Network Monitoring

&

Nagios

Introduzione all'attività di Network Monitoring
introduzione a Nagios come motore ideale

Nicholas Pocher
Poker SpA - Settimo Torinese, Novembre 2013

Indice **Pag.2**

Il Network Monitoring: che cos'è? Perché è importante? **Pag.3**

Nagios: perché è la scelta giusta? Che cosa fa? **Pag.4**

Nagios: i controlli di base **Pag.4**

Nagios: le notifiche **Pag.5**

Nagios: i requistiti hardware / software **Pag.6**

Il Network Monitoring: che cos'è? E perché è importante?

In tutte le aziende, il Network Monitoring è l'attività che impegna la maggior parte del tempo del personale dedicato all'area Information Technology.
Per "network monitoring" potremmo genericamente intendere il controllo del funzionamento e della salute della rete, e di tutte le periferiche ad essa collegate: dalla verifica dell'operatività di un server, allo stato di una stampante; dal controllo di un database al funzionamento delle connessioni esterne, e così via. Si tratta di operazioni spesso cruciali se non eseguite per tempo, o altre volte semplici ma gravose nella loro ripetitività … ma in tutti i casi è necessario un intervento puntuale e mirato. E, come è facile comprendere, l'impegno richiesto aumenta in modo proporzionale con l'aumentare della dimensione della rete, del numero di periferiche collegate e, soprattutto, **dei controlli che è necessario eseguire su di essa**.

Pertanto, è più corretto definire il **Network Monitoring** come **l'insieme dei controlli che è necessario eseguire, all'interno di una rete, per mantenerla in buona salute e per prevedere eventi critici, con il fine di assicurare, senza interruzioni, l'efficienza dell'intera struttura di Information Technology.**

Dal punto di vista dell'efficienza, quindi, è facile comprendere l'importanza strategica di poter eseguire l'attività di controllo in modo **centralizzato**, **costante** e **sostenibile**. La lista dei controlli da eseguire può essere lunghissima, e dipende dal tipo di rete, dalla dimensione, dalle periferiche e dalle attività considerate critiche; tuttavia è possibile determinare una serie di controlli di base (o di criticità da evitare) potenzialmente adatti, e quindi utili, alla maggior parte delle reti aziendali.

Dal punto di vista degli strumenti e delle risorse utili ad eseguire il network monitoring, è bene prendere in considerazione anche e soprattutto una piattaforma di tipo *open source*: l'impronta collaborativa permette non solo di determinare un **archivio esaustivo e aggiornato** delle casistiche, ma anche di poter realizzare le rispettive soluzioni, con un rapporto estremamente vantaggioso tra le risorse investite in sviluppo e i risultati operativi.

In parole più semplici: **con un investimento limitato, e in poco tempo, è possibile realizzare soluzioni sostenibili, efficienti e con un elevato contenuto tecnologico.**

Nagios

Nagios: perché è la scelta giusta? Che cosa fa?

Nagios è una soluzione open source, appositamente pensata e sviluppata per il monitoraggio delle infrastrutture IT.
E' una soluzione molto diffusa, e quindi è possibile reperire una grande quantità di controlli, personalizzazioni e parametrizzazioni, applicati a qualsiasi tipologia di rete. In particolare, **Nagios** rappresenta un'ottima base di partenza, dal punto di vista della soluzione finale:

- Perché il programma in sé è gratuito, e ciò permette di ridurre notevolmente i costi di base
- Perché è un "contenitore aperto" di tecnologia: il vero valore aggiunto si esprime attraverso la qualità e l'efficienza delle personalizzazioni
- Perché permette di eseguire tutti **i controlli di base** con un elevatissimo grado di affidabilità e garanzia di risultato.

Nagios: i controlli di base

Grazie alla sua struttura *open*, la comunità di **Nagios** nel corso degli anni ha determinato e sviluppato migliaia di controlli eseguibili nelle reti aziendali; tuttavia, possiamo identificare una famiglia più ristretta di controlli, che è sicuramente adatta alla maggior parte delle infrastrutture IT presenti in qualsiasi azienda: per la loro adattabilità universale, possono essere definiti come **controlli di base**, e di seguito ne presentiamo una sintetica panoramica.

Controllo di server Windows (stato, spazio su disco, processi, ecc)
Controllo di server Linux
Controllo di virtualizzatori VMWare
Controllo di servizi SMTP
Controllo di servizi POP
Controllo di servizi SSH
Controllo di servizi http
Controllo di servizi TCP
Controllo di servizi UDP

Nagios: le notifiche

L'analisi dell'infrastruttura, la determinazione dei controlli e la loro configurazione rappresentano certamente una buona parte del lavoro da portare a termine, per iniziare a utilizzare Nagios. Ma un controllo è inutile, fino a quando non invia un segnale relativo al verificarsi degli eventi per cui è stato impiegato: ecco perché è fondamentale portare a termine la corretta configurazione delle notifiche.
In linea di massima, le notifiche sfruttano due mezzi di comunicazione:

- Email: per ciascun controllo si determina una lista di destinatari (indirizzi email) che hanno titolo o necessità di ricevere l'esito o l'informazione relativa al controllo eseguito. Principalmente i destinatari sono persone o liste di distribuzione interne all'azienda; tuttavia, questo strumento rappresenta un'occasione per terziarizzare alcuni aspetti della gestione dell'infrastruttura (ad esempio: se stipulate un accordo preventivo con una società specializzata, le notifiche verranno inviate a personale esterno alla vostra rete)
- SMS: l'elevato potenziale di questo mezzo risiede nell'immediatezza di recapito (e di lettura): in qualsiasi ora del giorno e della notte, l'sms raggiunge un destinatario più rapidamente e con migliore esito dell'email.
  Un limite degli sms, inviati su rete GSM, è rappresentato da eventuali mancanze di copertura. Un'alternativa è inviare SMS attraverso servizi web; tuttavia, se un SMS dovesse ad esempio allarmare un tecnico in merito alla mancanza di linea dati, la notifica non arriverebbe mai a destinazione a causa della ragione stessa per cui era stata configurata. Quindi è bene effettuare la giusta scelta, in base a più fattori relativi all'infrastruttura da controllare.

Nagios: i requisiti Hardware / Software

Nagios ha conosciuto una crescita esponenziale nel corso degli anni, sia in termini di diffusione, sia per quantità di contenuti condivisi: un elemento che sicuramente ha favorito tale andamento è la sostenibilità dei requisiti hardware e software. Proviamo a capire in termini reali che cosa serve davvero per sostenere una buona installazione di Nagios:

- Hardware: è necessario dedicare un server a Nagios. E' sufficiente una macchina con caratteristiche paragonabili a quelle di un normale pc; inoltre, poiché essa verrà adibita unicamente a server, periferiche aggiuntive quali schede audio o video ad alte prestazioni non avranno alcuna rilevanza né utilità. Si potrà scegliere, ad esempio, un MicroServer di HP, o un Acer Veriton con processore Intel Celeron
- Software: il sistema operativo ideale, per l'esecuzione di Nagios, è Linux. Per garantire il massimo livello di affidabilità, oggi è preferibile scegliere una versione stabile come Ubuntu 12.04 LTS

L'investimento hardware è limitato, e il sistema operativo adottato è gratuito, pertanto la soluzione Nagios è sostenibile da subito, e i suoi costi di realizzazione variano in funzione delle effettive necessità.