

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*

PHALANX – Gli utilizzi “normali”

Phalanx e' un framework di applicazioni e technicalities che permette varie e diverse operazioni.

- 1) Discovery e inventory di rete “on field” e “hot-plugin” per rilevazioni, diagnosi, etc
- 2) Sistema di monitoraggio non invasivo
- 3) Sistema di monitoraggio invasivo (con agenti sui nodi)
- 4) Intrusion Detection System
- 5) Identity manager
- 6) Sistema di telecontrollo/teleintervento/teleaggiornamento
- 7) Sistema di licensing per applicazioni, sistemi, accessi
- 8) sistema diagnostico “buil-in”
- 9) sistema di diagnostica “locale” per l'utente o per manutentori
- 10) debugger applicativo

.....

PHALANX – I punti “forti”

- e' un framework, pertanto e' modificabile “su misura” delle vostre esigenze
- tutto il codice e' proprietario, non ci sono librerie aggiuntive di terzi, massima sicurezza
- il prodotto puo' operare in perfetta autonomia ma anche in sinergia con altri prodotti
- integrazioni per Openview, Tivoli, CA/Unicenter, GFI, mondo opensource (nagios), etc
- si possono allestire soluzioni scalabili e distribuite
- prodotto marchiabile secondo i desiderata del cliente o “anomimo”
- bassissimo impiego di risorse su clients, nessun setup, piccoli eseguibili <100kb
- il prodotto e' allestibile in formato “internet” e/o “intranet” sia lato agenti che lato clients
- nessuna necessita' di indirizzi statici
- impegno comunicativo (e tecnologie relative) modulabile
- non necessita modifiche su firewall
- codice implementabile su piattaforme eterogenee (win, linux, unix, as400, etc)
-

PHALANX – Soluzioni e commercializzazione

Phalanx ha un insieme di funzionalità ben difficili da catalogare, spaziando dall'inventario al monitoraggio per arrivare alla sicurezza dei sistemi.

Phalanx può essere fornito come “prodotto finito”, come “soluzione chiavi in mano”.

Può anche essere fornito come “servizio”, con soluzioni specifiche per determinate esigenze. Appositi contratti di assistenza prepagata permettono di definire le migliori condizioni per un proficuo utilizzo delle potenzialità del prodotto, con soluzioni scalabili e ridefinibili in corso d'opera.

Per aziende che non hanno infrastrutture tecnologiche e know-how specifico, DigitalExpert fornisce una soluzione completa, in grado di coprire tutti i vari aspetti di sicurezza, monitoraggio, inventario ed esercizio dei sistemi. In quest'ultimo caso l'offerta comprende solitamente:

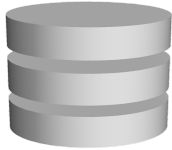
- una fase di preventiva analisi dell'infrastruttura
- la progettazione di un sistema di gestione “base”
- la formazione del personale per un uso “sicuro” dell'infrastruttura informatica
- l'implementazione di controlli specifici secondo le esigenze del cliente e le criticità
- la gestione del sistema di sicurezza “da remoto”, con eventuali segnalazioni di allarme
- una console di controllo presso il cliente per gli aspetti di specifico interesse del cliente

La soluzione viene in ogni caso “plasmata” sulle esigenze del cliente e sulle effettive criticità dell'infrastruttura.

PHALANX – Discovers Nodes&Apps Relationships

Monitoring Data

Controllers



Server **MAIL1**
192.168.1.1



Sessioni "posta"

Agente Phalanx - Accessi MAIL1

FTP	192.168.1.2
Exchange	192.168.1.104
Exchange	192.168.1.105
Exchange	192.168.1.106

192.168.1.106

192.168.1.105

192.168.1.104

Sessione FTP inter-server

Agent Phalanx - accessi WEB1

FTP	192.168.1.1
Apache	192.168.1.101
Apache	192.168.1.102
Apache	192.168.1.103

192.168.1.103

192.168.1.102

Phalanx Manager

Phalanx Manager

Rilevazione Connessioni Funzionali

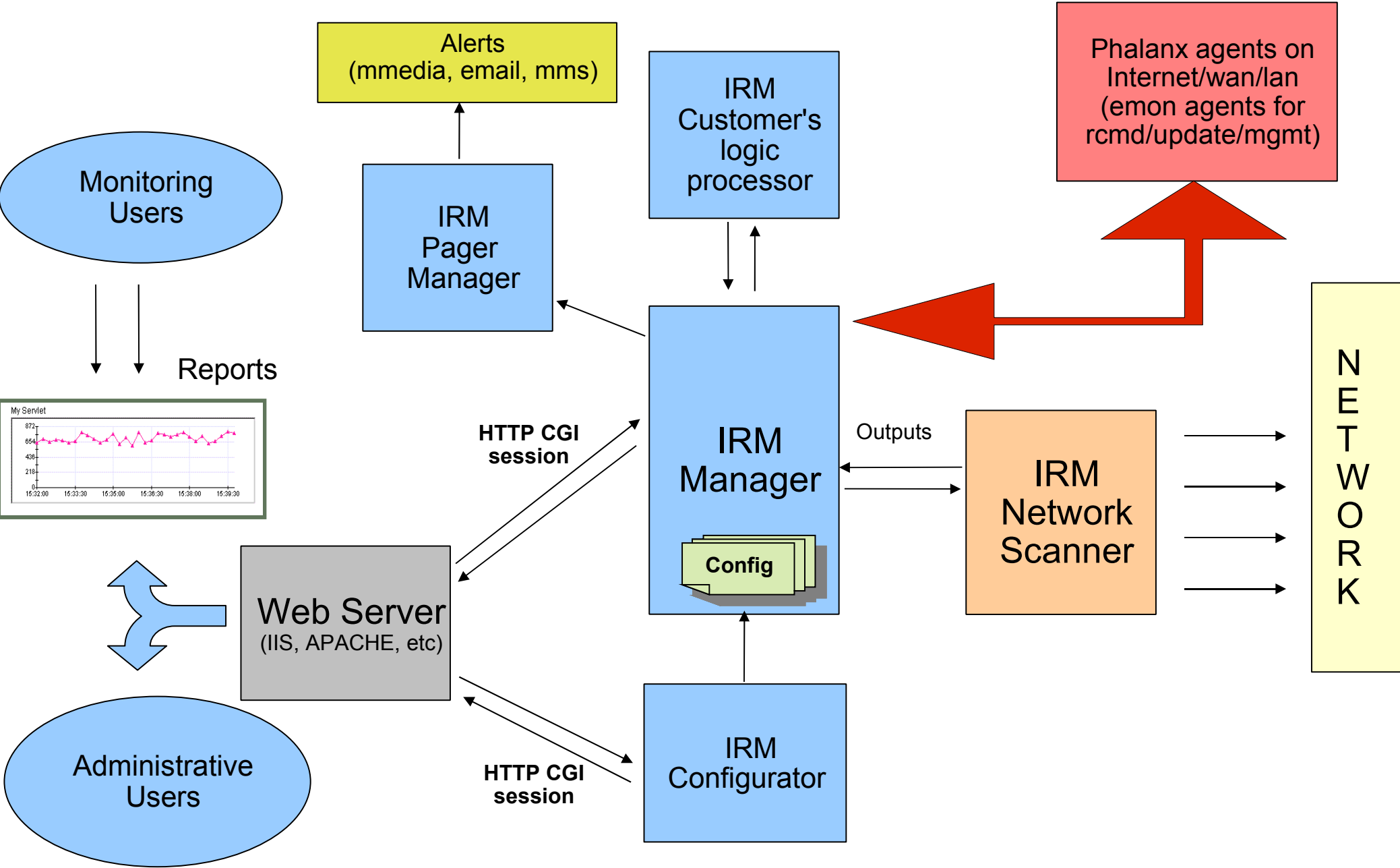
FTP	192.168.1.1 - 192.168.1.2
Apache	192.168.1.2 - 192.168.1.101
Apache	192.168.1.2 - 192.168.1.102
Apache	192.168.1.2 - 192.168.1.103
Exchange	192.168.1.1 - 192.168.1.104
Exchange	192.168.1.1 - 192.168.1.105
Exchange	192.168.1.1 - 192.168.1.106

Server **WEB1**
192.168.1.2

Sessioni "web"

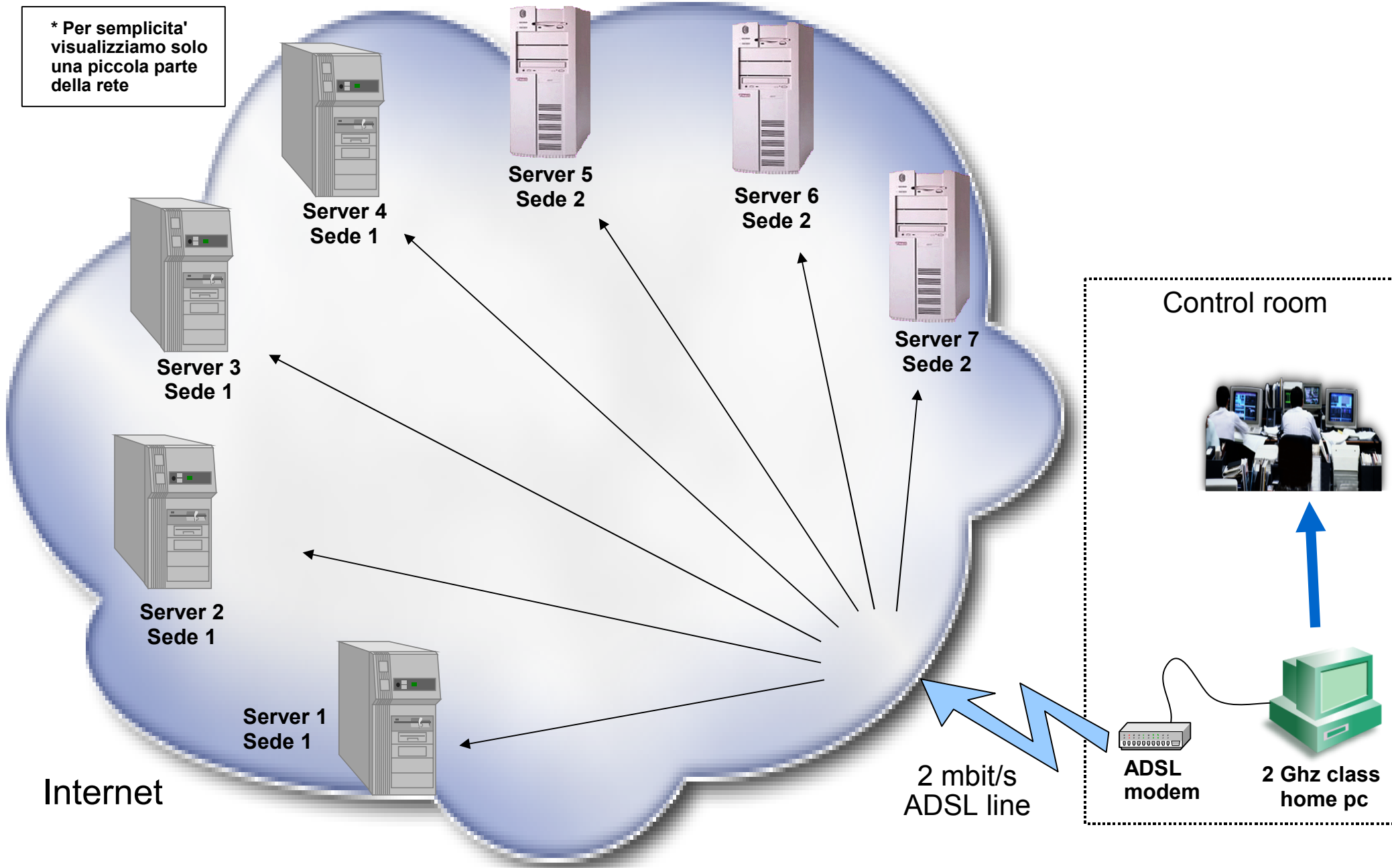
192.168.1.101

Schema a blocchi soluzione composita EMON-IRM-Phalanx



La soluzione EMON-IRM-Phalanx – Schema generale "light"

* Per semplicita' visualizziamo solo una piccola parte della rete



Internet

Control room

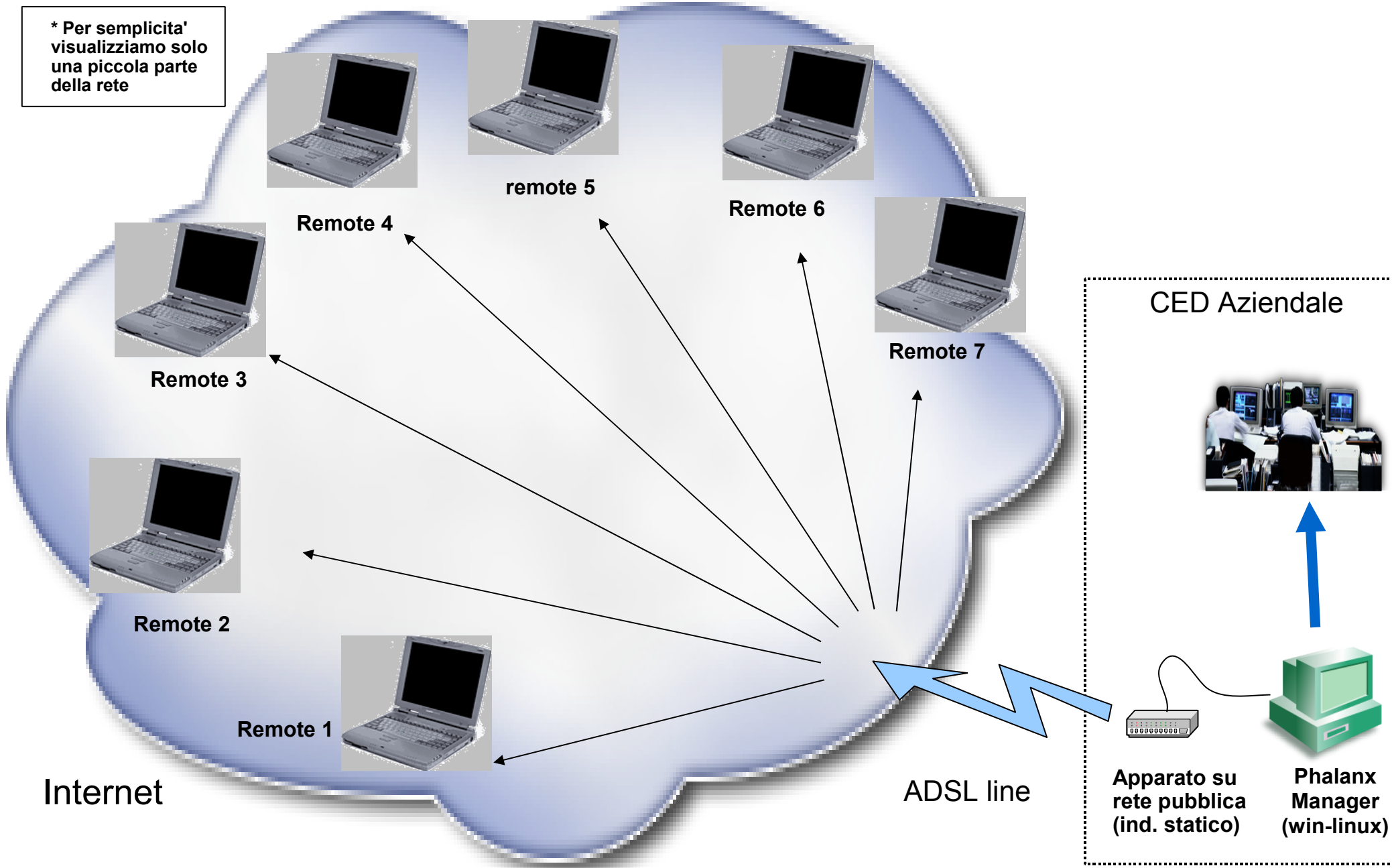
2 mbit/s ADSL line

ADSL modem

2 Ghz class home pc

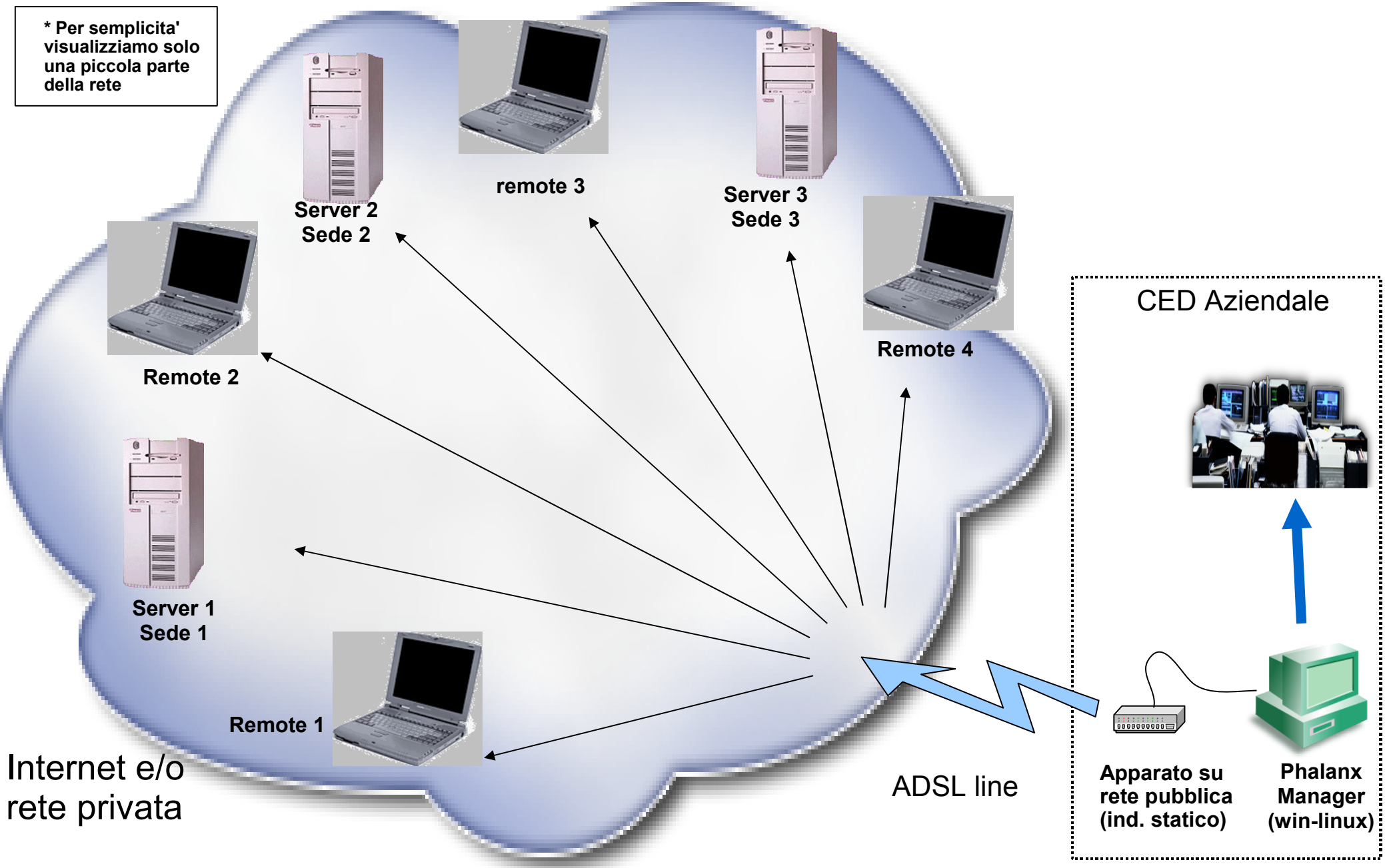
La soluzione Phalanx/Emon - Controllo "totale" utenti remoti

* Per semplicita' visualizziamo solo una piccola parte della rete



Soluzione Phalanx/Emon - Controllo "totale" azienda connessa

* Per semplicita' visualizziamo solo una piccola parte della rete



Internet e/o rete privata

ADSL line

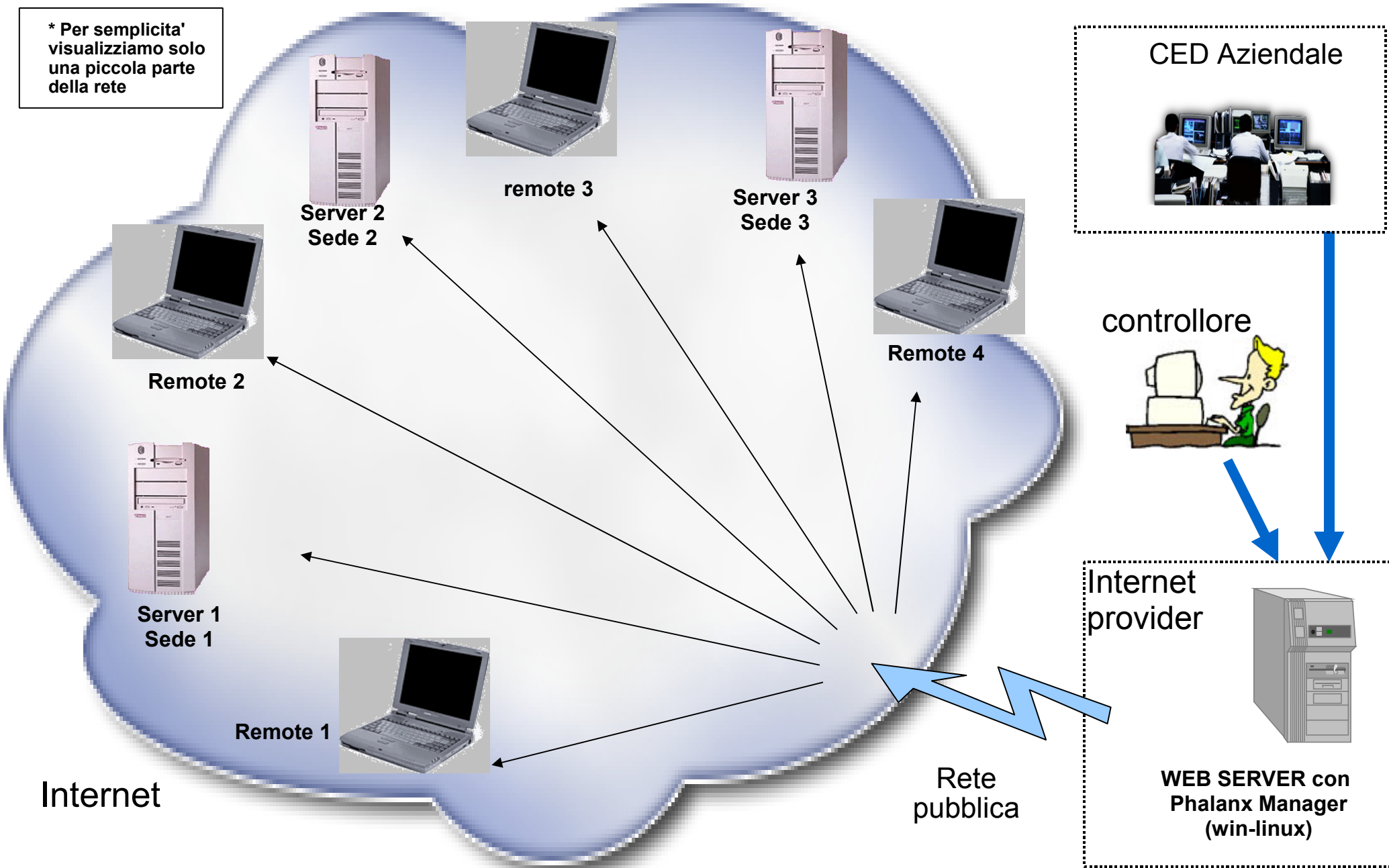
Apparato su rete pubblica (ind. statico)

Phalanx Manager (win-linux)

CED Aziendale

Soluzione Phalanx/Emon - Soluzione "esterna" internet

* Per semplicita' visualizziamo solo una piccola parte della rete



Internet

Rete pubblica

WEB SERVER con Phalanx Manager (win-linux)

Soluzione Phalanx/Emon – Console di tipo “lite”

The screenshot displays the Phalanx Lite web interface in a Windows Internet Explorer browser window. The browser title is "PHALANX - Inventory & Field Monitoring System - 2008/05/16 08:30:48 - Windows Internet Explorer". The address bar shows the URL "http://desc/casartor/login_su_file/EMON_INV/frame_main.php".

The interface includes a navigation menu with options like "Refresh", "Customer", "Ins.Subnet", "RESET", "MqrInfo", and "MqrConn". Below this, there are sections for "PINGcovery", "SNMPcovery", "HOSTcovery", "BaseCheck", "RouteRaw", and "DeepRaw".

The main content area is titled "View of PORT25 node type" and features a grid of 256 nodes (0-255). The grid is color-coded: green for active nodes, red for nodes with issues, and pink for nodes with specific configurations. The selected node is 217.172.4.

Below the grid, there is a "Show Detailed Report" section with a "Types of nodes" table. The table lists various node types and their corresponding icons:

Types of nodes	HOST	PORT80	PORT21	PORT25	PORT53	PORT110	PORT443
PING							
PORT993	SNMP_PING						
(all types)							

At the bottom left, there is a timestamp "2008/05/16 08:41:52" and a status message "status= customer selected".

Una delle console di amministrazione di Phalanx (in questo caso Phalanx Lite)

Si tratta generalmente di interfacce Web, altamente personalizzabili in quanto a estetica e funzionalità.

Uno dei punti “forti” e' proprio la versatilità, in quanto e' possibile implementare console “facili” (a “semafori”, ad esempio) quanto “difficili” (complesse console tecnologiche altamente dettagliate).

Soluzione Phalanx/Emon – Console di Monitoraggio per cliente

Monitoring Service - Desktop 2008-05-16 08:51:32 - Windows Internet Explorer

http://192.168.1.3/desktop_user.php

File Modifica Visualizza Preferiti Strumenti ?

Monitoring Service - Desktop 2008-05-16 08:51:32

Monitoraggio (Console Utente) 2008-05-16 08:51:32

www.google.com
www.msn.com
www.yahoo.com
www.interfree.it
www.digitalexpert.it
www.albacom.com
www.fastweb.it
www.tiscali.it
www.idealweb.it
www.idealweb.it
www.energit.it
casa
casa
www.telemaco.infocamere.it
www.php.net
www.php.net
www.hostingvirtuale.com
www.digitalexpert.it
www.descmain.it
smtp.idealweb.it
pop.idealweb.it
www.gemmo.com
www.gemmo.com
mail.gemmo.com
www.fast-mail.biz
www.fast-mail.biz
www.fast-mail.biz
www.ordine.avvocati.vi.it
www.l-systems.it
www.digitalexpert.it
www.faseaudio.com
www.adecco.it
www.gozzidegaspari.com
www.gozzidegaspari.com
www2.ordine.avvocati.vi.it
213.213.34.26
213.213.34.26
www.bogoni.com
www.adfor.it
85.32.103.9
www.venetoavvocati.it

Status OK, objects=41, filtered=41, data age=23 sec. mode=Icons,all Icons BoxText Text All Airt

http://192.168.1.3/dati/storico/www.descmain.it_HTTP

**Console di
monitoraggio.**

**Lo stato dei vari
sistemi e' reso
chiaramente visibile.**

**Cliccando sul singolo
nodo si ottiene la lista
storica degli eventi
ricevuti dal sistema di
monitoraggio per quel
singolo nodo.**

**Il sistema puo'
segnalare modifiche
in tempo reale tramite
diversi meccanismi di
paging, quali email,
sms, segnali acustici,
etc.**

PHALANX

*Utilizzi “fuori ordinanza”
della componente “agente”*

PHALANX – Gli ALTRI utilizzi “diversi”...

Altri utilizzi fuori ordinanza sono possibili...

- 1) lo sniffing dello user behaviour dal punto di vista delle connessioni tra il client e la rete (locale, wan, internet, dischi esterni, chiavette, siti, skype, emule, ftp, remotedesktop, etc)
- 2) l'intrusion detection (impulsivo, a tempo delimitato, a tempo indeterminato)
- 3) il supporto ad operazioni di change dinamico (quando il servizio “x” viene attivato sulla tal macchina allora riconfigura l'applicazione)
- 4) la sorveglianza del numero di interfacce di rete (nascita, morte, modifica caratteristiche)
- 5) la service surveillance... (sto a guardare una rete per vedere quand'e' che il furbone di turno attiva il chat server o il DHCP “aggiuntivo”)
- 6) in combinazione con EMON, predisporre appositi servizi di monitoraggio del contesto (ad esempio, quando un servizio mirrored va su, segnalarlo!)
- 7) il controllo “antifurto dati” (connessioni/disconnessioni di periferiche, chiavette USB, dischi esterni, alias di rete, printers, file transfert, file acceduti, etc)

PHALANX – Gli utilizzi “diversi”

Le technicalities inserite in Phalanx (agent/server) permettono di identificare “univocamente” il client su cui agente/server e' installato. Infatti, oltre al contesto di rete “catturato” da Phalanx, con la combinazione di informazioni ricavate dall'agente EMON e' possibile acquisire:

- 1) identificazione parametri fisici (biosinfo, processori, disk_size)
- 2) rilevazione “firme” hardware base (seriali dei dischi)
- 3) identificazione base sistema operativo
- 4) identificazione servizi/task attivi
- 5) parametri di contesto web (nel caso l'agente sia attivato come CGI (http GET da locale/remoto o consultato da EMON/IRM)
- 6) MAC della scheda di LAN
- 7) contesto di rete, sessioni di rete attive

Esempi

GET tabellare: http://desc/cgi-bin/emon_mgr.exe

GET internals: http://desc/cgi-bin/emon_mgr.exe?get_mon_var

PHALANX – Altri utilizzi “diversi”

Utilizzando Phalanx Manager e Agent in combinazione su una rete anche complessa, e' possibile ad esempio effettuare:

- 1) La mappatura completa del network context
- 2) la mappatura delle connessioni tra servizi/applicazioni in essere tra nodi
- 3) l'identificazione univoca di una macchina in rete
- 4) la validazione pervasiva passiva
(l'applicazione “x” sul nodo “a” NON puo' parlare con il servizio “y” della macchina “b”)
- 5) controllo “passivo” delle licenze
(plugin phalanx attivo sull'applicazione parla con manager Phalanx e lascia traccia)
- 6) controllo “attivo” delle licenze client-side
(L'agente Phalanx “butta giu'” l'applicazione che parla con un server non previsto)
- 7) controllo “attivo” delle licenze server-side
(l'agente Phalanx segnala le caratteristiche “spinte” del nodo e il server killa)
- 8)

PHALANX

*Informazioni rilevabili dagli agenti
(esempi)*

(indicative delle potenzialita', I dettagli rilevabili sono migliaia)

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 1: SKYPE

```
[{5C82DAE5-6EB0-4374-9254-BE3319BA4E82}]
  DisplayIcon: psz=(SZ) pszdata=C:\Programmi\Skype\Phone\Skype.exe
  PartnerCode: psz=(DWORD) pszdata=0 (dec=0)
  AuthorizedCDFPrefix: psz=(SZ) pszdata=
  Comments: psz=(SZ) pszdata=
  Contact: psz=(SZ) pszdata=
  DisplayVersion: psz=(SZ) pszdata=3.6.244
  HelpLink: psz=(EXPAND_SZ) pszdata=http://ui.skype.com/ui/0/3.6.0.244/it/help
  HelpTelephone: psz=(SZ) pszdata=
  InstallDate: psz=(SZ) pszdata=20080101
  InstallLocation: psz=(SZ) pszdata=C:\Programmi\Skype\
  InstallSource: psz=(SZ) pszdata=C:\Documents and Settings\All Users\Dati applicazioni\Skype\
                                     {5C82DAE5-6EB0-4374-9254-BE3319BA4E82}\
  ModifyPath: psz=(EXPAND_SZ) pszdata=MsiExec.exe /X{5C82DAE5-6EB0-4374-9254-BE3319BA4E82}
  NoModify: psz=(DWORD) pszdata=1 (dec=1)
  NoRepair: psz=(DWORD) pszdata=1 (dec=1)
  Publisher: psz=(SZ) pszdata=Skype Technologies S.A.
  Readme: psz=(SZ) pszdata=
  Size: psz=(DWORD) pszdata=6400 (dec=25600)
  EstimatedSize: psz=(DWORD) pszdata=7636 (dec=30262)
  UninstallString: psz=(EXPAND_SZ) pszdata=MsiExec.exe /X{5C82DAE5-6EB0-4374-9254-BE3319BA4E82}
  URLInfoAbout: psz=(SZ) pszdata=http://www.skype.com
  URLUpdateInfo: psz=(SZ) pszdata=http://ui.skype.com/ui/0/3.6.0.244/it/latestversion
  VersionMajor: psz=(DWORD) pszdata=3 (dec=3)
  VersionMinor: psz=(DWORD) pszdata=6 (dec=6)
  WindowsInstaller: psz=(DWORD) pszdata=1 (dec=1)
  Version: psz=(DWORD) pszdata=30600f4 (dec=50725108)
  Language: psz=(DWORD) pszdata=409 (dec=1033)
  DisplayName: psz=(SZ) pszdata=Skype101
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 2: SITI VISITATI DALL'UTENTE

[TypedURLs]

```
url1: psz=(SZ) pszdata=http://search.live.com/results.aspx?q="international+company+marketing
+service+and+research"&src=IE-Address
url2: psz=(SZ) pszdata=http://www.aruba.it/
url3: psz=(SZ) pszdata=http://www.surfwax.com/
url4: psz=(SZ) pszdata=http://www.libero.it/
url5: psz=(SZ) pszdata=http://www.devx.com/getHelpOn/Door/15766
url6: psz=(SZ) pszdata=file:///c:/temp/prova_csv.htm
url7: psz=(SZ) pszdata=http://desc/cgi-bin/emon_mgr.exe
url8: psz=(SZ) pszdata=http://desc/cgi-bin/emon_mgr.exe?get_mon_var
url9: psz=(SZ) pszdata=http://desc/casartor/login_su_file/EMON_INV/tools/emon_mgr.exe?
get_mon_var
url10: psz=(SZ) pszdata=http://desc/casartor/login_su_file/EMON_INV/node_info.php
url11: psz=(SZ) pszdata=http://desc/casartor/login_su_file/EMON_INV/tools/emon_mgr.exe
url12: psz=(SZ) pszdata=monitoring
url13: psz=(SZ) pszdata=http://www.alice.it/
url14: psz=(SZ) pszdata=http://casartor.dyndns.org/desktop_user.php
url15: psz=(SZ) pszdata=http://www.luigidemarchi.it/
url16: psz=(SZ) pszdata=http://www.unibas.it/utenti
url17: psz=(SZ) pszdata=http://www.unibas.it/utenti/ogdc
url18: psz=(SZ) pszdata=http://www.unibas.it/utenti/ogdc/scidem.html
url19: psz=(SZ) pszdata=http://www.unibas.it/
url20: psz=(SZ) pszdata=http://www2.unibas.it/
url21: psz=(SZ) pszdata=http://www.ilvirusinventato.it/
url22: psz=(SZ) pszdata=http://ndyguild.com/
url23: psz=(SZ) pszdata=http://ndyguild.com/css/ubibanca1.it.html
url24: psz=(SZ) pszdata=http://www.digitalexpert.it/
url25: psz=(SZ) pszdata=http://www.google.it/search?num=100&hl=it&q=computers
+vicenza&btnG=Cerca&meta=
```


PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 4: DECODER VIDEO DI QUICKTIME PER DVX

```
[{C546BD25-3E55-4C9B-88BC-F1DAFBFE1928}]
```

```
[1.0]
```

```
: psz=(SZ) pszdata=QuickTimeVideoDecoder 1.0 Type Library
```

```
[0]
```

```
[win32]
```

```
: psz=(SZ) pszdata=C:\Programmi\DivX\DivX Common Filters\gzHF330.ddc
```

```
[FLAGS]
```

```
: psz=(SZ) pszdata=0
```

```
[HELPPDIR]
```

```
: psz=(SZ) pszdata=
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 5: HARD DISK INFOS (1/2)

```
[DiskHitachi_HDS721616PLA380_____P22OABEA]
[5&3b379d3&0&0.0.0]
  DeviceDesc: psz=(SZ) pszdata=Unità disco
  LocationInformation: psz=(SZ) pszdata=0
  Capabilities: psz=(DWORD) pszdata=0 (dec=0)
  UINumber: psz=(DWORD) pszdata=0 (dec=0)
  HardwareID: psz=(MULTI_SZ) pszdata=IDE\DiskHitachi_HDS721616PLA380_____
                                          P22OABEA\0IDE\Hitachi_HDS721616PLA380_____
                                          P22OABEA\0IDE\DiskHitachi_HDS721616PLA380_____
                                          \0Hitachi_HDS721616PLA380_____P22OABEA\0GenDisk\0\0
  CompatibleIDs: psz=(MULTI_SZ) pszdata=GenDisk\0\0
  ClassGUID: psz=(SZ) pszdata={4D36E967-E325-11CE-BFC1-08002BE10318}
  Service: psz=(SZ) pszdata=disk
  ConfigFlags: psz=(DWORD) pszdata=0 (dec=0)
  Driver: psz=(SZ) pszdata={4D36E967-E325-11CE-BFC1-08002BE10318}\0013
  Class: psz=(SZ) pszdata=DiskDrive
  Mfg: psz=(SZ) pszdata=(unità disco standard)
  FriendlyName: psz=(SZ) pszdata=Hitachi HDS721616PLA380
  [Device Parameters]
  [LogConf]
  [Control]
    ActiveService: psz=(SZ) pszdata=Disk
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 5: HARD DISK INFOS (2/2)

```
[DiskSAMSUNG_HD080HJ/P_____ZH100-34]
[5&166d2a78&0&0.0.0]
  DeviceDesc: psz=(SZ) pszdata=Unità disco
  LocationInformation: psz=(SZ) pszdata=0
  Capabilities: psz=(DWORD) pszdata=0 (dec=0)
  UINumber: psz=(DWORD) pszdata=0 (dec=0)
  HardwareID: psz=(MULTI_SZ) pszdata=IDE\DiskSAMSUNG_HD080HJ/P_____
                                     ZH100-34\0IDE\SAMSUNG_HD080HJ/P_____
                                     ZH100-34\0IDE\DiskSAMSUNG_HD080HJ/P_____
                                     \0SAMSUNG_HD080HJ/P_____ZH100-34\0GenDisk\0\0
CompatibleIDs: psz=(MULTI_SZ) pszdata=GenDisk\0\0
ClassGUID: psz=(SZ) pszdata={4D36E967-E325-11CE-BFC1-08002BE10318}
Service: psz=(SZ) pszdata=disk
ConfigFlags: psz=(DWORD) pszdata=0 (dec=0)
Driver: psz=(SZ) pszdata={4D36E967-E325-11CE-BFC1-08002BE10318}\0002
Class: psz=(SZ) pszdata=DiskDrive
Mfg: psz=(SZ) pszdata=(unità disco standard)
FriendlyName: psz=(SZ) pszdata=SAMSUNG HD080HJ/P
[Device Parameters]
[LogConf]
[Control]
  ActiveService: psz=(SZ) pszdata=Disk
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 6: DETECT DI HYPERTRANSPORT BRIDGE NVIDIA

```
[VEN_10DE&DEV_02FA&SUBSYS_81D71043&REV_A2]
  [3&267a616a&0&01]
    DeviceDesc: psz=(SZ) pszdata=nForce HyperTransport Bridge
    LocationInformation: psz=(SZ) pszdata=Bus PCI 0, periferica 0, funzione 1
    Capabilities: psz=(DWORD) pszdata=0 (dec=0)
    HardwareID: psz=(MULTI_SZ) pszdata=PCI\VEN_10DE&DEV_02FA&SUBSYS_81D71043&
      REV_A2\0PCI\VEN_10DE&DEV_02FA&SUBSYS_81D71043\0PCI\VEN_10DE&
      DEV_02FA&CC_050000\0PCI\VEN_10DE&DEV_02FA&CC_0500\0\0
    CompatibleIDs: psz=(MULTI_SZ) pszdata=PCI\VEN_10DE&DEV_02FA&
      REV_A2\0PCI\VEN_10DE&DEV_02FA\0PCI\VEN_10DE&
      CC_050000\0PCI\VEN_10DE&
      CC_0500\0PCI\VEN_10DE\0PCI\CC_050000\0PCI\CC_0500\0\0
    ClassGUID: psz=(SZ) pszdata={4D36E97D-E325-11CE-BFC1-08002BE10318}
    Class: psz=(SZ) pszdata=System
    Driver: psz=(SZ) pszdata={4D36E97D-E325-11CE-BFC1-08002BE10318}\0016
    Mfg: psz=(SZ) pszdata=NVIDIA
    ConfigFlags: psz=(DWORD) pszdata=0 (dec=0)
    [LogConf]
    [Control]
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 7: Detect di Fast User Switching

```
[LEGACY_FASTUSERSWITCHINGCOMPATIBILITY]
NextInstance: psz=(DWORD) pszdata=1 (dec=1)
[0000]
  Service: psz=(SZ) pszdata=FastUserSwitchingCompatibility
  Legacy: psz=(DWORD) pszdata=1 (dec=1)
  ConfigFlags: psz=(DWORD) pszdata=0 (dec=0)
  Class: psz=(SZ) pszdata=LegacyDriver
  ClassGUID: psz=(SZ) pszdata={8ECC055D-047F-11D1-A537-0000F8753ED1}
  DeviceDesc: psz=(SZ) pszdata=Compatibilità di Cambio rapido utente
  [Control]
    ActiveService: psz=(SZ) pszdata=FastUserSwitchingCompatibility
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 8: Detect stampante Epson (su porta USB)

```
[Vid_04b8&Pid_0820&MI_00]
  [6&ad0ae71&0&0000]
    DeviceDesc: psz=(SZ) pszdata=EPSON Stylus CX4100/DX4200
    Capabilities: psz=(DWORD) pszdata=84 (dec=132)
    UINumber: psz=(DWORD) pszdata=0 (dec=0)
    HardwareID: psz=(MULTI_SZ) pszdata=USB\Vid_04b8&Pid_0820&Rev_0100&
        MI_00\0USB\Vid_04b8&Pid_0820&MI_00\0\0
    CompatibleIDs: psz=(MULTI_SZ) pszdata=USB\Class_ff&SubClass_ff&
        Prot_ff\0USB\Class_ff&SubClass_ff\0USB\Class_ff\0\0
    ClassGUID: psz=(SZ) pszdata={6BDD1FC6-810F-11D0-BEC7-08002BE2092F}
    Class: psz=(SZ) pszdata=Image
    Driver: psz=(SZ) pszdata={6BDD1FC6-810F-11D0-BEC7-08002BE2092F}\0000
    Mfg: psz=(SZ) pszdata=EPSON
    Service: psz=(SZ) pszdata=usbscan
    ConfigFlags: psz=(DWORD) pszdata=0 (dec=0)
    FriendlyName: psz=(SZ) pszdata=EPSON Stylus CX4100/DX4200
    [Device Parameters]
      ExtPropDescSemaphore: psz=(DWORD) pszdata=1 (dec=1)
    [LogConf]
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 9: Traccia utilizzo Antivirus Kaspersky via web

[KasperskyLab]

[KAVWebScanner]

```
UseDatabases: psz=(DWORD) pszdata=1 (dec=1)
NeutralizeTrojans: psz=(DWORD) pszdata=1 (dec=1)
ScanArchives: psz=(DWORD) pszdata=1 (dec=1)
ScanPackedExecutables: psz=(DWORD) pszdata=1 (dec=1)
ScanEmailFiles: psz=(DWORD) pszdata=1 (dec=1)
ScanDamagedFiles: psz=(DWORD) pszdata=0 (dec=0)
UseHeuristics: psz=(DWORD) pszdata=1 (dec=1)
ScanOnlyInfectableObjects: psz=(DWORD) pszdata=0 (dec=0)
ScanCertainFileExtensions: psz=(DWORD) pszdata=0 (dec=0)
StatisticsPrompt: psz=(DWORD) pszdata=1 (dec=1)
StatisticsEnable: psz=(DWORD) pszdata=1 (dec=1)
UniqueCode: psz=(SZ) pszdata=c3f8a072-d4ea-4231-8e92-1827476db029
ScanExtensions: psz=(SZ) pszdata=.EXE.COM.OVL.PRG.SCR.VXD.BIN.BOO.TD0
                .XLS.DOC.MDB.PPT.VBS.BAT.SAM.JS.HTM.DLL.POT.DRV.IMG.OVR.386
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 10: Traccia utilizzo chiavetta USB JetFlash

```
[##?#USBSTOR#Disk&Ven_JetFlash&Prod_TS1GJFV30&Rev_8.07#D3OHXNOY&0
      #{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
DeviceInstance: psz=(SZ)
pszdata=USBSTOR\Disk&Ven_JetFlash&Prod_TS1GJFV30&Rev_8.07\D3OHXNOY&0

[#] SymbolicLink: psz=(SZ) pszdata=\\?\USBSTOR#Disk&Ven_JetFlash&Prod_TS1GJFV30&Rev_8.07
      #D3OHXNOY&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

[Control]
  Linked: psz=(DWORD) pszdata=0 (dec=0)

[Control]
  ReferenceCount: psz=(DWORD) pszdata=0 (dec=0)
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 11: Traccia inserimento Hard Disk IDE aggiuntivo SAMSUNG

```
[##?#IDE#DiskSAMSUNG_HD080HJ#P_____ZH100-34#5&166d2a78&0&0.0.0#{53f56307-  
b6bf-11d0-94f2-00a0c91efb8b}]  
DeviceInstance: psz=(SZ) pszdata=IDE\DiskSAMSUNG_HD080HJ/P_____ZH100-34\  
5&166d2a78&0&0.0.0  
  
[#]  
SymbolicLink: psz=(SZ) pszdata=\\?\IDE#DiskSAMSUNG_HD080HJ#P_____  
ZH100-34#5&166d2a78&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}  
  
[Control]  
Linked: psz=(DWORD) pszdata=1 (dec=1)  
  
[Control]  
ReferenceCount: psz=(DWORD) pszdata=1 (dec=1)
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 12: Traccia inserimento stampante USB EPSON Stylus DX4450

[Driver]

[EPSON Stylus DX4400 Series]

```
InstallPath: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3
ModelID: psz=(SZ) pszdata=Stylus DX4400
E_SRUN: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FARNCAE.EXE
E_SENV: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FARNCAE.EXE
E_SICN: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FATICA.EXE
E_STMS: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FAMTCAE.EXE
E_SRCV: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FBCSCAE.EXE
Profile: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FAIFCAE.DAT
STMSRV_NAME: psz=(SZ) pszdata=E_S40RP7.EXE
STMSRV_INTERNALNAME: psz=(SZ) pszdata=EPSON_PM_RPCV4_01
EBAPI32: psz=(SZ) pszdata=E_FBA6CAE.DLL
LocalMonitoringTimer: psz=(SZ) pszdata=5
NetworkMonitoringTimer: psz=(SZ) pszdata=20
DepExe: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FARNCAE.EXE
SAgentType: psz=(DWORD) pszdata=1 (dec=1)
SAgentControlDll: psz=(SZ) pszdata=E_FBAGCAE.DLL
MapFileName: psz=(SZ) pszdata=StmV5MapFile_Ink
ADDNETWORK_NAME: psz=(SZ) pszdata=E_Addnet.exe
ADDNET_SET_Path: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_SAG4ST.EXE
SMRT_OLICOS: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FASOCAE.DLL
ProgressDllName: psz=(SZ) pszdata=E_FGRCCA.E.DLL
EBAPI_VERSION: psz=(DWORD) pszdata=5 (dec=5)
DriverUpdateName: psz=(SZ) pszdata=C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_DUPA20.EXE
LanguageMon: psz=(SZ) pszdata=EPSON Stylus DX4400 Series 32MonitorBE
LanguageMonDll: psz=(SZ) pszdata=E_FLBCAE.DLL
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 13: Traccia utilizzo disco remoto (disco X: del server SRV1274, share “documenti”)

[Network]

[x]

```
RemotePath: psz=(SZ) pszdata=\\SRV1274\documenti
UserName: psz=(SZ) pszdata=
ProviderName: psz=(SZ) pszdata=Rete di Microsoft Windows
ProviderType: psz=(DWORD) pszdata=20000 (dec=131072)
ConnectionType: psz=(DWORD) pszdata=1 (dec=1)
DeferFlags: psz=(DWORD) pszdata=4 (dec=4)
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 14: Traccia utilizzo prodotto Skype

```
[callto]
  : psz=(SZ) pszdata=URL:Callto Protocol
  EditFlags: psz=(BINARY) pszdata=02 00 00 00
  URL Protocol: psz=(SZ) pszdata=

[DefaultIcon]
  : psz=(SZ) pszdata="C:\Programmi\Skype\Phone\Skype.exe",0

[shell]
  [open]
    [command]
      : psz=(SZ) pszdata="C:\Programmi\Skype\Phone\Skype.exe" "/callto:%1"
```

PHALANX – funzionalita' del kernel “agente”...

ESEMPIO 15: Traccia utilizzo file compressi (ZIP) un po' sospetti....

```
[zip]
a: psz=(SZ) pszdata=C:\TEMP\sources\KeyloggerMore3HtmlPeeker.zip
b: psz=(SZ) pszdata=C:\TEMP\sources\KeyloggerMore3_Sample.zip
c: psz=(SZ) pszdata=C:\TEMP\sources\scan.zip
d: psz=(SZ) pszdata=C:\TEMP\sources\hwscan.zip
e: psz=(SZ) pszdata=C:\TEMP\sources\RegTip_Demo.zip
f: psz=(SZ) pszdata=C:\TEMP\sources\KeyLoggerMore_Sample.zip
g: psz=(SZ) pszdata=C:\TEMP\sources\KeyLoggerMore2Sample.zip
h: psz=(SZ) pszdata=C:\TEMP\sources\regscanner.zip
```

PHALANX

*Samples di output delle funzioni
base e custom dell'agente*

(alcuni oggetti contenuti negli agenti e relativi outputs)

PHALANX – funzionalita' del kernel “agente”...

Oggetto: conn_type

Output:

EMON Agent - (c) 2007 - DigitalExpert

Num Entries: 2

```
Index:      2
InterfaceName[0]:
Description[0]:      NVIDIA nForce Networking Controller
Type[0]:      Ethernet
Mtu[0]:      1500
Speed[0]:      100000000
Physical Addr: 00-15-F2-DF-2E-5C
Admin Status[0]:      1
Oper Status[0]:      Operational
```

```
Index:      1
InterfaceName[1]:
Description[1]:      MS TCP Loopback interface
Type[1]:      Software Lookback
Mtu[1]:      1520
Speed[1]:      10000000
Physical Addr:
Admin Status[1]:      1
Oper Status[1]:      Operational
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: tcp_table (connessioni applicative riversate su tasklist manager)

Output:

EMON Agent - (c) 2007 - DigitalExpert

Communications between node and others systems (on TCP/IP)
Found 18 entries (local and/or remote)

TCP	State	Status String	Source IP Addr	LPort	Target IP Addr	RPort
0	2	LISTEN	0.0.0.0	80	0.0.0.0	6184
1	2	LISTEN	0.0.0.0	135	0.0.0.0	2192
2	2	LISTEN	0.0.0.0	443	0.0.0.0	34956
3	2	LISTEN	0.0.0.0	445	0.0.0.0	24596
4	2	LISTEN	0.0.0.0	15475	0.0.0.0	26794
5	5	ESTABLISHED	127.0.0.1	1043	127.0.0.1	1044
6	5	ESTABLISHED	127.0.0.1	1044	127.0.0.1	1043
7	5	ESTABLISHED	127.0.0.1	1045	127.0.0.1	1046
8	5	ESTABLISHED	127.0.0.1	1046	127.0.0.1	1045
9	2	LISTEN	192.168.1.5	139	0.0.0.0	63641
10	5	ESTABLISHED	192.168.1.5	1379	80.180.61.243	31359
11	5	ESTABLISHED	192.168.1.5	2887	79.140.80.56	80
12	5	ESTABLISHED	192.168.1.5	2901	79.140.80.27	80
13	8	CLOSE-WAIT	192.168.1.5	2917	151.1.162.20	80
14	8	CLOSE-WAIT	192.168.1.5	2918	151.1.162.20	80
15	8	CLOSE-WAIT	192.168.1.5	2919	192.168.1.6	80
16	8	CLOSE-WAIT	192.168.1.5	2920	192.168.1.6	80
17	3	SYN-SENT	192.168.1.5	2921	80.180.77.140	1483

PHALANX – funzionalita' del kernel “agente”...

Oggetto: snmp_ping

Output:

```
EMON Agent - (c) 2007 - DigitalExpert
```

```
SNMP PINGER - RAW TYPE
```

```
Destination address=192.168.1.1
```

```
Bytes sent to 192.168.1.1: 39
```

```
Bytes received from 192.168.1.1: 52
```

```
SNMP RICONOSCIUTO
```

```
STRING=0,.0.....publicç,..!.0,..0,.....+.C..”kt.
```

```
data=30 82 00 30 02 01 00 04 06 70 75 62 6c 69 63 a2
```

```
data=82 00 21 02 01 01 02 01 00 02 01 00 30 82 00 14
```

```
data=30 82 00 10 06 08 2b 06 01 02 01 01 03 00 43 04
```

```
data=00 93 6b 74 00
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_processlist (w/connections!)

Type	Local	Remote	Status	PID	Pid Name
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	704	Skype
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	708	Svchost
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	704	Skype
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	*
TCP	0.0.0.0:15475	0.0.0.0:0	LISTENING	704	Skype
TCP	192.168.1.5:139	0.0.0.0:0	LISTENING	4	*
TCP	127.0.0.1:1043	127.0.0.1:1044	ESTABLISHED	344	firefox
TCP	127.0.0.1:1044	127.0.0.1:1043	ESTABLISHED	344	firefox
TCP	192.168.1.5:3794	206.190.50.59:80	TIME_WAIT	1780	Iexplore
UDP	0.0.0.0:1064	*:*		824	Svchost
UDP	0.0.0.0:500	*:*		504	LSASS
UDP	0.0.0.0:4500	*:*		504	LSASS
UDP	0.0.0.0:1437	*:*		824	svchost
UDP	0.0.0.0:15475	*:*		704	Skype
UDP	0.0.0.0:445	*:*		4	*
UDP	0.0.0.0:1025	*:*		824	Svchost
UDP	0.0.0.0:1056	*:*		824	Svchost
UDP	127.0.0.1:1378	*:*		704	Skype
UDP	127.0.0.1:4217	*:*		1780	Iexplore
UDP	127.0.0.1:1900	*:*		944	svchost
UDP	127.0.0.1:123	*:*		768	svchost
UDP	192.168.1.5:1900	*:*		944	svchost
UDP	192.168.1.5:138	*:*		4	*
UDP	192.168.1.5:123	*:*		768	svchost
UDP	192.168.1.5:137	*:*		4	*

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_network_params

Output:

```
EMON Agent - (c) 2007 - DigitalExpert
```

```
NetInfo:
```

```
Host Name: olidata-zetta
```

```
Domain Name:
```

```
DNS Servers:
```

```
    192.168.1.1
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_ip_info

Output:

```
EMON Agent - (c) 2007 - DigitalExpert  
GET IP INFO - a TPC Information tool
```

```
INFO FOR HOST www.google.com
```

```
Function returned:
```

```
  Official name: www.l.google.com
```

```
  Alternate names: \-
```

```
  Address type: AF_INET
```

```
  Address length: 4
```

```
  First IP Address: 209.85.129.99
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_interface_info

Output:

```
EMON Agent - (c) 2007 - DigitalExpert
```

```
Network Adapter Inventory
```

```
Number of Adapters: 1
```

```
Adapter Index[0]: 2
```

```
Adapter Name[0]: \DEVICE\TCPIP_{AC25D631-C746-49A7-8753-C5A55C788F42}
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_addr_table

Output:

EMON Agent - (c) 2007 - DigitalExpert

Network Entries: 2

Interface Index[0]: 2

IP Address[0]: 192.168.1.5

Subnet Mask[0]: 255.255.255.0

BroadCast[0]: 1.0.0.0 (1)

Reassembly size[0]: 65535

Type and State[0]: Primary IP Address

Interface Index[1]: 1

IP Address[1]: 127.0.0.1

Subnet Mask[1]: 255.0.0.0

BroadCast[1]: 1.0.0.0 (1)

Reassembly size[1]: 65535

Type and State[1]: Primary IP Address

PHALANX – funzionalita' del kernel “agente”...

Oggetto: get_adapter_info

Output:

```
EMON Agent - (c) 2007 - DigitalExpert
```

```
GET ADAPTER INFO
```

```
ComboIndex: 5d
```

```
Adapter Name: {AC25D631-C746-49A7-8753-C5A55C788F42}
```

```
Adapter Desc: NVIDIA nForce Networking Controller
```

```
Adapter Addr: 00-15-F2-DF-2E-5C
```

```
Index: 2
```

```
Type: Ethernet
```

```
IP Address: 192.168.1.5
```

```
IP Mask: 255.255.255.0
```

```
Gateway: 170.204.187.221
```

```
DHCP Enabled: No
```

```
Have Wins: No
```

PHALANX – funzionalita' del kernel “agente”...

Oggetto: friendly_conn_descr

Output:

EMON Agent - (c) 2007 - DigitalExpert

Connection(s):

Name: Connessione alla rete locale (LAN)
Description: NVIDIA nForce Networking Controller

Name: MS TCP Loopback interface
Description: MS TCP Loopback interface

PHALANX – funzionalita' del kernel “agente”...

Oggetto: software_inventory form local data presence

Output:

<object deleted>

PHALANX – funzionalita' del kernel “agente”...

Oggetto: software_inventory form user network context

Output:

<object deleted>

PHALANX – funzionalita' del kernel “agente”...

Oggetto: software_inventory (hidden objects NOT INCLUDED)

Output:

<object deleted>

PHALANX – funzionalita' del kernel “agente”...

Oggetto: software_inventory (hidden objects INCLUDED)

Output:

<object deleted>

PHALANX – funzionalita' del kernel “agente”...

Oggetto: software_inventory (CUSTOMER PREFERENCES)

Output:

<object deleted>

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*