggiornamenti LDAP da C1, si ipotizza che questo sia un sintomo certo del guasto di C1, e quindi si deve fare in modo che C2 ne prenda il posto.

## File da consegnare

(tutti gli script e i file di configurazione devono essere disponibili su entrambi i controller – normalmente sono in esecuzione su C1, fatta eccezione per *standby.sh* che viene eseguito su C2, e fatta eccezione per le condizioni di guasto descritte in tale script)

**finder.sh** – Lo script esegue ogni 30 secondi una scansione dell'intervallo di indirizzi dei server per rilevare col comando *nc* quali sono accesi e hanno il server SSH in ascolto (implementare il controllo in modo che l'intero set di tutte le potenziali risposte sia ricevuto nel giro di pochi secondi).

Per ogni nuovo server trovato rispetto all'iterazione precedente, invoca *config.sh* passando l'indirizzo come parametro, e al termine di questa sequenza scrive l'elenco completo degli indirizzi di tutti i server accesi nel file */root/active.list*

**config.sh** – Lo script, girando sul controller, deve fare in modo che sul server remoto specificato come parametro vengano eseguite queste operazioni:

- configurazione del packet filter per far sì che siano mandati al system logger i pacchetti in ingresso su ognuna delle porte TCP specificate, una per riga, nel file */root/ingress.list* (presente sul controller)
- configurazione del system logger perché i messaggi ricevuti dal packet filter siano inoltrati al controller su cui viene eseguito questo script (*config.sh*)
- configurazione dell'agent SNMP in modo da consentire la rilevazione della RAM libera e del carico del sistema

### Indicare nei commenti:

- cosa predisporre per consentire la connessione non interattiva dal controller ai server
- come configurare i syslog dei controller per scrivere i pacchetti ricevuti su */var/log/t.log*

**data.schema.ldif** – Definire i tipi di attributo *time*, *ram* (interi), *server*, *pp*, *load* (stringhe) e le classi *host* e *data* che li contengono come esemplificato in figura.

**logparse.sh** - Legge continuamente il file */var/log/t.log* per contare il numero di pacchetti visti per ogni server e ogni porta.

Quando riceve il segnale USR1, avvia un ciclo che per ogni server in */root/active.list*:

- legge via SNMP lo stato di RAM e carico medio negli ultimi 5 minuti
- compone una entry LDIF con i dati letti via SNMP e le statistiche sul traffico (il numero di pacchetti per porta va registrato nell'attributo *pp* nella forma *<porta>\_<num.pacch.>*) resettando contestualmente i contatori
- inserisce le entry sia su C1 che su C2

Lo script deve configurare il sistema perché invii automaticamente ogni 5 minuti il segnale USR1 al processo appropriato.

**standby.sh** – Su C2, controlla continuamente il contenuto della directory LDAP, e se non rileva nell'arco degli ultimi 10 minuti nuove entry, avvia un'istanza di *finder.sh* e di *logparse.sh*.