

DigitalExpert

Consulenze Informatiche

di Carloalberto Sartor

via Astichelli 14, 36031 Dueville (VI) - Italy

Web Site: www.digitalexpert.it

Email: info@digitalexpert.it

Sistemi – Reti - Sviluppo Software ed Hardware

Progetti Speciali - Soluzioni KanBan

Formazione - Integrazioni tra Tecnologie

Sistemi di Monitoraggio - *Web Applications*

Assistenza – Sicurezza - Forensic

Telecomunicazioni - Elettrosmog

Indice

cap.1 – Premessa – Cos'e' il monitoraggio

cap.2 – I principi del monitoraggio dei sistemi

cap.3 – Un esempio pratico di monitoraggio dei sistemi

cap.4 – La visualizzazione delle informazioni

cap.5 – Allarmi, automatismi ed elaborazioni

Capitolo 1

Premessa - Cos'e' il monitoraggio

Il monitoraggio - Premessa

Il monitoraggio e' un'attivita' particolare che permette di rilevare determinati eventi che accadono all'interno di sistemi informatici.

L'azione di riconoscimento dell'evento, la sua presa in carico da parte del sistema di monitoraggio e la sua fruizione finale da parte del gestore del sistema, costituiscono gli elementi principali e cruciali del monitoraggio.

Il monitoraggio contribuisce in maniera determinante a migliorare le componenti dei sistemi, sia in sede di progettazione o sviluppo, sia in fase di utilizzo dei sistemi da parte degli utenti finali.

Le tecniche fondamentali di monitoraggio nascono nei laboratori dove vengono sviluppati i prodotti hardware o software.

Lo sviluppo del software e' di per se' stesso permeato di tecniche di monitoraggio, per cui si puo' facilmente parlare di qualcosa di fortemente insito nelle tecnologie informatiche.

Sia in quanto “componente fondamentale” dei sistemi, sia in quanto estremamente utile in fase di utilizzo dei componenti informatici, il monitoraggio ha un'importanza enorme.

Il monitoraggio - Premessa

Perche' monitorare? Vediamolo con una storiellina.

Ci sono i mondiali di calcio e sta per iniziare la mitica “finale”. Non possiamo perderla. Siamo tranquillamente seduti davanti al televisore ma ad un certo punto non vediamo piu' la partita. Che e' successo?

Analizziamo la questione:

- 1) puo' essersi spento il televisore per mancanza di corrente.
- 2) il collegamento video internazionale con lo stadio e' interrotto
- 3) la partita e' stata sospesa
- 4) non abbiamo pagato l'abbonamento alla trasmissione

L'analisi del problema si fa “guardando” determinate cose. Il televisore e' acceso? Il logo del canale televisivo e' visibile sullo schermo? Siamo sintonizzati sul canale giusto ma stanno trasmettendo altro? Appare il messaggio “La ricezione del programma e' inibita a causa della mancanza del pagamento”?

Bene, il nostro “guardare intelligente” e' equivalente ad un processo di “monitoraggio”. Un sistema di elaborazione delle rilevazioni raccolte permette di dare una chiara indicazione del problema e, se istruito adeguatamente, puo' anche elaborare la diagnosi.

Il monitoraggio - Premessa

Traduciamo in “monitoraggese” la storiellina precedente.

Attiviamo innanzitutto i seguenti sensori:

- 1) sensore di “televisore acceso”
- 2) sensore di “canale visibile”
- 3) sensore di scritta “partita pagata”
- 4) sensore di “stadio visibile”

In base alle combinazioni di sensori “verdi” o “rossi” possiamo ricostruire esattamente la situazione ed esprimere un “giudizio” corretto. Ad esempio:

- se il sensore “televisore acceso” non e' verde... manca la corrente!!
- se il sensore “canale visibile” e' verde allora... siamo sul canale giusto!!
- se il sensore “partita pagata” e' verde, siamo in regola con il pagamento!
- se il sensore “stadio visibile” e' verde, allora tutto e' a posto!

A questo punto se ancora non si vedono i calciatori in azione e' perche'... siamo nell'intervallo tra il primo e il secondo tempo!!!

Quindi la visione dei “colori” di queste quattro lampadine ci permette di esprimerci sullo stato di “fruibilita” della partita tanto desiderata o, nel caso di condizioni non previste, di esprimere delle “ipotesi” su qual e' il motivo per cui non vediamo la partita!

Il monitoraggio - Premessa

Quindi il monitoraggio e' uno “strumento” che permette da una parte di rilevare lo stato di alcuni sensori (e di dare quindi visibilita' dello stato di essi) mentre dall'altra permette anche di elaborare una diagnosi, piu' o meno accurata.

Ma, tornando all'esempio precedente, supponiamo di far “girare” i controlli con regolarita' ogni x minuti e di tener traccia dei valori di tutti i sensori nell'arco del tempo. Se la partita viene trasmessa in ritardo di dieci minuti rispetto a quanto stabilito (supponiamo che fosse prevista per le ore 21), analizzando i dati registrati, troveremo tutti i sensori costantemente in verde, eccetto quello di “stadio visibile”, il quale starebbe in rosso fino alle 21 e 10, per poi cambiare in “verde” per un'ora e mezza e ritornare infine sul rosso a partita finita...

Migliorando il tipo e la qualita' dei sensori e aumentando la frequenza dei controlli, piu' preciso sara' il processo di controllo e piu' precisa sara' quindi la capacita di “vedere” esattamente cosa e' successo e “quando”.

Inoltre, sia che si tratti di “elaborazione umana” che “da programma”, migliore sara' la possibilita' di ottenere una diagnosi accurata.

I vantaggi “immediati” e a “consuntivo” di questi sistemi di controllo sono enormi.

Il monitoraggio - Premessa

Vediamo in termini generali in cosa il monitoraggio puo' essere utile ed importante.

E' innanzitutto possibile rilevare le specifiche condizioni, registrarle e, se necessario, avvertirsi di un evento specifico “avvertire qualcuno” per un tempestivo intervento. Inoltre si possono, ad inconveniente risolto, anche “fare i conti” dello specifico problema, calcolandone la sua esatta durata.

Nel caso poi di eventi che possono essere collegati tra loro da un nesso causale, e' possibile da una parte intervenire per evitare una serie di eventi a catena e dall'altra e' possibile misurare il tempo che un determinato evento richiede per scatenarne un altro.

Ad esempio: salta la corrente e un grosso frigorifero resta privo di alimentazione. Se intervengo tempestivamente riattivando l'energia elettrica in tempi brevi, non ci saranno particolari conseguenze sul contenuto del frigo. Mentre se intervengo in notevole ritardo la temperatura del frigo salira' sopra la soglia limite e il sensore relativo mi indichera' che devo “buttare” il suo contenuto.

Infine, analizzando a posteriori i dati posso anche “apprendere” qual e' il tempo massimo di mancanza di corrente prima di dover buttare il suo contenuto.

Il monitoraggio, seppure non possa “evitare” determinati eventi (in questo caso la caduta di corrente) dall'altra mi permette di correre ai ripari evitando le conseguenze piu' gravi!

Il monitoraggio - Premessa

Quindi nel monitoraggio coesistono diverse “anime”. Vediamone alcune.

Quella del “registratore” (la “scatola nera” con la storia degli eventi per capirne la logica)

Quella del “sorvegliante” (in caso avvenga qualcosa di grave, “suonare l'allarme”)

Quella del “previsore” (per gli eventi che notoriamente scatenano altri eventi in cascata)

In sostanza il monitoraggio e' anche uno strumento di “apprendimento” di come funziona (o non funziona) un determinato sistema.

Costruendo un oculato sistema di sensori, adattandolo alla specifica realta' si puo' da una parte tenere traccia di specifici eventi (attesi o meno) e dall'altra capire come intercettare determinate condizioni “particolari”, siano esse di banale “guasto” come pure di “alterazione funzionale”.

Da questo punto di vista lo strumento di monitoraggio diventa un “partner” utilissimo di gestione e controllo di un sistema complesso e il suo ruolo di banale “sorvegliante” si arricchisce di capacita' diagnostiche, interpretative, gestionali, permettendo di tenere “il polso” delle applicazioni e servizi erogati, ma anche di identificarne i punti deboli, siano essi costantemente presenti o siano essi presenti solo in determinate occasioni.

Dal punto di vista sistemistico ma anche applicativo e' possibile far si' che tutti gli eventi significativi siano tracciati, anche dove essi non rappresentino di per se' anomalie. Questa preziosa funzione di “scatola nera” permette di analizzare ogni fase operativa.

Capitolo 2

I principi del monitoraggio dei sistemi

Il monitoraggio dei sistemi

Il monitoraggio e' una tecnica per implementare specifiche esigenze di controllo.

Prendiamo quindi in considerazione alcune tipologie “classiche” di esigenze e andiamo a vedere per ognuna di esse le tecniche utilizzabili.

Si tratta ovviamente di esempi “teorici” a scopo didattico.

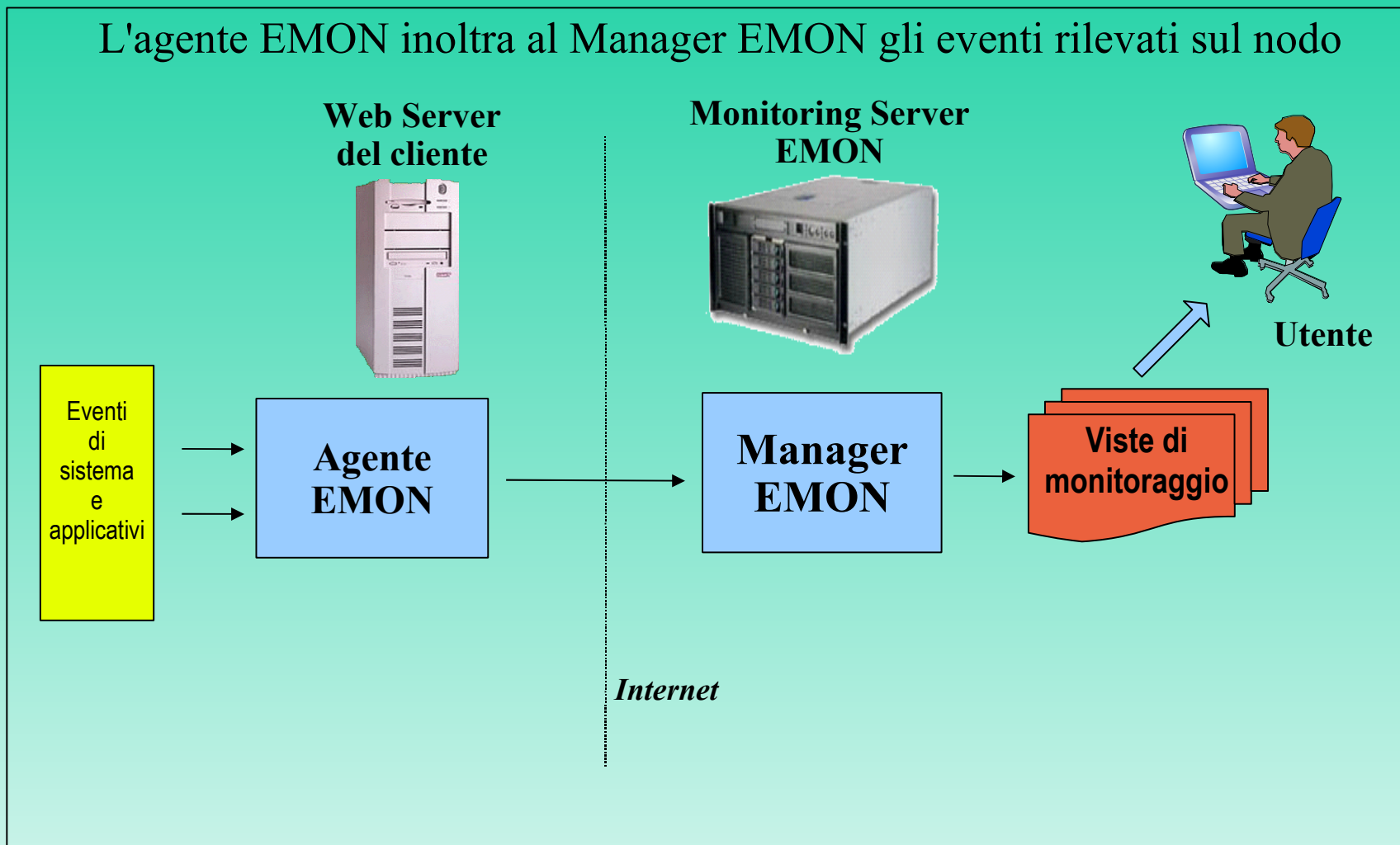
Iniziamo a prendere in considerazione prima di tutto i monitoraggi locali, quelli cioe' effettuati da un particolare programma (agente) dall'interno di uno specifico computer (nodo), con controllo di elementi locali.

Seguirà poi qualche esempio di monitoraggio “remoto” non invasivo. In questa tipologia di monitoraggio, il controllo di un nodo viene effettuato da un altro computer (chiamiamolo Manager) connesso al primo tramite una rete. Sul nodo non e' attivo alcun programma specifico di monitoraggio (da cui il “non invasivo”. Pertanto le “risposte” alle richieste del manager possono essere soddisfatte dalle sole applicazioni presenti sul nodo.

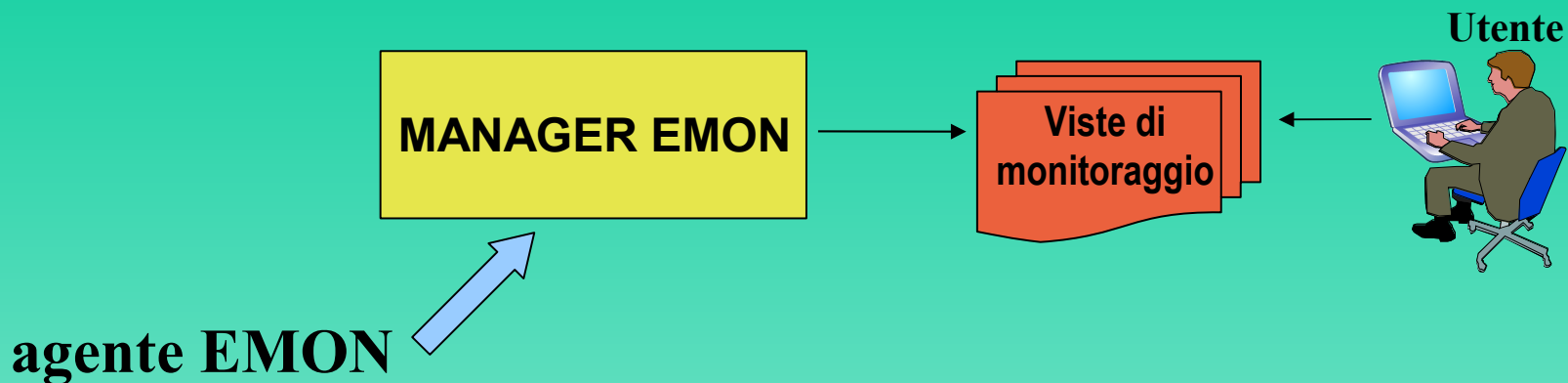
Infine darò indicazioni su tecniche di monitoraggio composite (agente + manager).

Monitoraggio locale – Schema generale

L'agente EMON inoltra al Manager EMON gli eventi rilevati sul nodo



Monitoraggio locale – esempio



Compiti dell'agente Emon su WEB1

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	inetinfo.exe
applicazione attiva	mysql.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

Compiti dell'agente Emon su WEB2

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	inetinfo.exe
applicazione attiva	mysql.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

Monitoraggio locale - Sistema attivo

L'esigenza e' di tenere sotto controllo (e registrare) lo stato di “**sistema attivo**” di un determinato computer. Non e' un controllo inutile, anzi, vedremo in altre parti l'utilita' estrema di questo controllo.

La logica di implementazione di questo controllo e' la seguente:

- 1) creo un programma che registri “da qualche parte” ogni x tempo, la data e ora
- 2) faccio in modo che il sistema attivi questo programma alla partenza

Otterro' un insieme di dati di questo tipo (supponiamo la cadenza di un'ora):

```
.....  
2006/06/04 - 14.00 - sistema vivo!  
2006/06/04 - 15.00 - sistema vivo!  
2006/06/04 - 16.00 - sistema vivo!  
2006/06/04 - 17.00 - sistema vivo!  
2006/06/04 - 18.00 - sistema vivo!  
2006/06/04 - 19.00 - sistema vivo!  
2006/06/04 - 20.00 - sistema vivo!  
2006/06/04 - 21.00 - sistema vivo!  
.....
```

Nell'esempio specifico, alle 17 e alle 18 il programma non ha operato, visto che mancano le registrazioni relative... quindi in quella fascia oraria, o il computer era fermo oppure il programma non era attivo!

Monitoraggio locale - Applicazione attiva

Il controllo di “**applicazione attiva**” e' uno dei monitoraggi in teoria piu' semplice. La logica di implementazione e' basata sulla disponibilita' da parte del sistema operativo, di una funzione che permetta di ricavare il nome dei vari programmi in esecuzione sul computer. Banalmente l'equivalente del “task manager” di windows.

L'applicazione di controllo, dato il nome della applicazione da controllare (“prova.exe”, nell'esempio) deve:

- 1) periodicamente leggere la lista di applicazioni attive nel sistema
- 2) cercare nella lista dei programmi attivi quello interessato, registrandone l'esistenza o meno (stato)

L'applicazione di controllo, come in altri casi, deve essere sempre attiva ed operare in continuazione.

Supponendo che l'applicazione venga fermata dalle 16 alle 18, se ne otterra' un tracciato di questo tipo:

```
.....  
2006/06/04 - 14.00 - applicazione "prova.exe" funzionante!  
2006/06/04 - 15.00 - applicazione "prova.exe" funzionante!  
2006/06/04 - 16.00 - applicazione "prova.exe" FERMA!  
2006/06/04 - 17.00 - applicazione "prova.exe" FERMA!  
2006/06/04 - 18.00 - applicazione "prova.exe" FERMA!  
2006/06/04 - 19.00 - applicazione "prova.exe" funzionante!  
2006/06/04 - 20.00 - applicazione "prova.exe" funzionante!  
.....
```

Monitoraggio locale - Risorsa operativa

Il monitoraggio di “**Risorsa sufficiente**” e' un tipo di controllo molto semplice, in generale. La logica di implementazione e' basata sulla disponibilita' da parte del sistema operativo, di una serie di funzioni che permettano di ricavare dimensione e percentuale di utilizzo di una risorsa. Ad esempio nel caso di un disco, il sistema operativo fornisce una funzione che mostra la dimensione del disco e la sua percentuale di spazio utilizzata di una specifica partizione. Cosa analoga per quel che riguarda la memoria RAM o altri “oggetti”.

Nel caso il sistema operativo non fornisca direttamente la funzione necessaria, essa si puo' scrivere appositamente e “inserire” nell'agente del nodo da gestire.

L'applicazione di monitoraggio, dati il tipo, il nome della risorsa da controllare e il valore di riferimento, esegue ad esempio la lettura dello spazio disponibile su disco e, nel caso il valore sia superiore alla soglia, prende nota del fatto che il disco e' occupato **sopra** il livello predefinito (50% nell'esempio), producendo una registrazione simile (considerando che venga riempito oltre il limite dalle 16 alle 18):

```
.....  
2006/06/04 - 14.00 - risorsa disco C: normale!  
2006/06/04 - 15.00 - risorsa disco C: normale!  
2006/06/04 - 16.00 - risorsa disco C: sopra la soglia del 50%!  
2006/06/04 - 17.00 - risorsa disco C: sopra la soglia del 50%!  
2006/06/04 - 18.00 - risorsa disco C: sopra la soglia del 50%!  
2006/06/04 - 19.00 - risorsa disco C: normale!  
2006/06/04 - 20.00 - risorsa disco C: normale!  
.....
```

Monitoraggio locale - Lettura di logfile

Il monitoraggio di un file di log e' un'operazione teoricamente semplice. Partiamo dal presupposto che vogliamo intercettare un evento che un programma operante nel sistema va a scrivere in un file testuale (il file di log).

La logica e' la seguente: l'applicazione di monitoraggio, sempre attiva, esegue con periodicit  definita la lettura di un file, alla ricerca di un messaggio identificabile tramite una regola precisa.

Supponiamo che l'applicazione da controllare registri sul file una serie di informazioni, tra cui l'accesso di un utente, scrivendo sul file la seguente scritta "ACCESSO UTENTE xxx", dove 'xxx' sta per l'identificativo dell'utente.

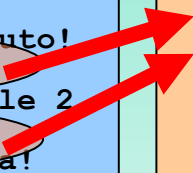
L'applicazione di monitoraggio registrera' quindi l'evento desiderato (l'accesso di un utente), intercettando la sola riga presente nel file di log e scartando le altre.

FILE DI LOG DELL'APPLICAZIONE MONITORATA

```
.....  
2006/06/04 14.00 - disconnesso utente pluto!  
2006/06/04 15.00 - ACCESSO UTENTE PIPPO  
2006/06/04 16.00 - spedizione dati filiale 2  
2006/06/04 19.00 - ACCESSO UTENTE PLUTO  
2006/06/04 20.00 - elaborazione terminata!  
.....
```

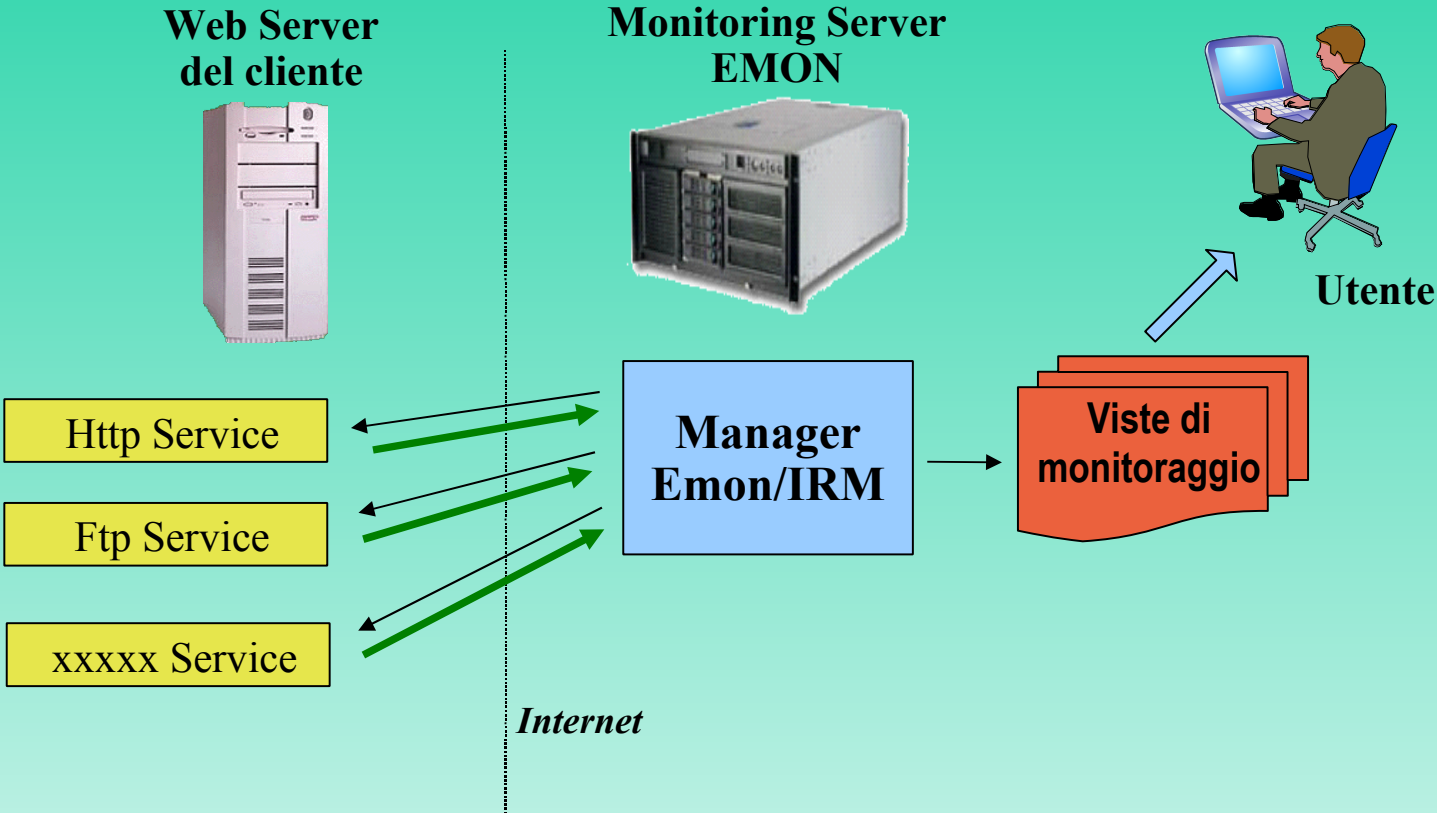
REGISTRAZIONE DEL MONITORAGGIO

```
.....  
2006/06/04 15.00 - ACCESSO di PIPPO  
2006/06/04 19.00 - ACCESSO di PLUTO  
.....
```

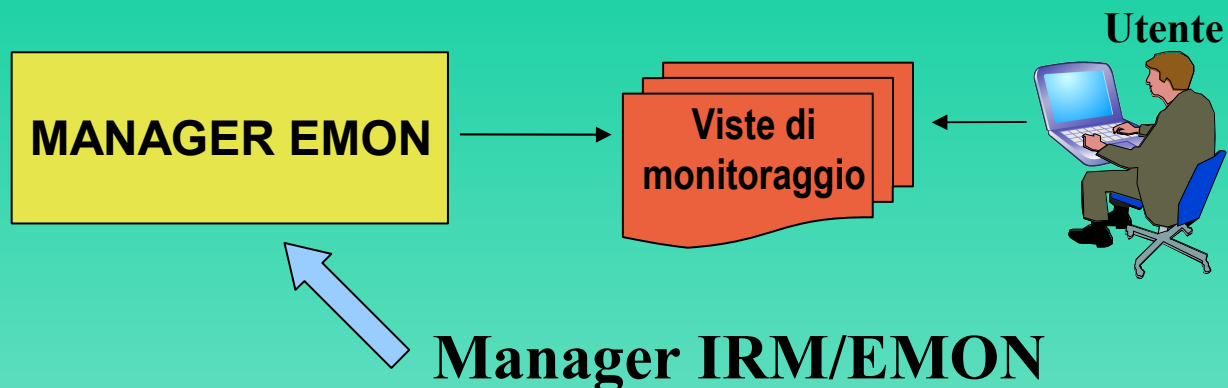


Monitoraggio remoto – Schema generale

Il manager Emon/IRM verifica remotamente la funzionalita' di specifici servizi.



Monitoraggio remoto – esempio



WEB1 Compiti del Manager Emon/IRM

<u>controllo</u>	<u>valore</u>
stato porta 80 (HTTP)	SI
stato porta 21 (FTP)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

WEB2 Compiti del Manager Emon/IRM

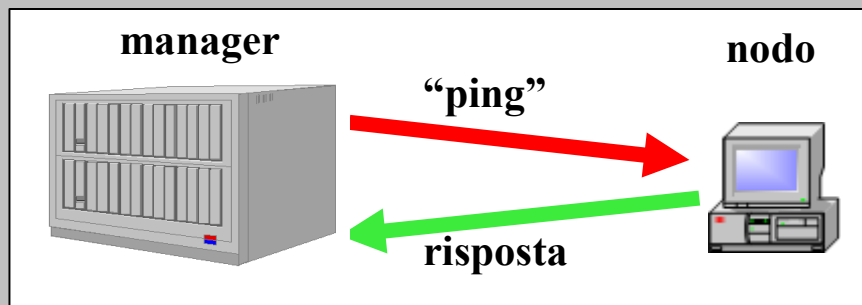
<u>controllo</u>	<u>valore</u>
stato porta 80 (HTTP)	SI
stato porta 21 (FTP)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

Monitoraggio remoto – Visibilita' del nodo

Lo stato di visibilita' di un nodo richiede che sullo stesso sia attivo il software di base di connessione ad una rete, il quale, se interrogato dall'esterno (tramite il “ping”), risponde con un “sono vivo”. La logica di implementazione del programma di controllo attivo sul manager e' grosso modo la seguente:

- 1) il programma “manager” lancia a cadenza regolare una “richiesta” verso il nodo
- 2) il nodo controllato “risponde” (ovviamente se raggiungibile e se in grado di rispondere)
- 3) il programma di controllo riceve la risposta e la registra.

Vediamo l'esito nel caso di un nodo spento (o non connesso alla rete comune al manager) dalle 16 alle 18.



```
2006/06/04 - 14.00 - ping: il nodo 192.168.1.1 e' raggiungibile
2006/06/04 - 15.00 - ping: il nodo 192.168.1.1 e' raggiungibile
2006/06/04 - 16.00 - ping: il nodo 192.168.1.1 NON E' RAGGIUNGIBILE
2006/06/04 - 17.00 - ping: il nodo 192.168.1.1 NON E' RAGGIUNGIBILE
2006/06/04 - 18.00 - ping: il nodo 192.168.1.1 NON E' RAGGIUNGIBILE
2006/06/04 - 19.00 - ping: il nodo 192.168.1.1 e' raggiungibile
```

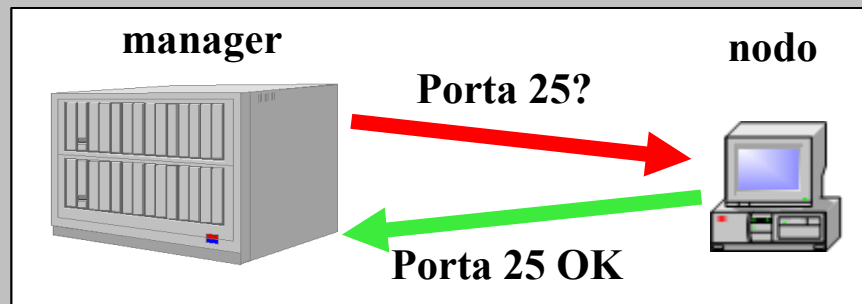
Monitoraggio Remoto – stato di porta TCP

Nel caso di un controllo di una porta TCP/IP il manager effettua una richiesta di connessione ad uno specifico port, attendendo una qualche risposta.

La logica di implementazione del programma e' analoga a quella del “ping” solo che la tipologia di richiesta al nodo e' diversa e comporta, sul nodo, l'esistenza e attivita' di una applicazione specifica pronta a dialogare su quello specifico indirizzo di porta:

- 1) il programma “manager” effettua una richiesta ad una specifica porta del nodo
- 2) il nodo controllato “risponde” (nel caso l'applicazione specifica per la porta sia attiva)
- 3) Il programma di controllo riceve la risposta e la registra.

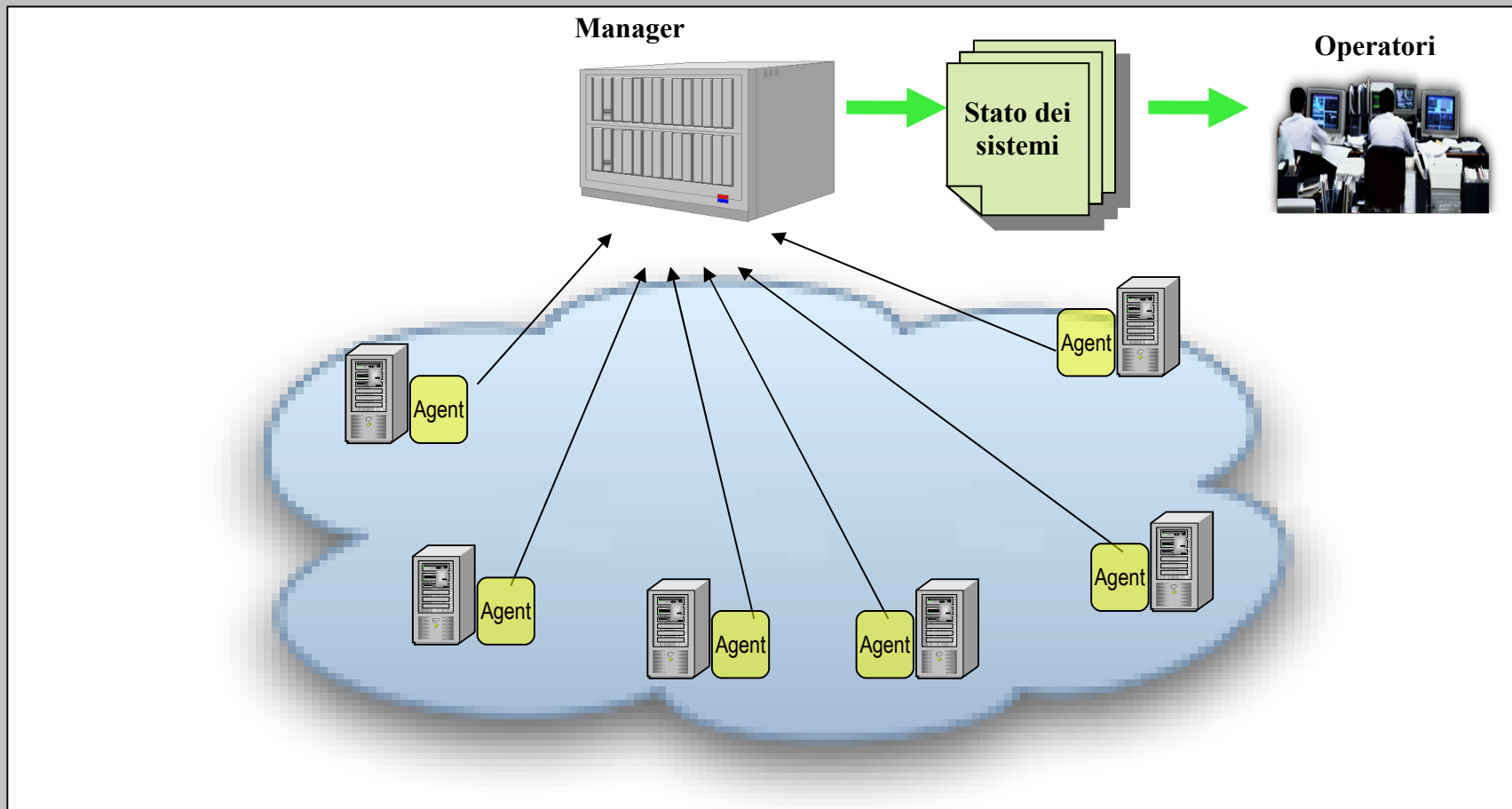
Ecco l'esito del monitoraggio su un nodo con la porta 25 spenta dalle 16 alle 18.



```
2006/06/04 - 14.00 - portcheck: porta 192.168.1.1:25 raggiungibile
2006/06/04 - 15.00 - portcheck: porta 192.168.1.1:25 raggiungibile
2006/06/04 - 16.00 - portcheck: porta 192.168.1.1:25 IRRAGGIUNGIBILE
2006/06/04 - 17.00 - portcheck: porta 192.168.1.1:25 IRRAGGIUNGIBILE
2006/06/04 - 18.00 - portcheck: porta 192.168.1.1:25 IRRAGGIUNGIBILE
2006/06/04 - 19.00 - portcheck: porta 192.168.1.1:25 raggiungibile
```

Monitoraggio composito – Schema base

La tipologia ideale di controllo e' quella rappresentata dal monitoraggio composito. In questo caso ogni nodo da controllare ha un agente installato che comunica con il manager. Vediamo in dettaglio una piccola rete con monitoraggio composito.



Monitoraggio composito – Schema base

La capacita' di raccolta di dati dell'agente installato sul nodo da controllare, unita alle potenzialita' di monitoraggio “dall'esterno” rese possibili dal manager, permettono di ottenere i migliori risultati.

Il sistema di controllo e' “fuori” dall'oggetto controllato, per cui si risolve innanzitutto il problema fondamentale di poter avere qualche informazione sul nodo interessato anche quando esso non e' piu' raggiungibile. Le informazioni sono salvate e consultabili da un'altra parte!

Il fatto che il programma di controllo sia “da altre parti” rende possibile anche generare un “allarme” o compiere qualunque altra azione con affidabilita', dato che tale compito non e' in carico a un programma che gira sul nodo monitorato, magari in cattive condizioni, privo di collegamento o addirittura spento.

Tramite il manager esterno e' possibile elaborare le informazioni in modo piu' raffinato che sul singolo nodo. Ad esempio e' possibile effettuare considerazioni “collettive”, ad esempio correlando stati di piu' nodi e' possibile riconoscere condizioni particolari. La correlazione di stati permette ad esempio di riconoscere condizioni comunicative “di gruppo” (un gruppo di nodi irraggiungibili appartenenti alla stessa area significa “problema di rete” e non una serie di singoli problemi separati).

Monitoraggio composito – Schema base

La somma di “rilevazioni locali” e di “rilevazioni remote” permette al manager una piu' ricca e articolata “conoscenza” degli stati dei nodi monitorati.

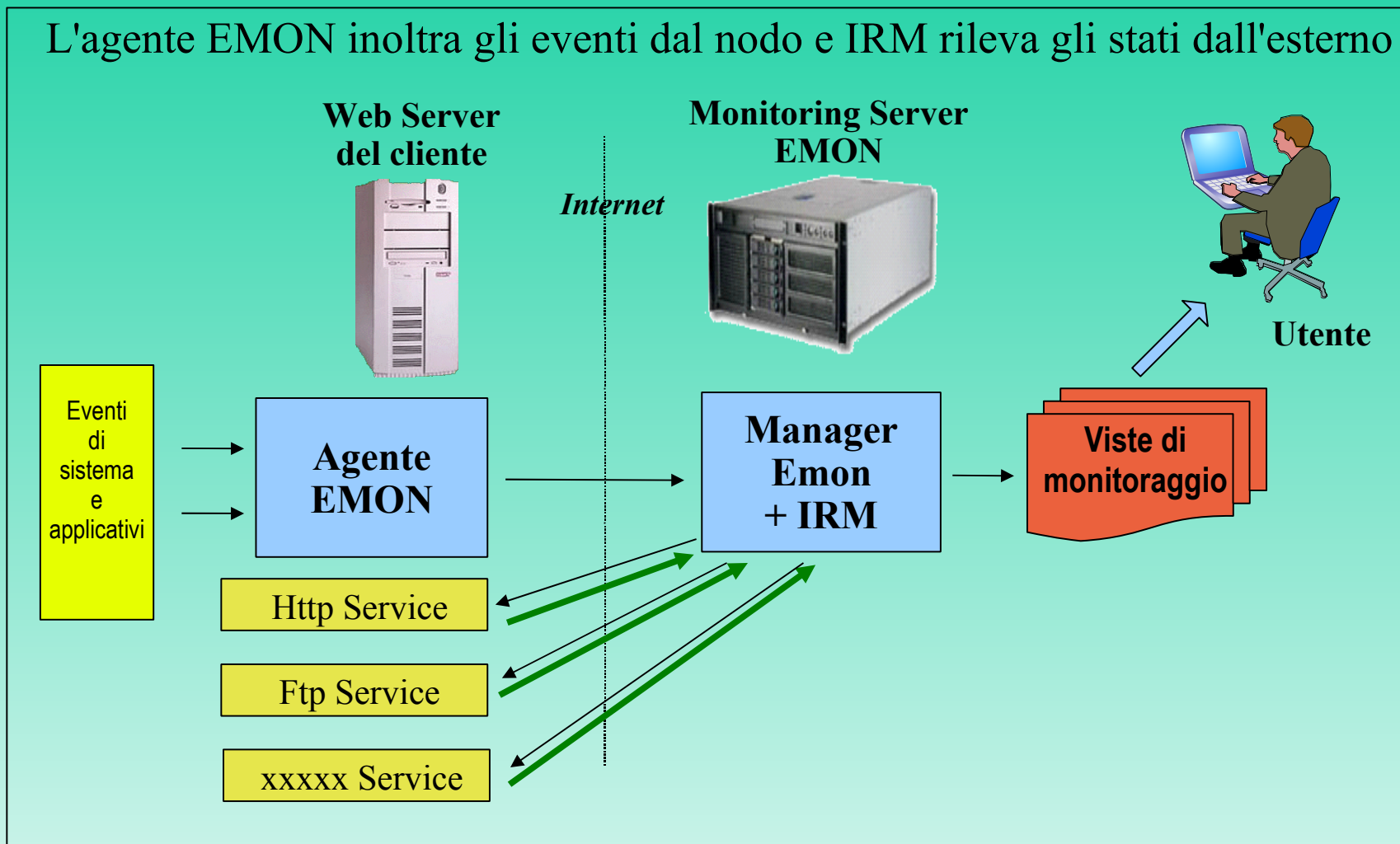
La storicizzazione dei dati degli eventi di tutti i nodi, effettuata sul manager, permette, anche, in assenza momentanea di contatto con uno specifico nodo, di “rivedere” cosa e' successo e quando.

Il monitoraggio composito, ovviamente, richiede una grande affidabilita' del manager.

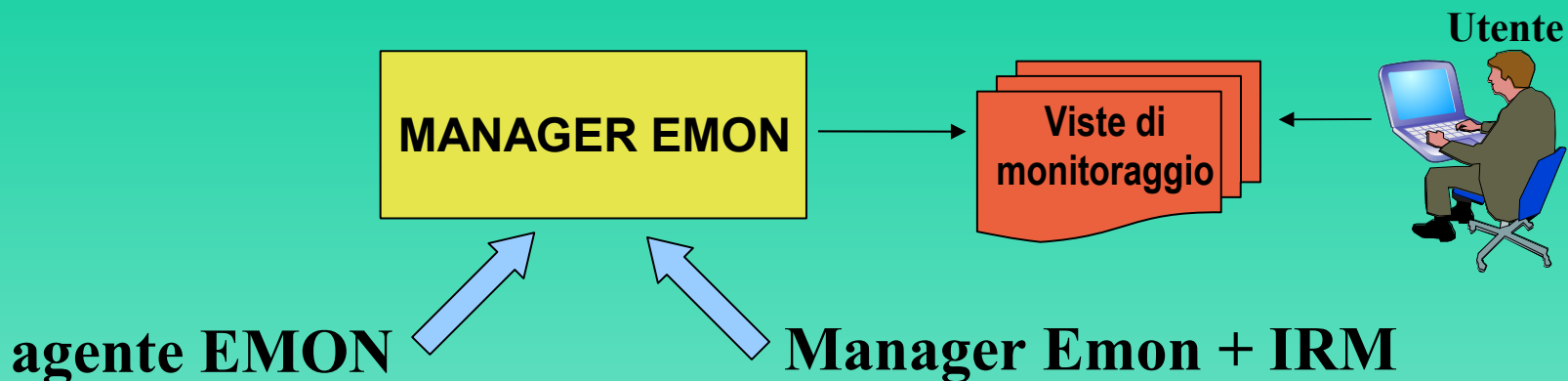


Monitoraggio composito – Schema generale

L'agente EMON inoltra gli eventi dal nodo e IRM rileva gli stati dall'esterno



Monitoraggio composito – esempio



Compiti dell'agente Emon su WEB1

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	inetinfo.exe
applicazione attiva	mysql.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

Compiti del Manager Emon/IRM su WEB1

<u>controllo</u>	<u>valore</u>
stato porta 80 (HTTP)	SI
stato porta 21 (FTP)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

Compiti dell'agente Emon su WEB2

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	inetinfo.exe
applicazione attiva	mysql.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

Compiti del Manager Emon/IRM su WEB2

<u>controllo</u>	<u>valore</u>
stato porta 80 (HTTP)	SI
stato porta 21 (FTP)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

Capitolo 3

*Un esempio pratico di
monitoraggio dei sistemi*

Il monitoraggio – un esempio pratico

Vediamo ora un caso “reale” per quanto sempre in forma semplificata e “didattica”. Il nostro “cliente” e' una piccola azienda con due server “importanti” situati nella rete interna aziendale:

- 1) POSTA1 - server di posta (protocolli POP3,SMTP)
- 2) WEB1 - web server con il sito aziendale (protocolli HTTP, FTP)

Sul server di posta si deve controllare se “rispondono” le seguenti porte: 25 (SMTP) e 110 (POP3). Il servizio WEB si controlla sulle porte 80 (HTTP) e 21 (FTP).

Si tratta di due server windows con dischi da 60 Gbytes e 512 Mbytes di ram.

In base alle indicazioni del cliente, tra gli allarmi da attivare ce ne sono due specifici da attivare localmente relativamente a “spazio disco” (avvertire se lo spazio occupato sale oltre i 59 gb) e “memoria RAM” (segnalare occupazione superiore a 448 mb).

Per Windows, i nomi delle applicazioni da controllare sono (sto semplificando):

- 1) il servizio di posta viene erogato dal programma “exchange.exe”
- 2) il servizio Web viene erogato dal programma “inetinfo.exe”

Questa analisi dettagliata degli “oggetti” da monitorare e' ovviamente essenziale!

Il monitoraggio – un esempio pratico

Vediamo ora le impostazioni per i due agenti installati su POSTA1 e su WEB1, oltre alle impostazioni per il manager:

AGENTI

Agente su server POSTA1

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	exchange.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

Agente su server WEB1

<u>controllo</u>	<u>valore</u>
sistema vivo	SI
applicazione attiva	inetinfo.exe
risorsa disco	<=59 gb
risorsa RAM	<448 mb

MANAGER

Manager verso server POSTA1

<u>controllo</u>	<u>valore</u>
stato porta 25 (SMTP)	SI
stato porta 110 (POP3)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

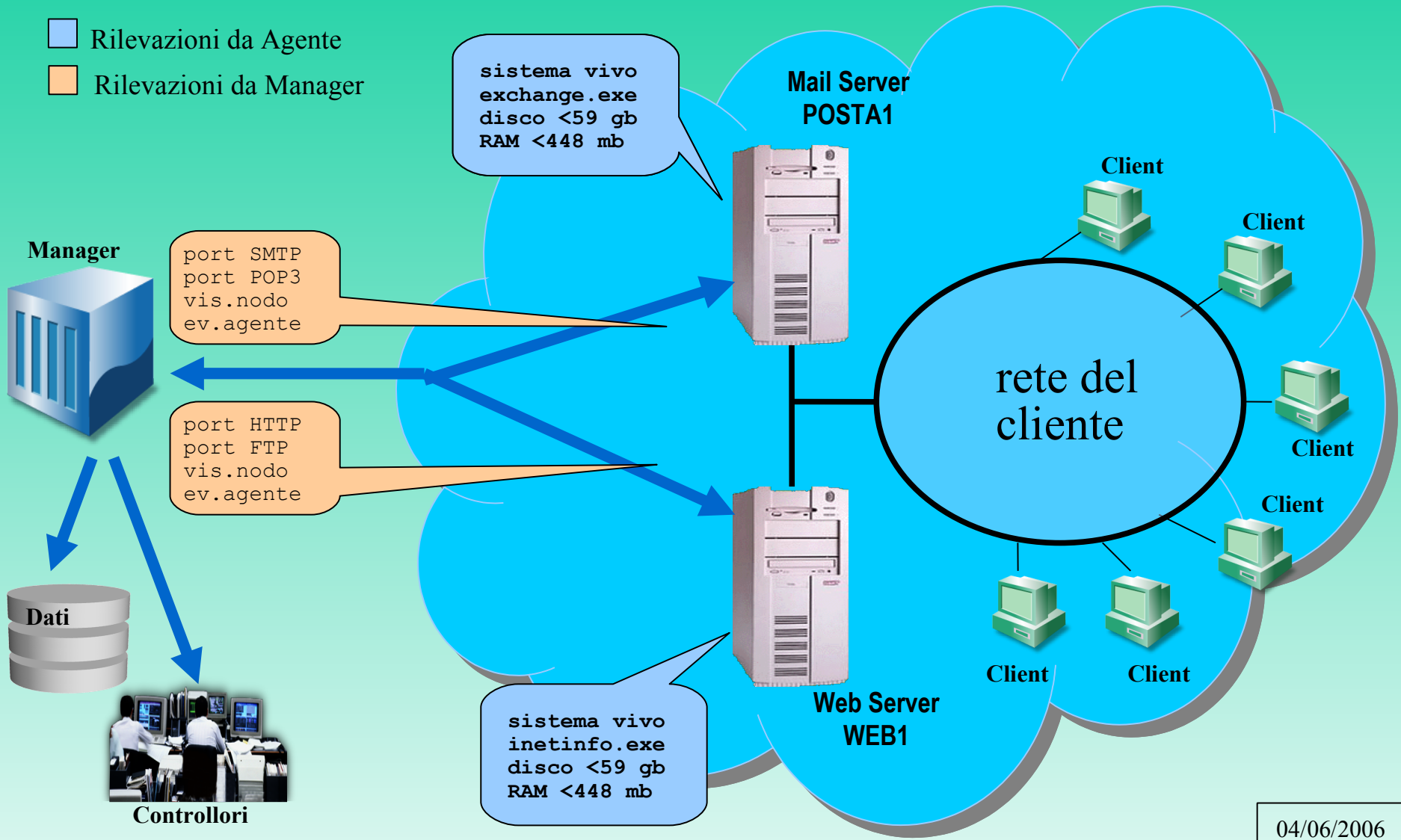
Manager verso server WEB1

<u>controllo</u>	<u>valore</u>
stato porta 80 (HTTP)	SI
stato porta 21 (FTP)	SI
visibilita' nodo	SI
raccolta eventi agente	SI

Il monitoraggio – un esempio pratico

Vediamo ora il sistema di monitoraggio nel suo complesso:

- Rilevazioni da Agente
- Rilevazioni da Manager



Capitolo 4

La visualizzazione delle informazioni

Monitoraggio – Visualizzazione delle informazioni

Il sistema di monitoraggio elabora e storicizza stati ed eventi raccolti dagli agenti o dal manager stesso. La prima importante esigenza da soddisfare e' quella della visualizzazione di queste informazioni.

Possiamo innanzi tutto citare due tipologie fondamentali di “viste”: la vista “storica” (un elenco dettagliato degli eventi accaduti recentemente), e la vista di “stato” (lo stato dei vari elementi da controllare visualizzato in tempo reale).

Naturalmente poi la visualizzazione “utile” puo' essere concepita in estrema liberta' e adatta a soddisfare le necessita' reali dell'utente.

Ad esempio si possono creare viste complesse contenenti sia dati di monitoraggio (e sue eventuali elaborazioni) sia dati provenienti dall'esterno del monitoraggio (ad esempio indicazioni sulle azioni da intraprendere, riferimenti tecnici e operativi, elementi per “disegnare” gli oggetti nel modo corretto, informazioni di gestione degli interventi, riferimenti telefonici, etc).

Un funzionale “cruscotto” sul quale poter concentrare tutte le informazioni, le operazioni e gli interventi.

Da questo punto di vista, ovviamente, l'applicazione di monitoraggio fa' “un salto in piu” e diventa il fulcro, la “sala regia”, del sistema informativo del nostro cliente.

Monitoraggio – La vista “storica” degli eventi

Un modo completamente diverso di usufruire delle rilevazioni effettuate da un sistema di monitoraggio e' quello della vista “storica”. Questa vista non visualizza lo “stato” del sistema (anche se permette comunque di averne la percezione) ma elenca l'andamento degli eventi, permettendo di collocarli temporalmente.

Gli eventi sono ordinati in ordine di tempo (i piu' recenti in alto, i meno recenti in basso) e ogni evento viene “colorato” a seconda del tipo di evento (“condizione di errore” o “condizione corretta”).

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista “storica” - dettaglio 1

Evento n.1 - dalle 09:07 alle 13:07 – nodo POSTA1

Alle 09:07 la memoria RAM di POSTA1 viene occupata oltre la soglia di 448 mbytes. Il sistema si trova a lavorare con un margine “basso” di memoria disponibile. Si tratta di una condizione potenzialmente pericolosa. La condizione viene risolta alle 13:07, quando l'occupazione scende sotto il limite.

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista “storica” - dettaglio 2

Evento n.2 - dalle 12:36 alle 12:39 – nodi POSTA1 e WEB1

Alle ore 12:36 il manager di monitoraggio non riesce a contattare entrambi i nodi. Probabilmente e' caduta la connessione tra il manager e la rete del cliente, visto che l'evento e' avvenuto contemporaneamente su due nodi diversi.

Si tratta di una condizione grave, anche se di breve durata (3 minuti).

La condizione viene risolta alle 12:39, quando la comunicazione e' ristabilita.

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista “storica” - dettaglio 3

Evento n.3 - dalle 13:15 alle 13:34 – nodo POSTA1

Alle 13:15 la memoria RAM di POSTA1 viene occupata oltre la soglia di 448 mbytes. Il sistema si trova a lavorare con un margine “basso” di memoria disponibile. Si tratta di una condizione potenzialmente pericolosa. La condizione viene risolta alle 13:34, quando l'occupazione scende sotto il limite.

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista “storica” - dettaglio 4

Evento n.4 - dalle 13:21 alle ??:?? – nodo WEB1 (evento in corso)

Alle 13:21 il servizio FTP del nodo WEB1 e' caduto.

Da quel momento non e' possibile utilizzare FTP fino a scomparsa dell'anomalia.

Si tratta di una condizione grave, dato che nessun trasferimento file potra' avvenire.

La condizione non e' stata risolta.

(*tenere presente questo evento: concorre a valorizzare l'oggetto nella vista di “stato”)

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb



Monitoraggio – La vista “storica” - dettaglio 5

Evento n.5 - dalle 14:07 alle 14:26 – nodo POSTA1

Alle 14:07 la memoria RAM di POSTA1 viene occupata oltre la soglia di 448 mbytes. Il sistema si trova a lavorare con un margine “basso” di memoria disponibile. Si tratta di una condizione potenzialmente pericolosa. La condizione viene risolta alle 14:26, quando l'occupazione scende sotto il limite.

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista “storica” - dettaglio 6

Evento n.6 - dalle 14:53 alle ??:?? – nodo POSTA1 (evento in corso)

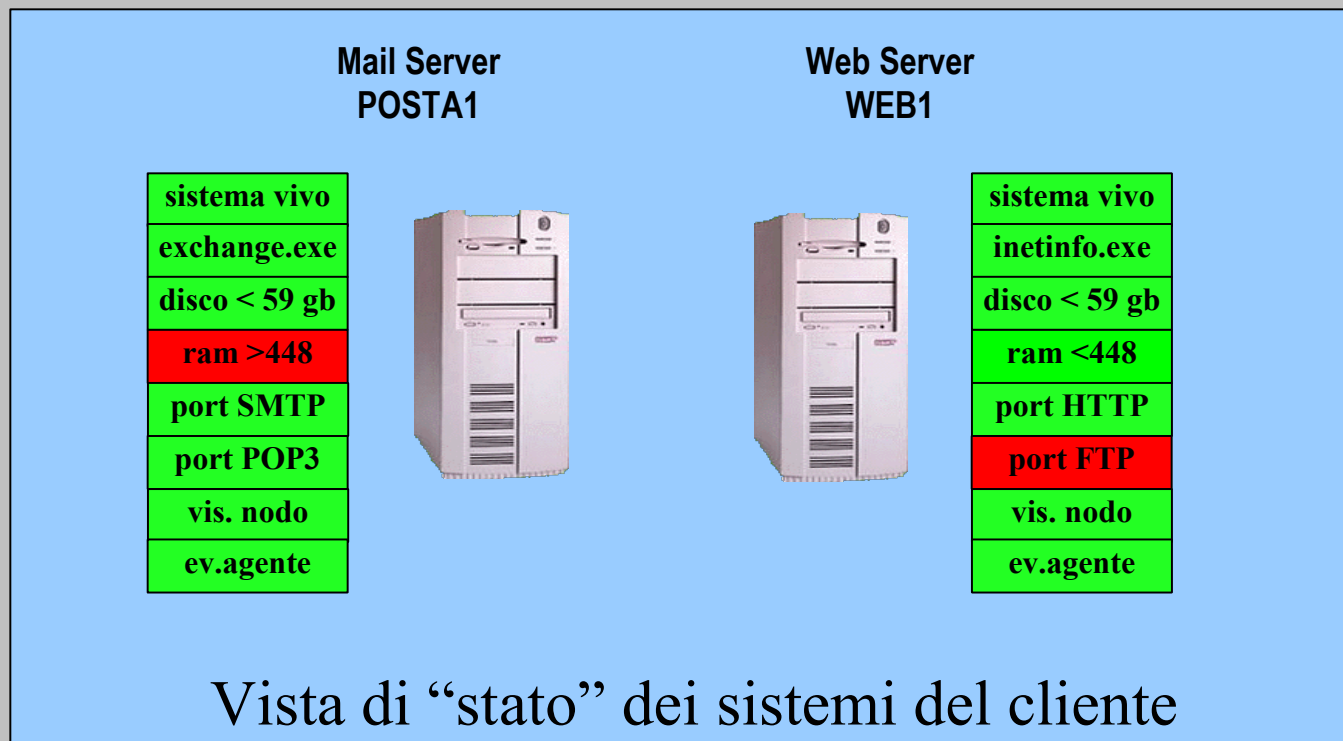
Alle 14:53 la memoria RAM di POSTA1 viene occupata oltre la soglia di 448 mbytes. Il sistema si trova a lavorare con un margine “basso” di memoria disponibile. Si tratta di una condizione potenzialmente pericolosa. La condizione non e' stata risolta.

(*tenere presente questo evento: concorre a valorizzare l'oggetto nella vista di “stato”)

1	Date	Time	St	node	type	event
2	04/06/06	14.53.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
3	04/06/06	14.26.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
4	04/06/06	14.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
5	04/06/06	13.34.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
6	04/06/06	13.21.00	KO	WEB1	service	Il servizio FTP e' caduto
7	04/06/06	13.15.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb
8	04/06/06	13.07.00	OK	POSTA1	resource	La memoria RAM occupata e' inferiore a 448 mb
9	04/06/06	12.39.00	OK	WEB1	network	La visibilita' del nodo e' ripristinata
10	04/06/06	12.39.00	OK	POSTA1	network	La visibilita' del nodo e' ripristinata
11	04/06/06	12.36.00	KO	WEB1	network	La visibilita' del nodo e' interrotta
12	04/06/06	12.36.00	KO	POSTA1	network	La visibilita' del nodo e' interrotta
13	04/06/06	09.07.00	KO	POSTA1	resource	La memoria RAM occupata e' maggiore di 448 mb

Monitoraggio – La vista di “stato” degli oggetti

Ecco la vista di “stato” della rete del nostro cliente. Contiene due “sensori” in allarme. Il primo e' nel server **Posta1** (RAM occupata oltre la soglia). Il secondo e' nel server **Web1** (servizio FTP non attivo). E' l'esito di quanto descritto nella vista “storica”.



Capitolo 5

Elaborazioni, allarmi e automatismi

Monitoraggio – Allarmi, automatismi ed elaborazioni

ALLARMI

In prima battuta da un sistema di monitoraggio ci si aspetta che esegua (in modo sofisticato ed affidabile, certo) il compito “semplice” di eseguire i controlli richiesti e di visualizzare le informazioni relative, nella forma migliore per l'utente del sistema.

L'utente di un sistema così strutturato, dopo breve tempo, sentirà fortemente l'esigenza di aggiungere alcune funzionalità importanti.

Partiamo innanzitutto da una constatazione: può sorgere la necessità di non poter mantenere una persona davanti alla console in perenne attesa che “avvenga qualcosa”. Si istruisce quindi il sistema di monitoraggio ad eseguire, a fronte di un evento che abbia il grado di gravità sufficiente, un'azione di “chiamata” dell'operatore. L'azione di allarme può essere di vario tipo (e le tecnologie moderne ci danno una mano).

L'allarme può essere fondamentalmente di due tipi: “volatile” (cioè che se non viene percepito dall'operatore per un qualche motivo viene “perso”) o “non volatile” o “permanente”, cioè che se l'operatore è impossibilitato a vederlo nel momento in cui viene generato, può anche essere percepito in momenti successivi.

Monitoraggio – Allarmi, automatismi ed elaborazioni

ALLARMI VOLATILI

Iniziamo con il classico allarme “volatile”, cioè l'emissione (magari combinata) di una segnalazione “ottica” o “acustica” (un “lampeggio” consistente prodotto sul monitor o un forte suono emesso da un altoparlante) nel luogo dove normalmente è posizionato l'utente responsabile dei controlli del sistema.

Analogamente l'allarme può anche essere banalmente costituito da una indicazione “evidente” sulla console, indicazione sempre “non permanente” e che per vari motivi possa essere prima o poi rimossa (pensiamo ad esempio a un semaforo la cui luce passi dal verde al rosso e poi dal rosso al verde...).

Monitoraggio – Allarmi, automatismi ed elaborazioni

ALLARMI NON VOLATILI

Un primo esempio di allarme “non volatile” puo' essere costituito anch'esso da un meccanismo audiovisivo simile, ma per essere “non volatile” e per essere sicuramente recepito, deve essere generato in continuazione e interrompersi non automaticamente solo dopo che l'operatore ha “recepito” il messaggio.

Un altro esempio di allarme “non volatile” puo' essere costituito da un “paging”, cioe' una segnalazione inviata ad esempio via email o sms, un messaggio vocale lasciato in una casella vocale, etc.

Monitoraggio – Allarmi, automatismi ed elaborazioni

STRATEGIE DI ALLARME

L'importante e' identificare correttamente la modalita' di allarme, in modo adatto a coprire le esigenze di controllo e di intervento necessarie.

Quindi un evento che segnala una anomalia che potrebbe portare, in mancanza di rapidi interventi, ad un problema grave, va segnalata in modo “forte” (e non certo solo nel senso di “volume”) e nella modalita' migliore ad essere recepito con sicurezza e tempestivita'.

Anche ricorrendo all'uso di piu' strumenti di avvertimento contemporaneamente, se necessario.

Inoltre e' anche importante far si' che in situazioni particolari (quelle che si risolvono senza intervento dell'operatore) l'indicazione di allarme “urgente” venga trattata adeguatamente (esempio: spegnendo la sirena se il problema e' ormai risolto!!) andando peraltro a registrare l'evento tra i “fatti importanti” accaduti.

Monitoraggio – Allarmi, automatismi ed elaborazioni

AUTOMATISMI

Lo strumento di monitoraggio e' un ausilio a identificare determinate anomalie.

L'obbiettivo ovviamente non e' solo quello di “osservare” passivamente lo svolgersi degli eventi, ma di poter anzi scatenare delle azioni correttive.

Supponiamo (facendo riferimento all'esempio pratico visto precedentemente) che il programma di posta (exchange.exe) abbia avuto un problema e abbia cessato di funzionare. Il monitoraggio rileva l'anomalia e la segnala all'operatore.

L'operatore effettua una certa serie di azioni e il problema viene risolto. Il sistema di monitoraggio recepisce il corretto funzionamento del programma di posta e visualizza, per quel componente, lo stato di “ok”.

Se le azioni intraprese dall'operatore sono “semplici” (ad esempio una serie di banali comandi) e' possibile che il sistema di monitoraggio le effettui “automaticamente” (previa o meno supervisione dell'utente).

In questo caso quindi il sistema di monitoraggio funziona da “operatore automatico” e dal punto di vista dell'anomalia e' possibile ridurre i tempi di “fermo reale”, oltre che ovviamente avere questo tipo di beneficio anche in assenza di un operatore (esempio: di notte o in fasce orarie non coperte).

Ovviamente la cosa puo' essere fatta quando l'insieme di azioni correttive e' di esito “certo” e incruento. Inoltre il sistema deve “dosare” l'intervento in modo da evitare che una determinata segnalazione produca una serie “senza fine” di inutili sequenze di comandi.

Monitoraggio – Allarmi, automatismi ed elaborazioni

ELABORAZIONI

Vediamo ora alcuni contributi particolari che un buon strumento di monitoraggio puo' fornire.

Innanzitutto la rilevazione e storicizzazione degli eventi puo' permettere l'importantissimo processo di “calcolo” della durata e dell'impatto di una specifica anomalia. Cio' e' importantissimo, sia dal punto di vista strettamente tecnico che dal punto di vista dell'elaborazione dei livelli di servizio. La contrattualizzazione di un servizio erogato attraverso piattaforme informatiche e' sempre piu' spesso legata a specifici parametri di disponibilita' del servizio. Pertanto e' necessario che lo strumento di monitoraggio sia in grado di effettuare misure ed elaborazioni su questo fronte.

Inoltre elaborazioni apposite possono “consultare” l'archivio storico degli eventi e riconoscere specifiche “periodicita” o comunque “ripetizioni” frequenti di determinati eventi, permettendo l'identificazione di un “elemento critico” del sistema.

Interfacciando componenti applicative con il sistema di monitoraggio e' pure possibile tenere traccia di eventi previsti o di obbligatoria esecuzione. In questo modo si possono effettuare sofisticate “traces” applicative o tenere sotto controllo e monitoraggio i flussi di salvataggio o replica dei dati, trasferimenti di dati da e per altri sistemi.

Ultimo aspetto da non sottovalutare, la possibilita' di “maneggiare” gli eventi combinando piu' rilevazioni contemporanee per “tradurre” una serie di complicati messaggi in una semplice sintesi “comprensibile”.

FINE DEL DOCUMENTO

DigitalExpert

Consulenze Informatiche
di Carloalberto Sartor
via Astichelli 14, 36031 Dueville (VI) - Italy

Web Site: www.digitalexpert.it

Email: info@digitalexpert.it

Sistemi – Reti - Sviluppo Software ed Hardware
Progetti Speciali - Soluzioni KanBan
Formazione - Integrazioni tra Tecnologie
Sistemi di Monitoraggio - Web Applications
Assistenza – Sicurezza - Forensic
Telecomunicazioni - Elettrosmog