Appunti delle lezioni di Gestione di Sistemi e Reti
2006-2007

Franco Sirovich
© Franco Sirovich [1]

3. (Network) Control

Il testo fa riferimento solo al controllo della rete ma le considerazione sviluppate sono di portata assai più generale. Cercheremo di usare la parola "sistema gestito" al posto di "rete" per sottolineare la generalità dei temi presentati e delle soluzione proposte.

E' altresì opportuno sottolineare la differenza di significato fra i termini inglesi “monitoring” e “control”: ambedue in italiano si traducono con il termine "controllare", ma *monitoring* ha il significato di *tenere sotto esame*, mentre *control* significa controllare nel senso di essere capaci di *determinare e dettare il comportamento*. Per determinare il comportamento del sistema gestito, è necessario essere in grado di modificare (opportunamente) i parametri del sistema che ne influenzano il comportamento, come pure di fare eseguire specifiche azioni al sistema gestito. Queste funzionalità devono essere disponibili per tutti i componenti del sistema del sistema.

Le esigenze di controllo e di monitoring sono due aspetti della gestione che sono presenti in tutte le cinque aree funzionali: performance, fault, accounting, configuration e security. Nelle prime tre aree (performance, fault e accounting management) sono più pressanti le esigenze di monitoring, mentre nelle aree di configuration e di security management l'aspetto del controllo del comportamento è più importante di quello di monitoring. In ogni area funzionale della gestione si ritrova quindi, in grado diverso sia l'esigenza di monitoring che di controllo del comportamento.

Esamineremo quindi le due aree on cui gli aspetti di controllo sono più importanti, e ci ci permetterà di illustrare le tematiche di gestione che fanno capo a queste aree funzionali.

3.1. Controllo nella gestione della configurazione

Il configuration management si occupa di inizializzare, mantenere in esercizio e spegnere sia componenti individuali che sottosistemi logici di risorse di calcolo e di comunicazione nell'intero sistema da gestire. La gestione della configurazione detta in primo luogo il processo di inizializzazione (avvio) del sistema *identificando* e *specificando* le caratteristiche dei componenti e delle risorse che costituiscono il sistema da gestire. Per poter determinare il comportamento di un sistema occorre in primo luogo definire da quali componenti e risorse è costituito il sistema e in che

1 Quest'opera è stata rilasciata sotto la licenza Creative Commons Attribuzione-Non commerciale-Non opere derivate 2.5 Italia. Per leggere una copia della licenza visita il sito web http://creativecommons.org/licenses/by-nc-nd/2.5/it/ o spedisci una lettera a Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

modo questi componenti e risorse interagiscono.

Il termine risorsa è qui usato in senso assai generale; le risorse possono essere *risorse fisiche* quali una macchina server o una workstation o un router, ma anche oggetti "logici" quali una entità di transport, oppure ancora di livello più basso come il timer di ritrasmissione di un transport, o la massima dimensione del segmento, o la tabella di instradamento di IP.

La gestione della configurazione deve poter specificare sia i valori iniziali che quelli di default di attributi dei componenti del sistema, in modo tale che le risorse gestite inizino a lavorare nello stato desiderato, possedendo i valori appropriati dei parametri che determinano il loro comportamento, e che formino fra di loro le relazioni desiderate.

Mentre il sistema sta operando, la gestione della configurazione deve monitorare la configurazione, ed effettuare cambiamenti nella configurazione in risposta a comandi del gestore del sistema o di altre funzioni del sistema di gestione. Ad es., la funzione di performance management può chiedere di redistribuire il carico nel sistema, a seguito della rilevazione di uno sbilanciamento di carico; oppure il fault management può chiedere di isolare un componente che è stato individuato come guasto, in modo che non sia utilizzato nel sistema e quindi non ne deteriori il comportamento.

La gestione della configurazione include le seguenti funzioni:

- Definire la informazione di configurazione
- Settare e modificare valori di attributi
- Definire e modificare relazioni
- Inizializzare e terminare operazioni all'interno del sistema
- Distribuire il software
- Esaminare valori e relazioni
- Riportare lo stato (il cambiamento di stato) della configurazione

Le ultime due sono funzionalità più propriamente di monitoring, e sono realizzabili mediante interazioni di tipo domanda-risposta (polling), e funzionalità di event report. Le altre sono invece funzionalità di controllo: il confronto fra i due tipi di funzionalità aiuta a comprendere la differenza fra monitoring e controllo.

3.1.1. Definire la informazione di configurazione

L'informazione di configurazione descrive la natura e lo stato delle risorse che sono sottoposte a gestione. Per prima cosa occorre specificare quali sono le risorse, sia fisiche che logiche, che compongono il sistema, e quali loro attributi interessa specificare, ad es., nomi, indirizzi, numeri identificativi, stati, caratteristiche operazionali, numero di versione del software, livello di release.

Come ogni informazione di gestione, l'informazione di configurazione può essere strutturata in un certo numero di modi diversi.

- *Semplice lista di campi di dati*, nella quale ogni campo dati possiede un solo valore; questo approccio è seguito ad es. da SNMP, il sistema di gestione specificato da Internet.
- *Object-oriented database*, ad es. in OSI, in cui gli oggetti del database rappresentano elementi di interesse per la gestione. Questo approccio è seguito dal sistema di gestione di OSI. Ogni oggetto può contenere numerosi *attributi*, che descrivono caratteristiche dell'oggetto, *comportamenti*, che l'oggetto è in grado di eseguire, e *notifiche*, che l'oggetto è in grado di inviare ai manager. L'uso del contenimento e delle relazioni di ereditarietà permette di definire relazioni fragli oggetti.

- *Database relazionale*, in cui i vari campi delle relazioni contengono valori che riflettono caratteristiche di componenti e risorse del sistema gestito; la struttura del database riflette relazioni fra i componenti del sistema.

Questa informazione di configurazione è certamente disponibile sulle macchine manager, che sono quelle che effettuano il monitoring e il controllo del sistema, ma deve essere anche immagazzinata "dentro" la risorsa a cui si riferisce, perché la risorsa fa uso di questa informazione nelle sue operazioni. Spesso, l'informazione d configurazione è anche contenuta nell'agent che gestisce la risorsa, perché deve sapere come interagire con la risorsa e quale informazioni la risorse dovrebbe avere. Nei componenti che non ospitano un agent di gestione e che sono gestiti via proxy, l'informazione di gestione può essere contenuta all'interno del proxy.

La funzione di controllo dovrebbe permettere di specificare il tipo delle informazioni di configurazione, e anche di introdurre nuovi tipi di oggetti o di elementi informativi. Questa forma importante di estensione è raramente supportata perché è molto complessa da implementare dal lato della risorse e dei componenti che devono utilizzare questi nuovi tipi di informazione. Quando una forma di estensione è presente, richiede quasi sempre che la risorsa sia messa off-line, riconfigurata in modo che accetti i nuovi tipi di informazione di gestione, e poi rimessa on-line perché venga sottoposta a nuova inizializzazione da parte del sistema di gestione.

3.1.2. Settare e modificare valori di attributi

Il controllo della configurazione dovrebbe permettere ad un manager di modificare da remoto i valori degli attributi negli agent e nei proxy (che poi a loro volta devono effettuare le necessarie modifiche sulla risorsa vera e propria. Tali modifiche devono esseresoggette a due limitazioni. In primo luogo, il manager deve essere autorizzato a fare il cambiamento: non è accettabile che una operazione che può avere effetti "devastanti" sul comportamento del sistema gestito possa essere effettuata senza verificare che chi la richiede ha i diritti per eseguire tale operazione. In secondo luogo, vi sono attributi che riflettono la natura della risorsa: tali attributi devono essere non modificabili; ad es. il numero e la natura delle schede di un router non sono informazioni che ha senso che il manager modifichi, mentre informazioni quale la indicazione della persona responsabile della gestione dell'apparato, oppure l'indirizzo IP legato ad una interfaccia di rete *devono* essere modificabili dal manager, una volta che ci si sia accertati che sia proprio il manager a richiedere la modifica.

Vari tipi di modifiche sono possibili, principalmente a seconda della natura della informazione modificata.

- *Modifica nel solo database*: In questi casi ma modifica delle informazioni nel database delle informazioni di gestione non ha (altri) effetti sulla risorsa. Questo approccio è utilizzato quando il valore dell'attributo non influenza il comportamentodella risorsa; ad es. nome della persona responsabile della risorsa.
- *Modifica nel database e modifica nella risorsa*: la risorsa viene modificata perché l'attributo determina almeno parte del comportamentodella risorsa; ad es. settare a "disabilitata" una scheda di un router.
- *Modifica nel database e azione*: in alcuni ambiente di gestione (ad es. SNMP) non esiste la possibilità di ordinare l'esecuzione di azioni. In questi casi le azioni vengono intraprese dall'agent in risposta alla modifica di attributi della risorsa. L'azione intrapresa dall'agent può ovviamente consistere nell'eseguire azioni o richiedere l'esecuzione di comandisulla risorsa gestita. Un esempio potrebbe essere il reset di una interfaccia di rete di un router, o il reboot di un host o di un servizio.

3.1.3. Definire e modificare relazioni

Una relazione fra componenti o risorse del sistema gestito può descrivere informazione di natura molto diversa. Ad es.

- una associazione,
- una connessione,
- una condizione,

che esistono fra componenti e/o risorse del sistema. Essere in grado di descrivere una relazione è assai diverso che descrivere semplicemente gli elementi della relazione, perché nel caso della relazione è più facile mantenere la "integrità" della relazione.

Come osservazione conclusiva, è opportuno notare che la modifica delle risorse non dovrebbe richiedere lo spegnimento dell'intero sistema, e nemmeno del componente. Infatti, la re-inizializzazione del sistema o del componente comporta un tempo di indisponibilità del servizio che a volte può anche essere notevole. Per avere però questa modificabilità "a caldo" occorre che la risorsa stessa sia in grado di accettare modifiche a caldo; il sistema di gestione può solo richiedere comportamenti che la risorsa sia in grado di esibire. Occorre quindi non confondere limitazioni della risorsa con l'ambiente (quello di gestione) in cui queste limitazioni sono rese evidenti!

3.1.4. Inizializzare e terminare operazioni

Il sistema di gestione della configurazione dovrebbe permettere di far partire e arrestare le operazioni del sistema o di alcune sue parti. La inizializzazione deve includere la verifica che tutte le inizializzazioni dei parametri di configurazione siano state effettuate e le relazione definite appropriatamente. Le inizializzazioni mancanti devono esseresegnalate al gestore

I comandi di terminazioni devono permettere la richiesta del salvataggio o meno di informazioni statistiche.

3.1.5. Distribuire software

La gestione della configurazione dovrebbe permetteredi distribuire software sui sistemi intermedi e finali. Oltre ad eseguibili dovrebbe essere distribuibile anche informazione accessoria quale tabelle o dati che guidano la esecuzione del software. Molto importanti ad es. le tabelle di routing: vi sono casi di software, come ad es. IP, che sono talmente guidati da dati di configurazione che distribuire solo il software risolve solo una piccola parte del problema.

3.2. Controllo della sicurezza

Le tematiche di controllo della sicurezza dovrebbero essere già state coperte dai corsi di sicurezza che avete fatto; per un breve riassunto, si può fare riferimento al libro di testo. Chi non ha fatto esami di sicurezza studi il capitolo sul libro, perché potrà capitare di dover parlare di sicurezza usando le conoscenze ivi contenute.

In particolare occorre avere dimestichezza con la diversità fra le funzionalità di *segretezza* (detta anche *confidenzialità*), *integrità*, e *disponibilità* (*availability*). Sono caratteristiche di sicurezza che è necessario che tutti i sistemi informatici posseggano (anche in gradi diversi).

Gli attacchi che vengono fatti ai sistemi sono attacchi a queste caratteristiche di sicurezza: *interruzione*, contro la disponibilità, *intercettazione*, contro la confidenzialità, *modifica*, contro la integrità, *contraffazione*, contro la integrità.

Gli attacchi si dividono in *attacchi passivi*, ad es. *divulgazione di contenuti* e *analisi del traffico,*

che sono due forme di intercettazione, e attacchi attivi, ad es. *modifiche del flusso dei messaggi*, *denial of service*, e *masquerade* che sono forme di intercettazione e di interruzione. Gli attacchi passivi sono caratterizzati dalla assenzadi qualunque azione sull'obbiettivo dell'attacco (servizio di comunicazione, apparato, host, server, servizio applicativo, ...): sono quindi effettuati in modo da nascondere al massimo l'esistenza dell'attaccante. Negli attacchi attivi invece si agisce sul sistema attaccato (servizio di comunicazione,servizio applicativo, host, server, ...) in alcuni casi perch<è è necessario per ottenere il risultato desiderato (ad es. masquerade) in altri perché è proprio l'azione sul sistema il fine dell'attacco (ad es. denial of service).

Gli attacchi passivi sono molto difficili da individuare e quindi occorre esercitare molta attenzione sulla prevenzione degli attacchi piuttosto che sulla loro pronta individuazione.