

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

E-Mon – Premessa

Alcune considerazioni

- Non esiste il “prodotto perfetto”
- Le esigenze di monitoraggio dipendono da vari elementi slegati spesso dagli aspetti tecnologici
- Il contesto da monitorare può essere estremamente eterogeneo
- I prodotti “standard” tendono ad avere costi, complessità e limitazioni d'uso spesso inaccettabili, ad esempio con sistemi datati
- “Il prodotto X funziona bene ma non rileva l'evento y...”
- “Voglio una cosa facile, una lampadina accesa o spenta...”

E-Mon – Filosofia

Le filosofie di sviluppo Digitalexpert per il monitoraggio

Definire le varie tipologie di funzionamento dei meccanismi base del monitoraggio (modelli)

- Progettazione “su carta” di un telaio applicativo minimale per ognuna delle tipologie identificate
- Implementazione in modalita' aperta dei componenti base del telaio per i principali sistemi operativi e per le varie piattaforme comunicative esistenti
- Definizione dei protocolli di integrazione dei singoli controlli
- Capitalizzazione delle logiche di funzionamento dei vari componenti
- Astrazione dallo specifico linguaggio di programmazione
- Forte orientamento alla compattezza del codice e del carico indotto
- Costante confronto con i prodotti standard del mercato

E-Mon – Modelli operativi

Vediamo alcuni modelli operativi

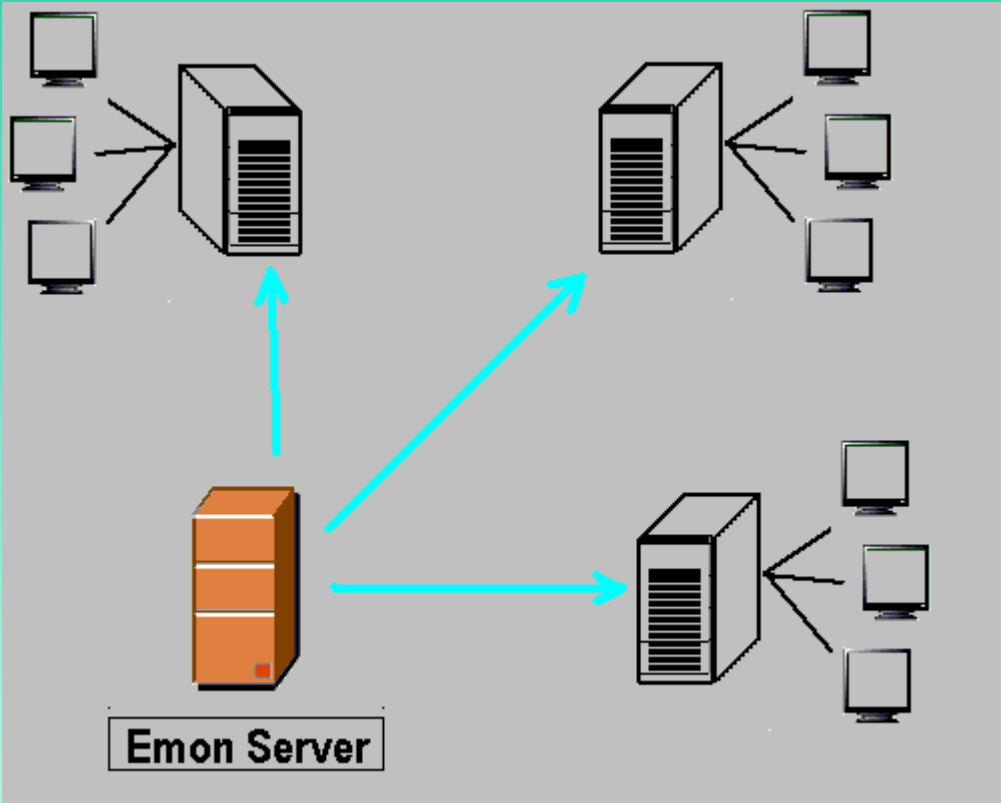
- Monitoraggio in rete locale non invasivo
- Monitoraggio in rete locale invasivo
- Monitoraggio distribuito
- Monitoraggio remoto
- Monitoraggio remoto via gateway

E-Mon – Modello “Locale non Invasivo”

Implementazione del modello locale non invasivo:

- Si utilizza un elaboratore dedicato al monitoraggio, posto nella rete locale del/dei sistemi da controllare
- L'applicazione di monitoraggio gira esclusivamente all'interno dell'elaboratore dedicato, effettuando i controlli degli oggetti da monitorare tramite dei “ping” (usiamo questo termine improprio)
- Non si installa alcuna cosa sui sistemi da controllare, da cui la non invasività di questo modello
- Il tipo di controlli è limitato a ciò che in un qualche modo è “visibile” dall'esterno dei singoli sistemi da controllare
- Ottimo per un approccio del tipo “visione lato utente finale” (“controllo di esistenza in vita”, controllo di server di posta, web, applicativi, etc...)

E-Mon – Modello “Locale non Invasivo”

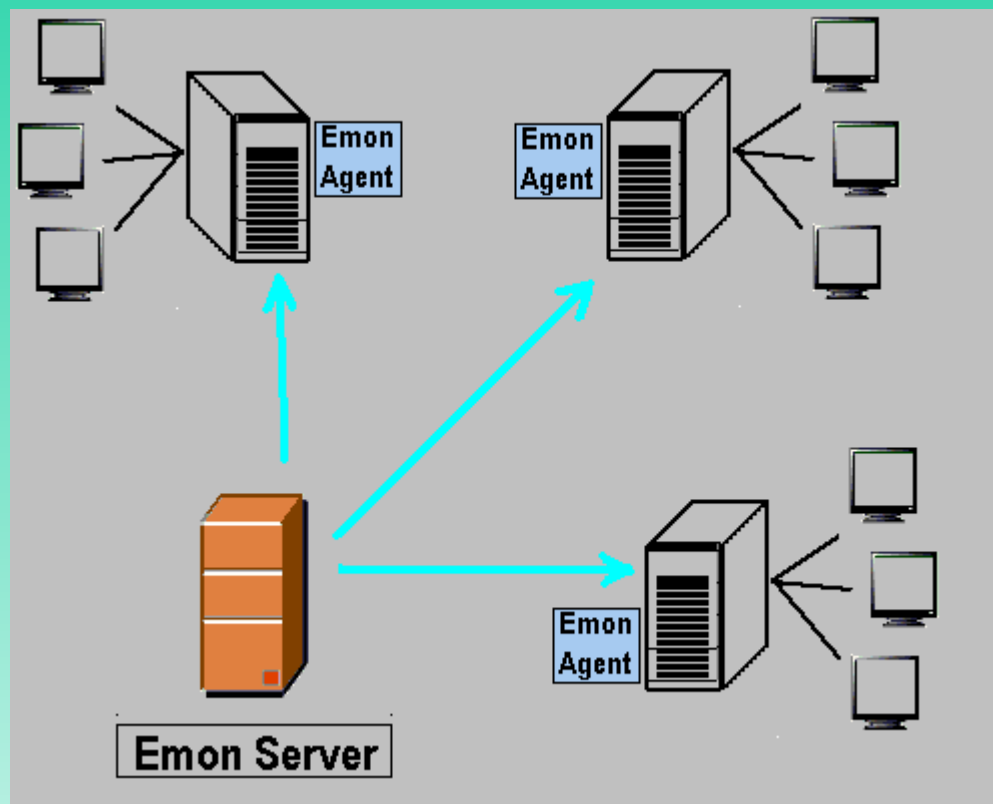


E-Mon – Modello “Locale Invasivo”

Implementazione del modello locale invasivo

- Si utilizza sempre l'elaboratore dedicato al monitoraggio, posto nella rete locale del/dei sistemi da controllare
- Sui sistemi da controllare, se possibile, si installano degli agenti specializzati a “sentire” tutto quello che interessa (eventi standard e non)
- Il server di monitoraggio puo' quindi effettuare sia gli stessi “ping” del modello non invasivo, sia acquisire le rilevazioni effettuate localmente dagli agenti
- Il tipo di controlli e' molto ampio. Oltre a cio' che e' visibile dall'esterno, e' infatti possibile rilevare cio' che accade “all'interno” dei sistemi
- Questo modello e' ottimo e copre la totalita' delle esigenze di monitoraggio.
- Ovviamente se ci sono possibilita' di implementare controlli “ad hoc” sia su server che sui vari nodi, “il gioco e' fatto”

E-Mon – Modello “Locale Invasivo”



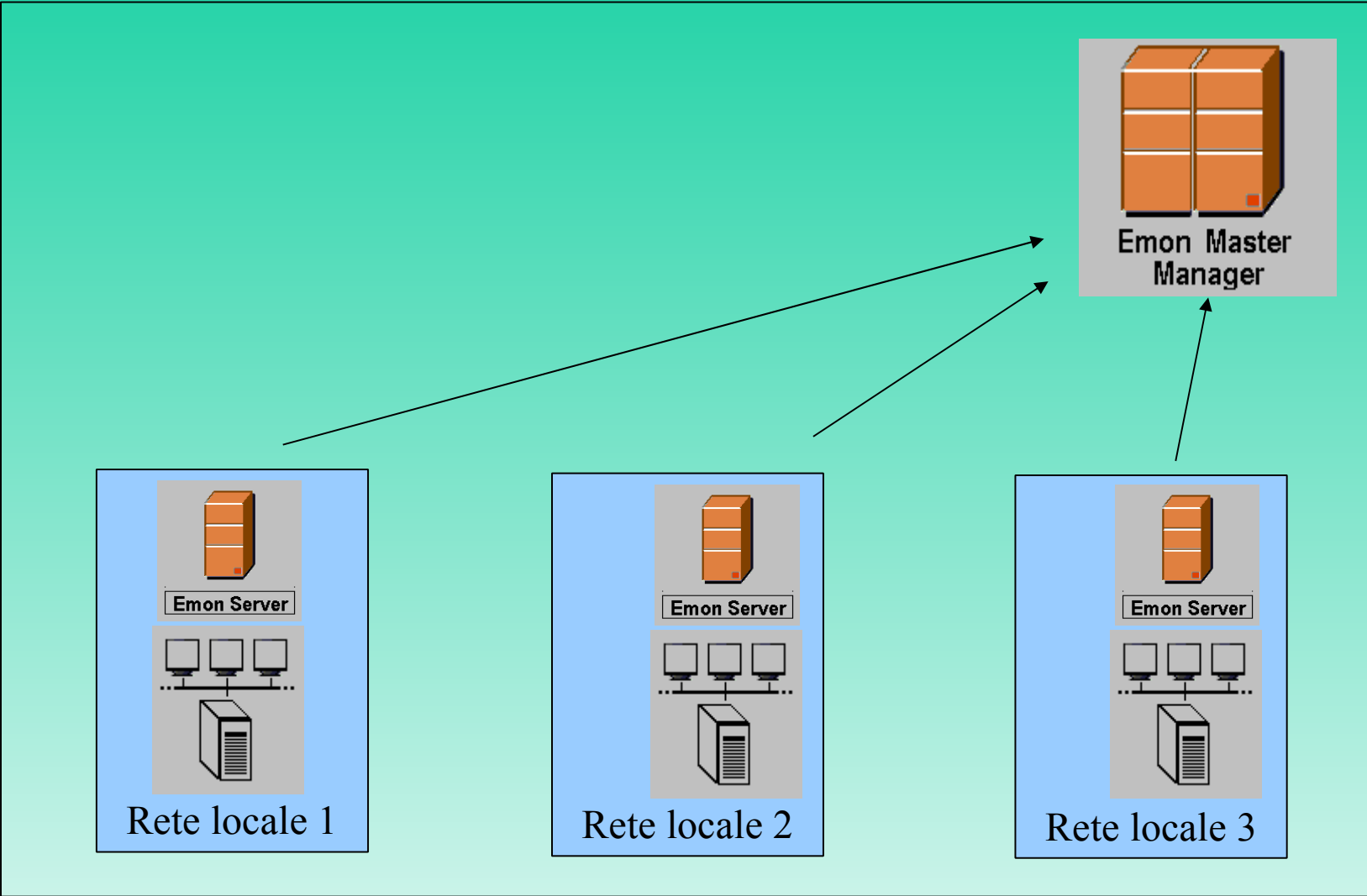
Rete locale

E-Mon – “Modello Distribuito”

Implementazione del modello distribuito

- Nel caso del modello distribuito si parte da una struttura articolata in piu' aree (logiche o fisiche) in ognuna delle quali si presenta una struttura di tipo “Modello locale” (invasiva o no)
- I vari computer che effettuano il monitoraggio possono essere interconnessi in una struttura gerarchica, nel qual caso c'e' un computer “manager centrale”, collocato o in una delle aree o all'esterno
- In ogni caso le attivita' “locali” sono effettuate anche in mancanza di comunicazione tra le singole aree, per cui determinati controlli possono essere comunque fruiti localmente.
- Tutto cio' che e' invece delegato al manager centrale in termini di controllo e allarme, risente ovviamente del corretto funzionamento (e della perfetta comunicazione) tra se' e ogni singolo computer d'area
- Il vantaggio di questa struttura e' di poter avere un punto centrale di controllo coordinato di tutta la struttura, dal quale poter ricavare le informazioni complete di stato dei vari sistemi

E-Mon – Modello “Distribuito”

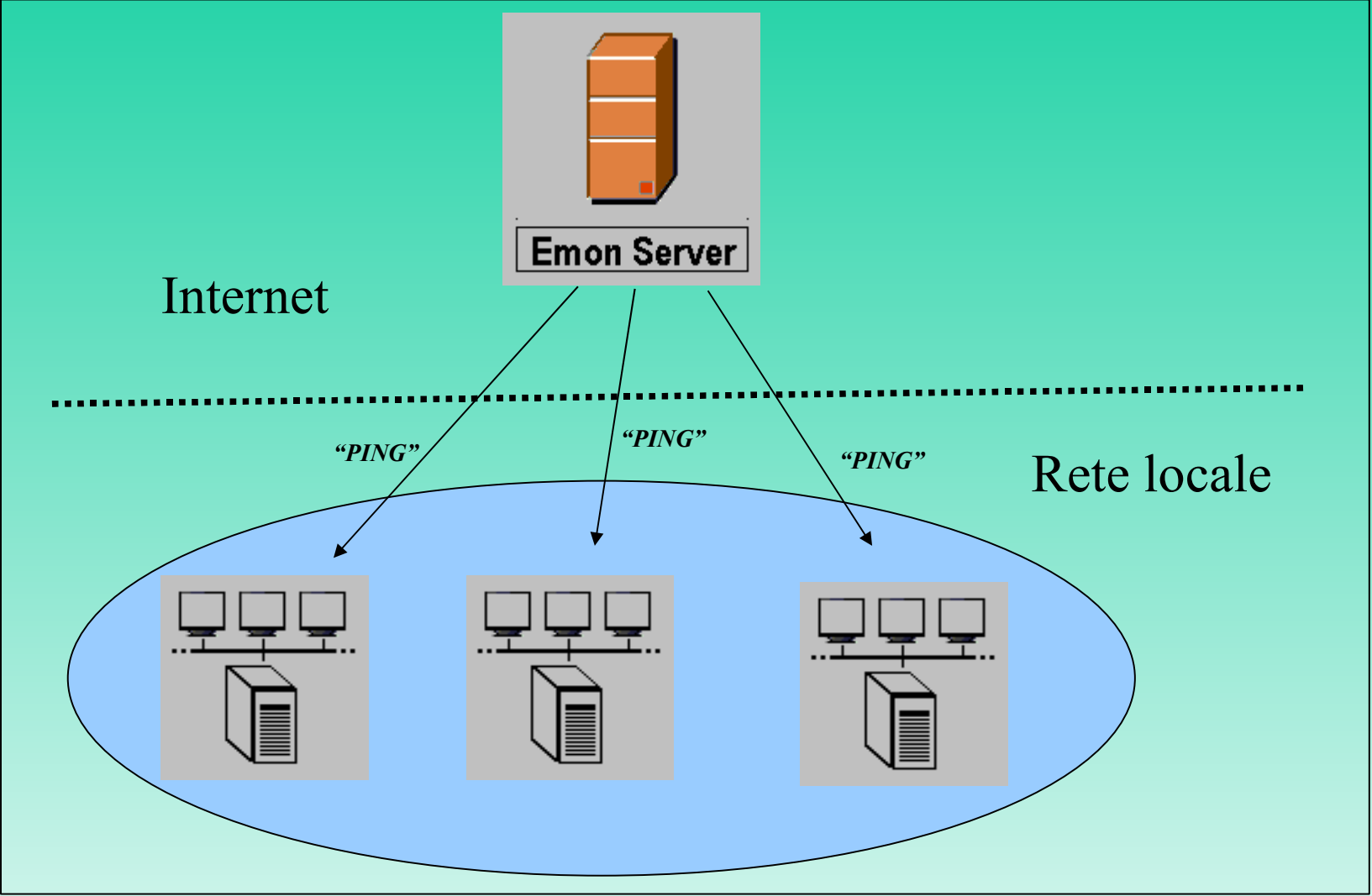


E-Mon – Modello “Remoto”

Il modello di monitoraggio remoto via Internet

- Si utilizza la stessa filosofia del modello locale (invasivo o meno) solo che il/i computer su cui gira il programma di monitoraggio e' un computer remoto ed e' collocato sulla rete Internet
- E' facilmente gestito il modello “locale non invasivo”, a patto di permettere il passaggio dei “ping” sugli apparati di rete dell'area interessata. Se si controllano server di posta o web server aziendali che siano visibili da Internet questi canali sono gia' aperti
- Il modello “invasivo” e' ugualmente accessibile, a patto di aprire la rete aziendale al tipo di dialogo necessario per la comunicazione tra agente e manager di monitoraggio (si puo' scegliere appositamente, ad esempio, i protocolli “classici” ftp o http)

E-Mon – Modello “Remoto”

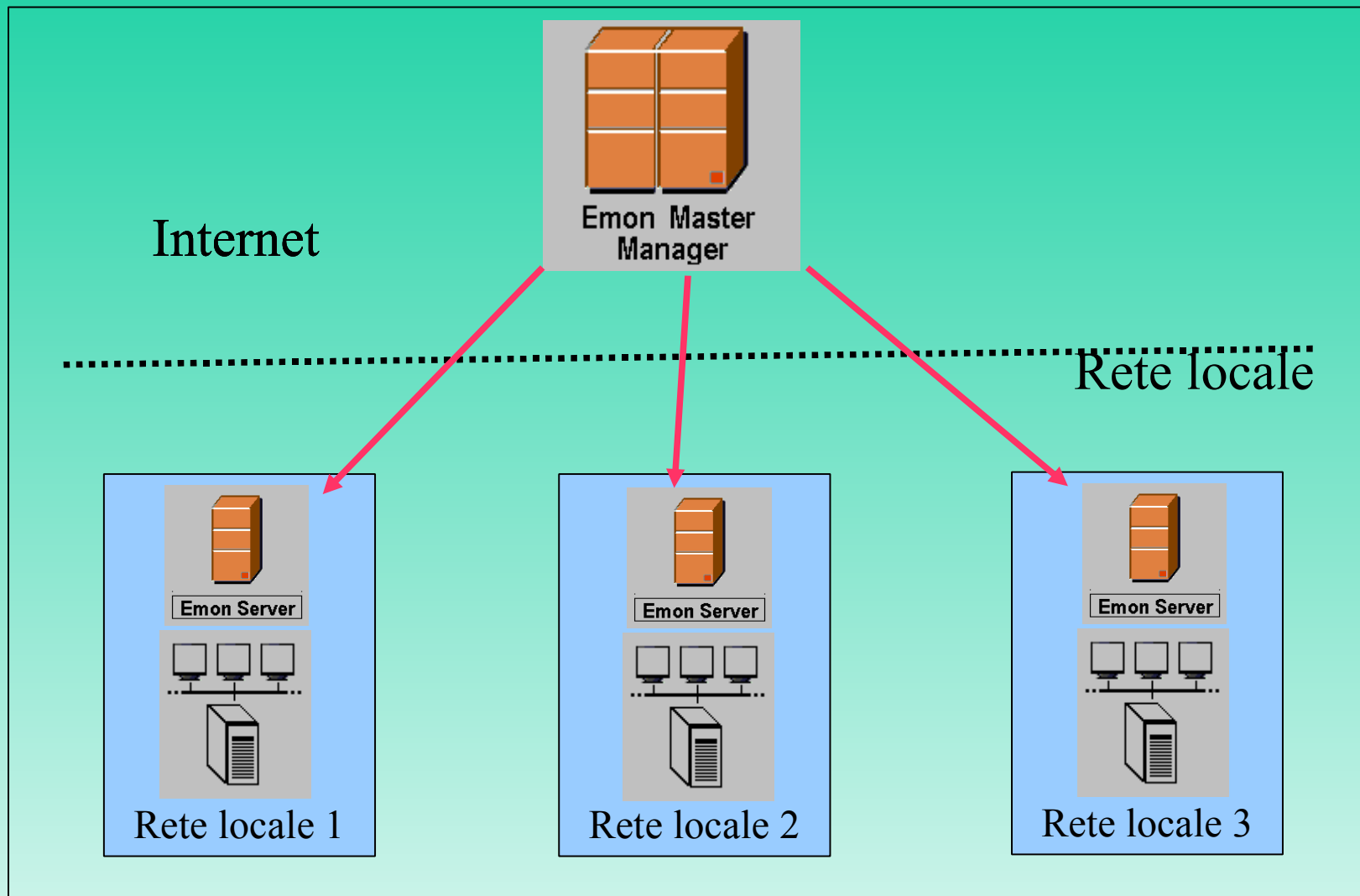


E-Mon – Modello “Remoto via Gateway”

Il modello di monitoraggio remoto via gateway

- Si utilizza per ogni area un elaboratore dedicato al monitoraggio, posto nella rete locale del/dei sistemi da controllare, con funzioni di gateway
- Si utilizza un manager remoto posto in internet
- L'elaboratore “gira” le sue rilevazioni al manager remoto tramite un protocollo scelto ad hoc, garantendo la separazione “galvanica” tra i vari nodi della rete locale e il resto del mondo
- In pratica e' un modello distribuito con l'aggiunta di un computer di “transito” che, funzionalmente e' un server di monitoraggio ma che non e' accessibile come console locale.
- Funzionalmente il gateway puo' anche essere una macchina non dedicata, a patto di garantire uno spazio operativo adeguato.

E-Mon – Modello “Remoto via Gateway”



E-Mon – Tecnologie di sviluppo

Alcune tecnologie di sviluppo

- Traccia in pseudocodice per tutte le logiche dell'applicazione
- Profiling applicativo e sistemistico per tutte le funzioni del prodotto
- La trace applicativa esiste per ogni singola funzione
- Utilizzo di database proprietario per erogare prestazioni adeguate
- Le implementazioni in linguaggio C sono a basso impatto e alto sfruttamento del multitasking (sistemi Windows/Linux e Unix)
- Le elaborazioni “stack intensive” sono, se necessario, riscritte in “cpu intensive” per minimizzare carichi e influenze negative sul sistema
- I tool correlati al sistema e al networking sono realizzati con la massima cura e con il minimo impatto
- L'implementazione dei sorgenti “a blocchi” e' soggetta ad una procedura di “Inline”, per migliorare le prestazioni
- Sono supportate varie piattaforme sistemistiche

E-Mon – Filosofie operative

- Le funzionalita' di “agente”, di “manager” e di “master manager” sono “platform independent” e non hanno alcun prerequisito software (sql server, java, librerie particolari). Sono realizzate senza alcu codice proveniente da terze parti
- Agenti e Manager possono operare su macchine non dedicate
- L'altissima integrazione rende possibili soluzioni “low impact” anche su sistemi che gia' possiedono altri sistemi di monitoraggio (Hp Openview, CA-TNG, Tivoli, GFI, Nagios, eccetera)
- E' possibile creare “entry point” ed “exit point” da e per altri sistemi di monitoraggio, convogliando esiti di controlli particolari verso altri prodotti oppure raccogliendo dati dagli altri sistemi.
- Le consoles possono essere di vario tipo anche se le soluzioni piu' aperte sono attualmente quelle basate su browser internet di qualunque tipo (piu' portabili di cosi'....)

E-Mon – Alcuni numeri

- Un tipico agente per Windows (qualunque versione) e' realizzato come singolo file eseguibile della dimensione variabile dai 40 ai 150 kbytes. Analoga la dimensione per Linux
- L'occupazione di memoria di un agente con funzionalita' piene e' di circa 700 kbytes sotto Windows e di circa 1 Mbyte sotto Linux
- Lo spazio disco occupato e' minimo (sotto il megabyte). La storicizzazione locale dei dati di monitoraggio ad eventuale futuro e' di pochi Mbytes all'anno e puo' essere pre-eseguita per minimizzare problemi di spazio disco. Pure l'agente non ha malfunzionamenti per problemi di condizioni di "disk full".
- Un banale client windows, mediamente dotato e non dedicato, puo' fare da server tranquillamente per un centinaio di nodi
- Un client windows con almeno 512 mb di Ram e processore da almeno 2 Ghz puo' gestire virtualmente fino a 65535 nodi e varie consoles
- L'agente e il manager operano con frequenze di polling di un minuto, configurabile, per un'alta risoluzione di gestione, mentre il manager remoto internet puo' effettuare controlli anche ogni 10 secondi!

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*