

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*

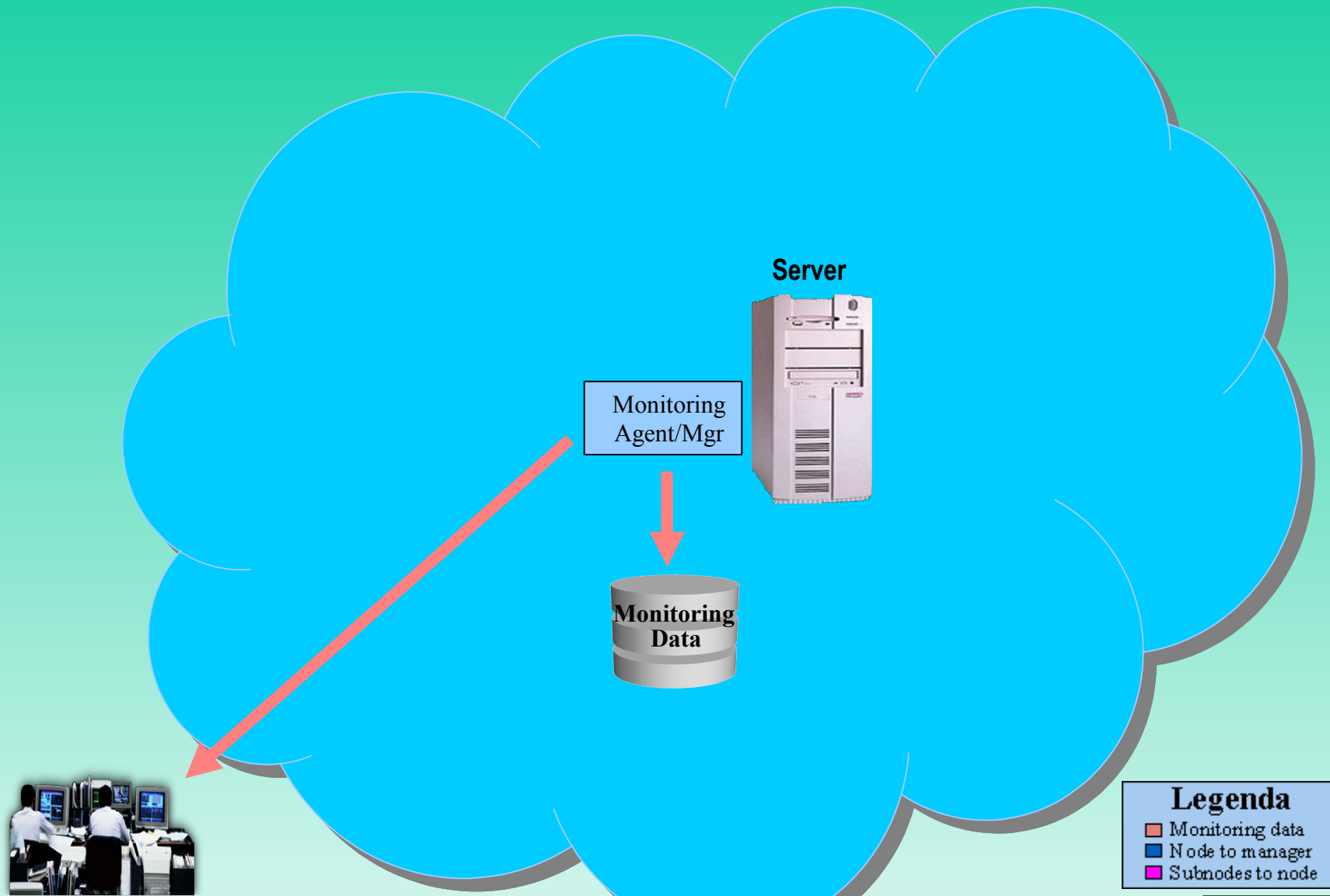
Assistenza – Sicurezza - Forensic

Telecomunicazioni - Elettrosmog

EMON Monitoring Framework

Agent Description

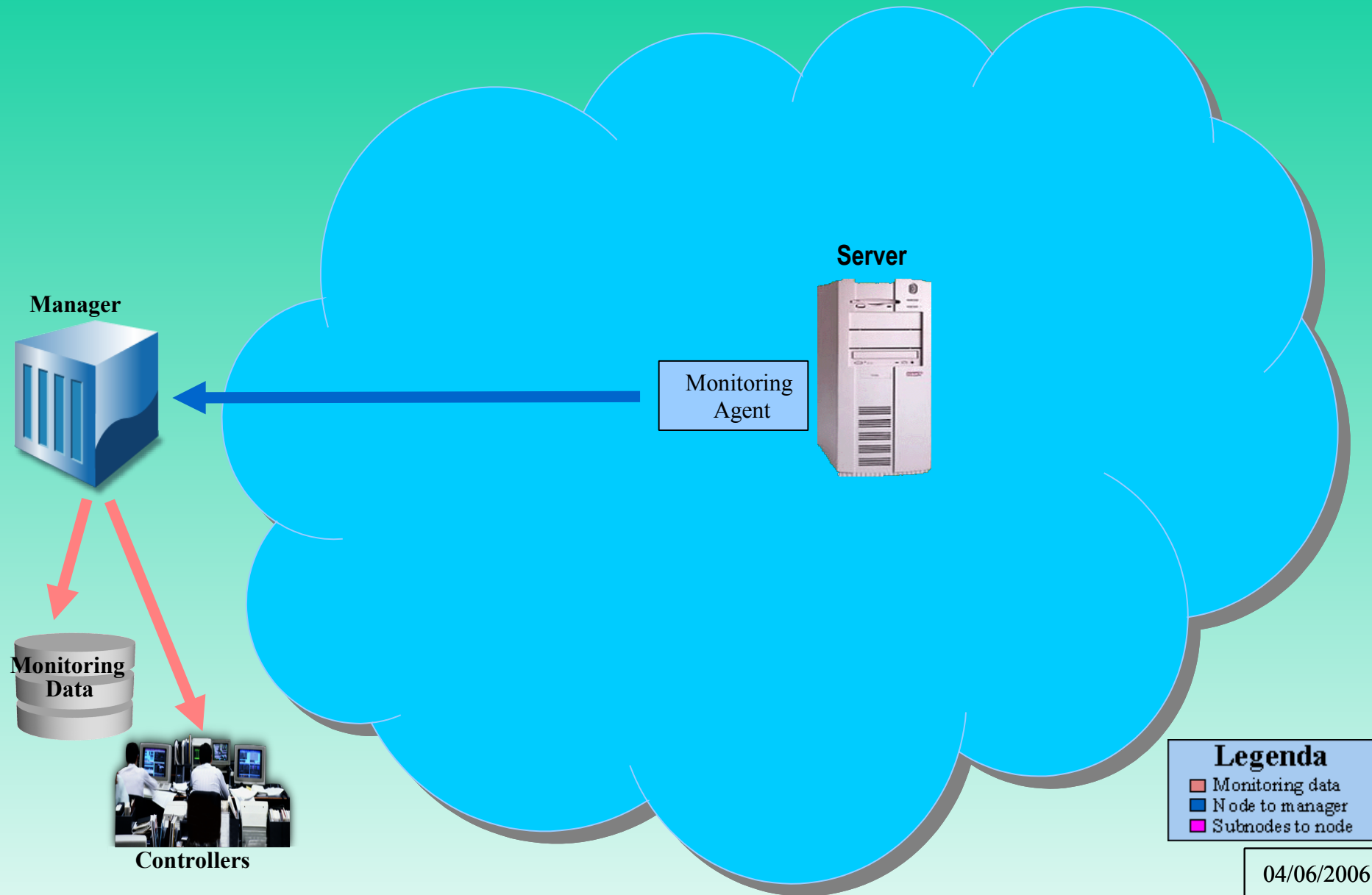
Monitoring – Real World



Legenda

- Monitoring data
- Node to manager
- Subnodes to node

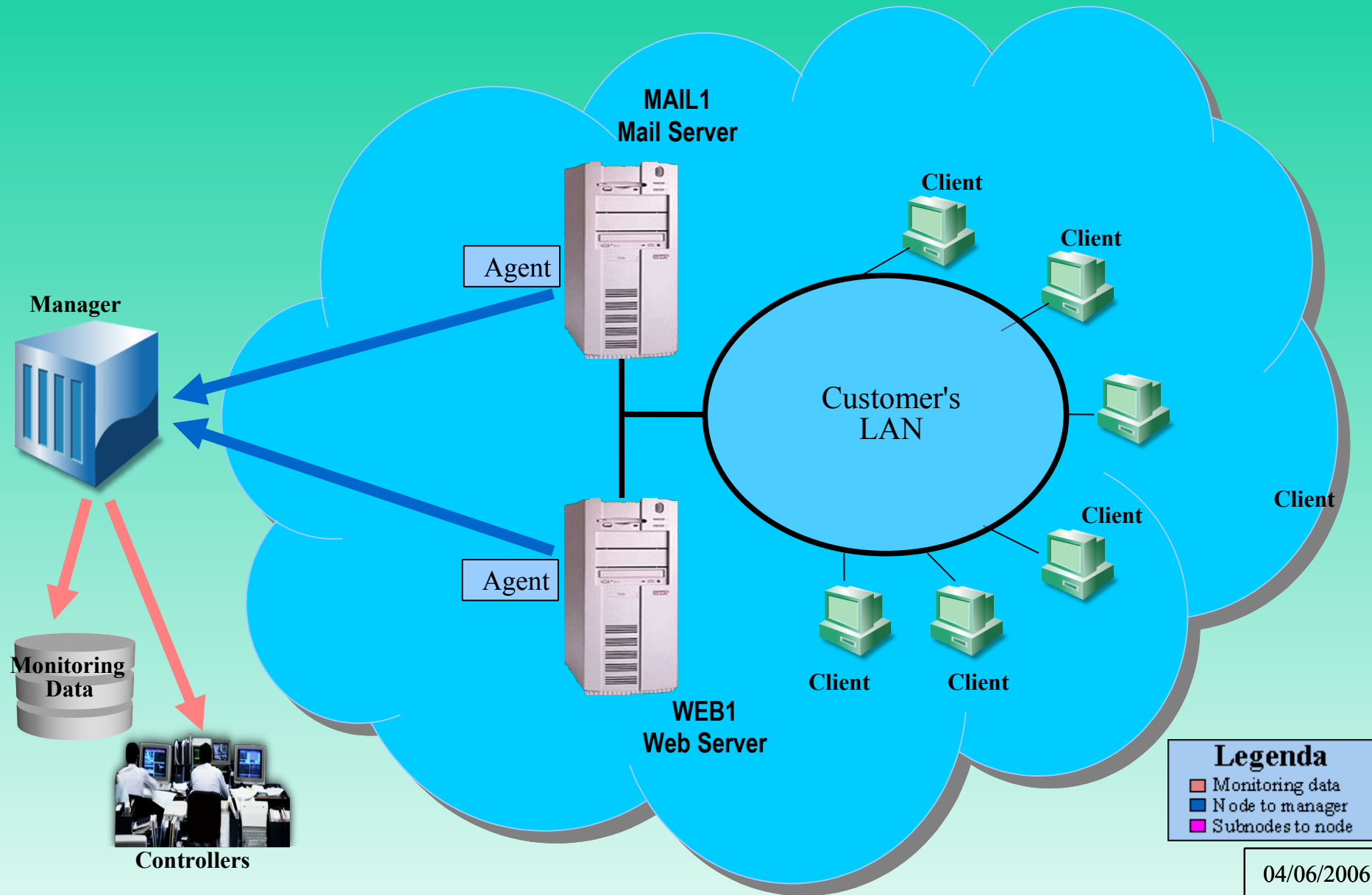
Monitoring – Real World



Legenda

- Monitoring data
- Node to manager
- Subnodes to node

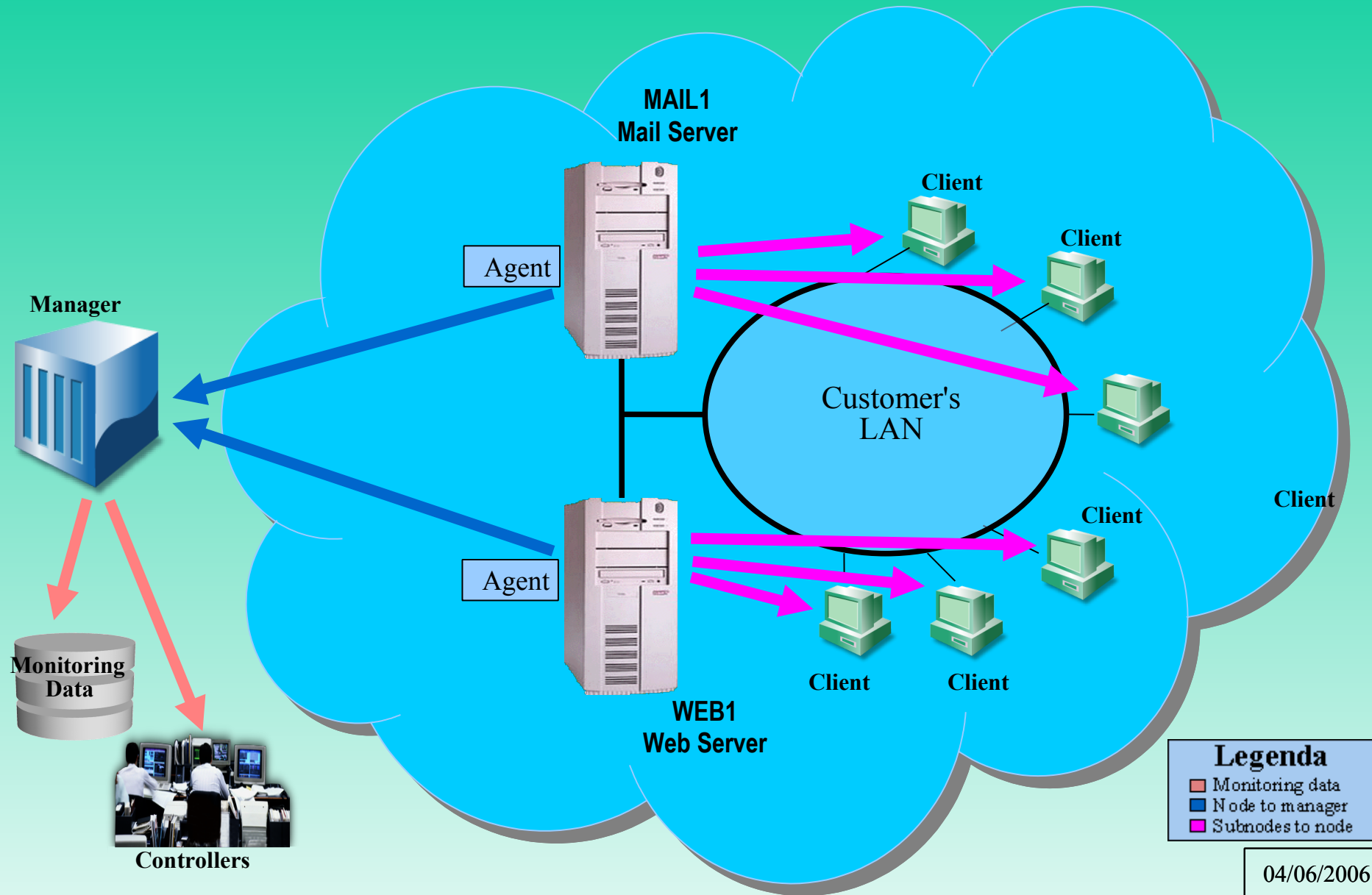
Monitoring - Real World



Legenda

- Monitoring data
- Node to manager
- Subnodes to node

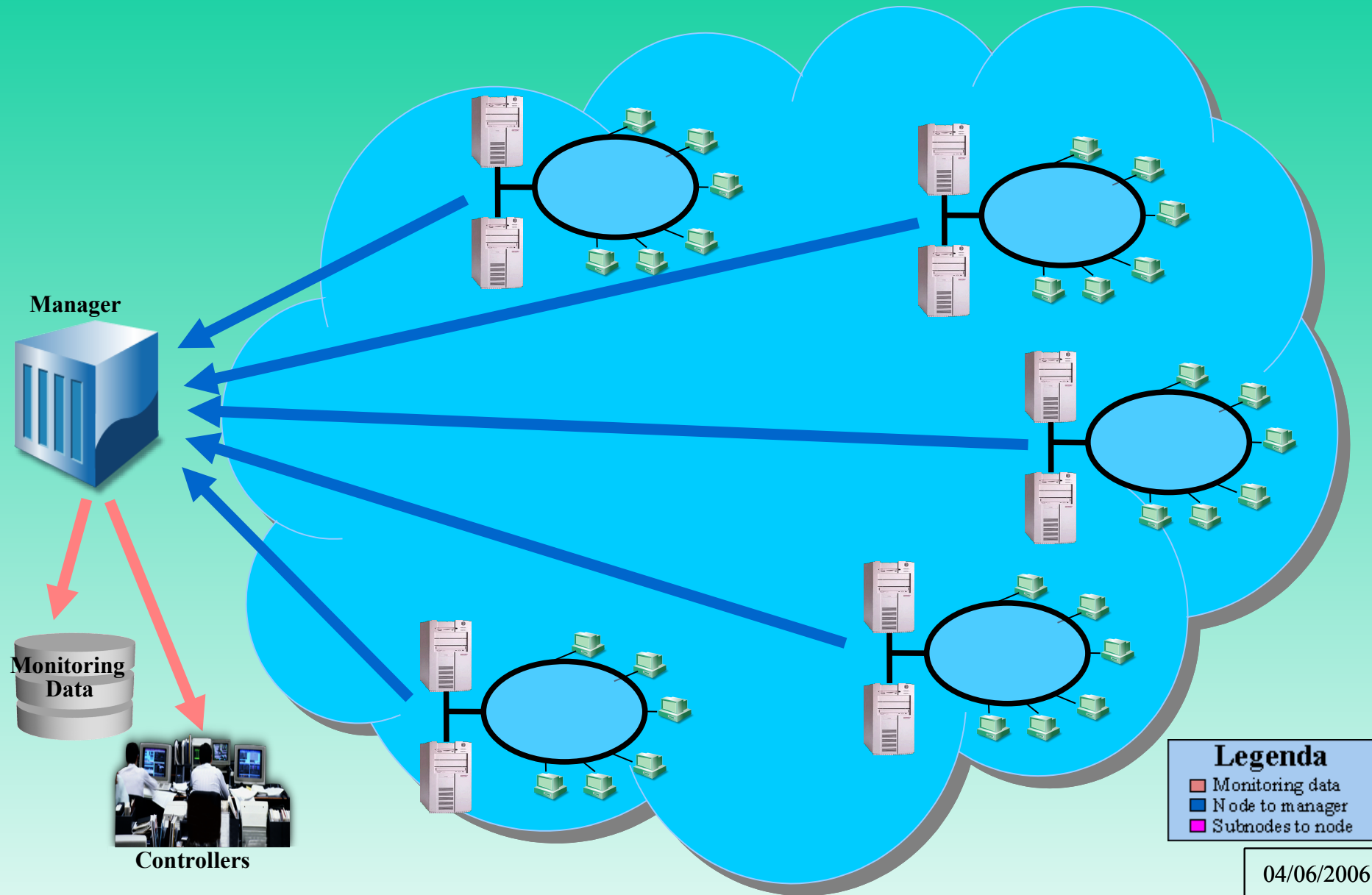
Monitoring - Real World



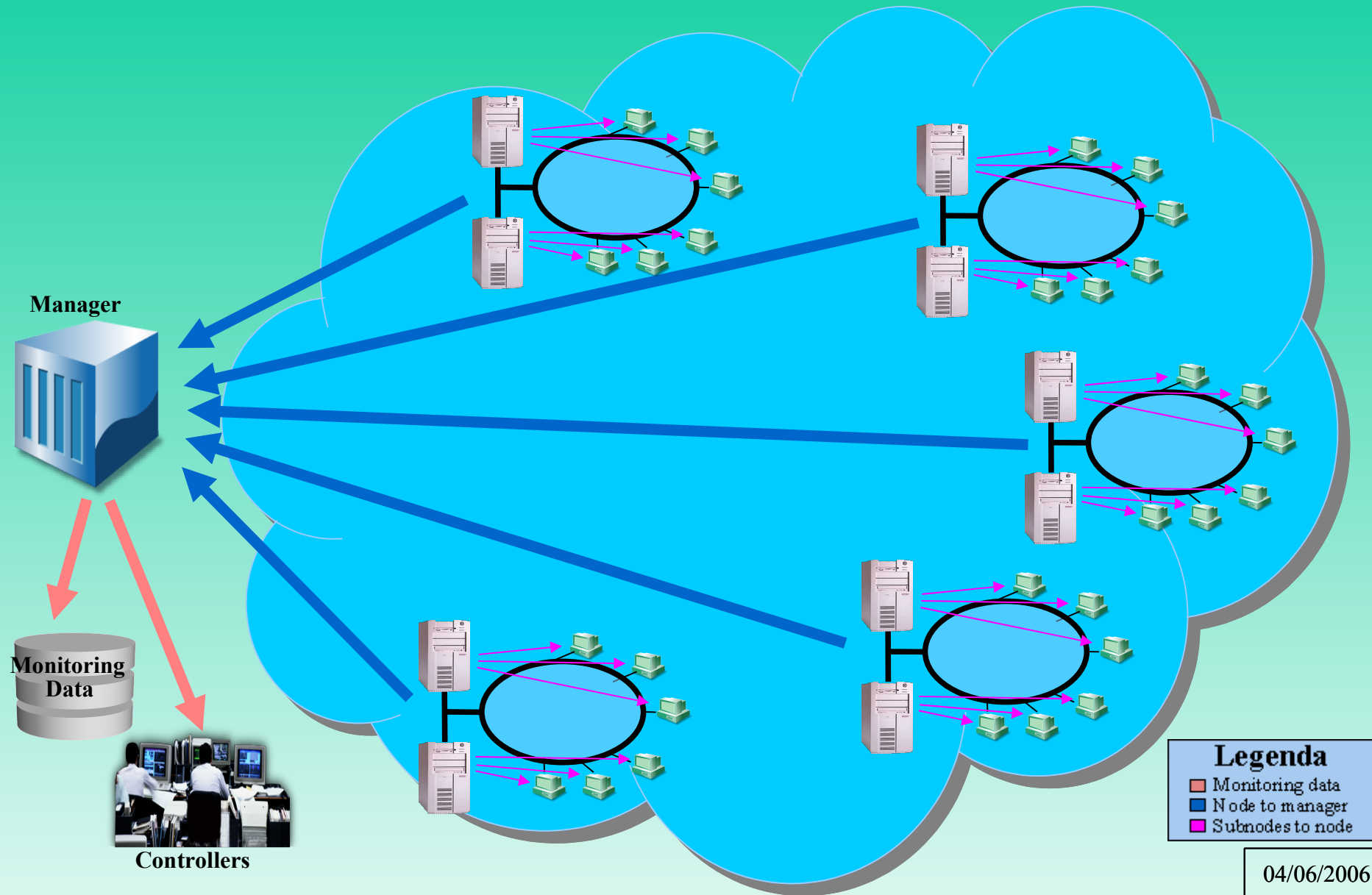
Legenda

- Monitoring data
- Node to manager
- Subnodes to node

Monitoring – Real World



Monitoring – Real World



Un buon agente....

- non deve invadere il sistema ospitante
- non deve richiedere supporti applicativi (db, libraries, etc)
- deve monitorare cio' che serve
- deve recepire situazioni critiche dell'ospite
- deve operare anche in assenza del manager
- deve essere implicitamente affidabile
- deve essere modulare e integrabile con programmi esterni

Cosa ci piacerebbe controllasse un buon agente....

- il buono stato di funzionamento del sistema
- il buon contesto comunicativo
- lo stato dell'antivirus/IDS
- lo stato di aggiornamento del sistema operativo e delle applicazioni base
- lo stato delle operazioni di gestione dei dati (backup, file transfer, etc)
- lo stato di gestione del nodo (asset, posizione in rete, info varie di manutenzione)
- il contesto elettrico, termico e di sicurezza fisica (UPS, sensori, etc)
- altri nodi o oggetti di rete privi di agente, agendo come un submanager

E vediamo qualcosa dell'agente EMON....

- puo' leggere i parametri resi disponibili via API e interagire con il sistema
- puo' leggere files di log di sistema (eventlog, drwatson, log di IIS, etc)
- puo' interagire con tutte le applicazioni che forniscono API accessibili in C o altro
- puo' lanciare programmi esterni leggendone il return code o l'output
- puo' leggere file di log (esempio: antivirus, IDS, log di applicazioni particolari)
- puo' effettuare operazioni sui socket per controllare oggetti e applicazioni in rete
- puo' richiamare servizi o attivare applicazioni esterne agendo "like-user"
- puo' interagire con altri sistemi di monitoraggio, inviando o ricevendo informazioni
- puo' controllare caratteristiche hardware o consultare dispositivi esterni

Alcune funzionalita' dell'agente

- 1) L'agente effettua di default un polling ogni minuto. Alta risoluzione temporale degli eventi, elevata precisione e possibilita' di rilevare eventi "rapidi". Sono 1440 controlli al giorno.
- 2) Al polling vengono misurati (e storicizzati "a vita") tutti i valori "standard" (memoria, spazio disco, carico CPU, processi attivi e relativi parametri di attivazione etc) oltre al livello di SLA dell'agente stesso. E' quindi possibile elaborare i dati storici, esaminando incidenti o rilevando limiti funzionali.
- 3) Motore di elaborazione degli stati completamente configurabile e parametrizzabile. E' possibile sapere se e' in corso un DrWatson, se un processo resta attivo (o inattivo) per un tempo superiore al normale o se la CPU e' soggetta ad una condizione di "intasamento" per eccesso di task e thread attivi. E' possibile tra le varie cose correlare eventi diversi: se avviene un DrWatson l'agente e' in grado di segnalare anche il nome e le caratteristiche del programma che e' caduto!

Alcune funzionalita' dell'agente (2)

4) L'agente puo' effettuare operazioni specifiche a fronte di specifiche situazioni sistemistiche. Ad esempio, su una macchina Wintel, a fronte del verificarsi di un DrWatson, puo' successivamente ripulire il file "user.dmp" per evitare problemi di spazio disco.

5) L'agente puo' leggere specifici files di log, anche tramite logiche cablate "custom". Pertanto e' identificabile una condizione anche se espressa in forma "multiriga". Cio' sia sull'eventlog (esempio: nel systemlog di Windows la terna di eventi 6008,6009,6005 dell'applicazione 'Eventlog' e' chiara traccia di un reboot) che su files applicativi di qualunque tipo e dimensione. Viene anche gestito il puntatore dell'ultimo record gia' letto come pure il rewind del file

6) E' possibile effettuare un'insieme di survey su specifici files, identificando modifiche di qualunque tipo (creazione, cancellazione, modifica, cambio data, cambio parametri sicurezza....)

Alcune funzionalita' dell'agente (3)

- 7) Le survey possono anche essere effettuate su dimensioni e tipologie di contenuto di intere cartelle (ad esempio e' possibile implementare un sofisticato "quota manager") come pure su operazioni delicate. E' ad esempio possibile effettuare un controllo coerente di integrita' di specifiche operazioni (backups, file transfer, etc) tramite la verifica puntuale tra cio' che doveva essere spedito/salvato e il corrispettivo set di dati ottenuto dall'operazione.
- 8) L'agente puo' effettuare un sofisticato insieme di controlli di rete, identificando ad esempio se il proprio contesto operativo di rete e' corretto tramite l'analisi di ping, disponibilita' di porte locali e remote, esistenza di specifici protocolli di rete in nodi esterni. Ad esempio, nel caso non sia raggiungibile l'application server e il database server, l'agente del web server puo' registrare (e notificare) la condizione di "io sono a posto ma il resto no!".
- 9) Le capacita' di rilevazione sono associate a possibilita' di intervento attivo (o pro-attivo). Nel caso il sistema sia gravemente compromesso nelle sue funzionalita' oltre specifiche soglie, l'agente puo' comandare un immediato (o schedulato) reboot del server.

Alcune funzionalita' dell'agente (4)

10) il controllo dettagliato dei task permette di riconoscere eventi altrimenti invisibili, quali la chiusura e ripartenza "rapida" di specifiche applicazioni, anche se tali ripartenze vengono effettuate rapidamente, in quanto viene alterato l'insieme di informazioni del task.

11) L'agente puo' effettuare operazioni di discovery in rete. Ad esempio in pochi secondi puo' effettuare una scansione di una intera subnet (ad esempio 192.168.1.1-192.168.1.255) per identificare lo stato di tutti gli oggetti della rete determinando ad esempio se ci sono state aggiunte o rimozioni. Il plugin EMON_MNA permette la scansione di 256 indirizzi in pochi secondi, rendendo possibile implementare a livello di monitoraggio alcune funzionalita' di IDS, oltre che di Asset management!

12) L'agente puo' effettuare una scansione approfondita delle connessioni aperte sul server. In questo modo e' possibile ad esempio identificare quando una sessione TCP viene aperta con uno specifico indirizzo (interno o internet) e/o con un determinato port TCP/UDP. In questo modo si puo' ad esempio sorvegliare una specifica connessione o uno specifico utente

Alcune funzionalita' dell'agente (5)

13) L'agente puo' operare come submanager, effettuando monitoraggi "da remoto" su un insieme di nodi di competenza. I sottonodi possono essere con o senza agente EMON/altri agenti. E' pertanto possibile effettuare una gran mole di controlli sui nodi (ad esempio clients) oltre che operare come "sistema di monitoraggio ausiliario", segnalando anomalie del sistema di monitoraggio principale o sostituendolo nelle fasi di manutenzione/aggiornamento/sostituzione

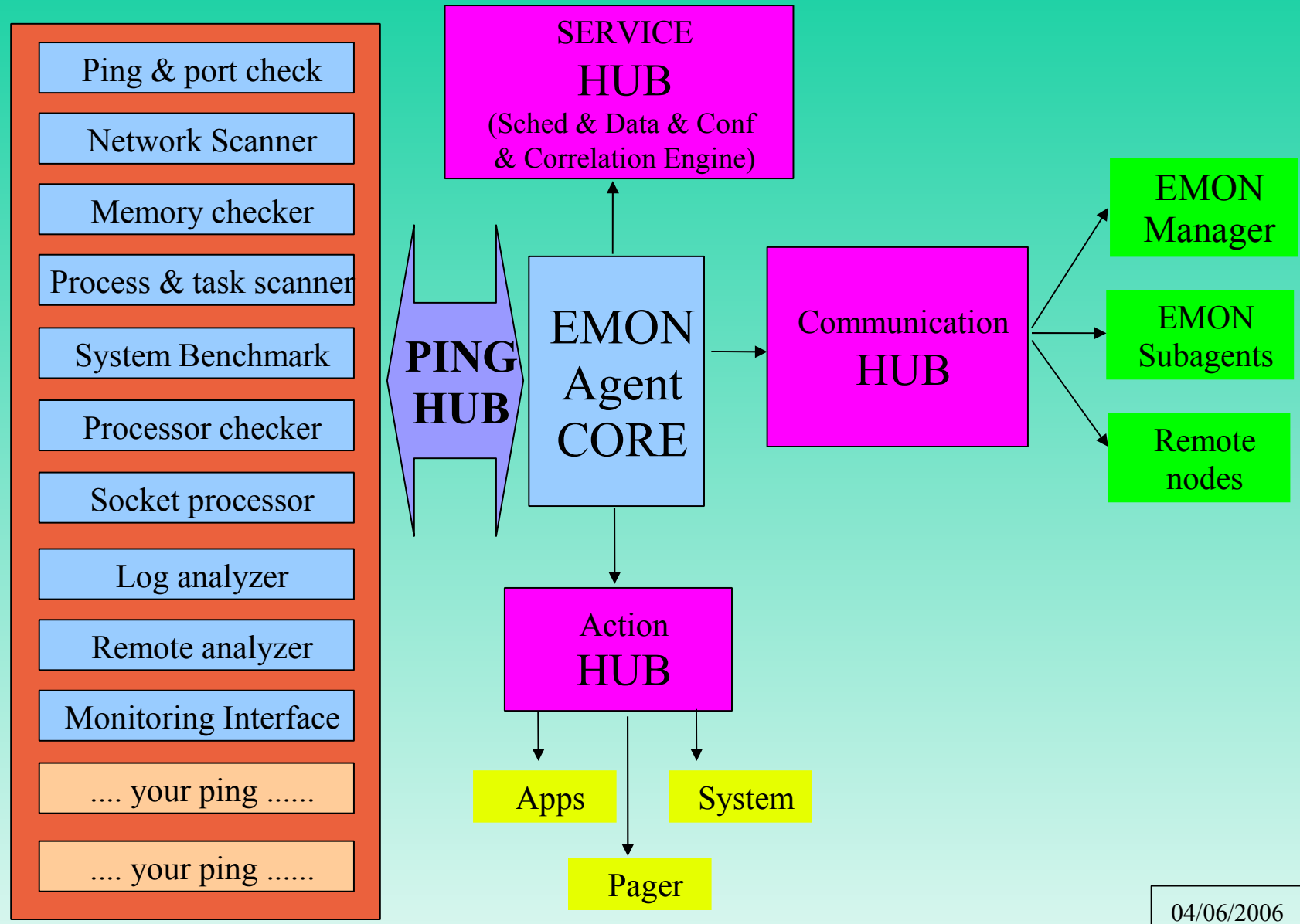
14) Tramite l'agente e' possibile instradare sul manager anche informazioni "di servizio" da script di manutenzione o da specifici breakpoint collocati all'interno delle applicazioni. Cio' permette di utilizzare il sistema di monitoraggio anche come sistema di gestione complessivo dei flussi informativi della rete. Associare l'esecuzione di una operazione specifica da parte di una applicazione con la caduta di un task (ad esempio per mancanza di memoria) diventa quindi possibile.

15) L'agente puo' effettuare dei check continui su una o piu' pagine di un sito web controllando la mancanza di errori "standard" ma anche la completezza e congruenza del contenuto della pagina con quello previsto (dimensione, presenza di specifici oggetti) rilevando (e segnalando eventuali anomalie) anche per i tempi di esecuzione.

I punti forti dell'agente EMON...

- 1) l'agente EMON e' "aperto" e strutturato modularmente, in modo da poter modificare le funzionalita' dell'agente secondo le esigenze specifiche.
- 2) e' possibile pertanto aggiungere all'agente qualunque codice risolva le tue necessita' di controllo, anche attingendo a librerie di programmi e applicazioni opensource. Puoi aggiungere qualunque funzione in C, ma, ovviamente, e' possibile utilizzare anche qualunque altro linguaggio sia interfacciabile con il linguaggio C, cioe'.... tutti!
- 3) l'agente e' "leggero" e molto piccolo (un singolo eseguibile di 70 kbytes e' in grado di eseguire tutti i classici controlli su un nodo!) e non causa alcun impatto al nodo che lo ospita. Pertanto puo' tranquillamente essere installato anche sui clients.
- 4) la registrazione locale di stati ed eventi e il suo invio "copia conoscenza" al manager sono pienamente configurabili in modo da poter consultare sul manager (o direttamente sul nodo) tutte le informazioni raccolte sulle attivita' del nodo. Questo permette di analizzare approfonditamente non solo gli eventi rilevanti ma anche tutto il contesto relativo. Attraverso l'analisi dei dati e' possibile quindi effettuare un perfetto tuning dei vari sensori per ottenere allarmi tarati perfettamente sulle necessita' specifiche e quindi realmente utili ed efficaci.

Schema a blocchi funzionale...



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