Lezione 5:

THE CLOUD

Presentazioni:

- Renato Mainetti (Grafica Programmazione Reti)
- Mail per info: renato.mainetti@gmail.com
  (grande fantasia)
- Sito Web da cui scaricare le slide :
  http://tamberlo.altervista.org

lista

- Definizione cloud
- A cosa serve
- Servizi vari, host computing etc
- Normativa, privacy, sicurezza?
- Cifrare I dati
- Chi offre cloud ?
- HomeMade…

Cloud Computing:

Con il termine inglese **cloud computing** si indica un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente,
di memorizzare/archiviare e/o elaborare dati grazie all'utilizzo di
risorse hardware/software distribuite e virtualizzate in Rete.

Old Style:

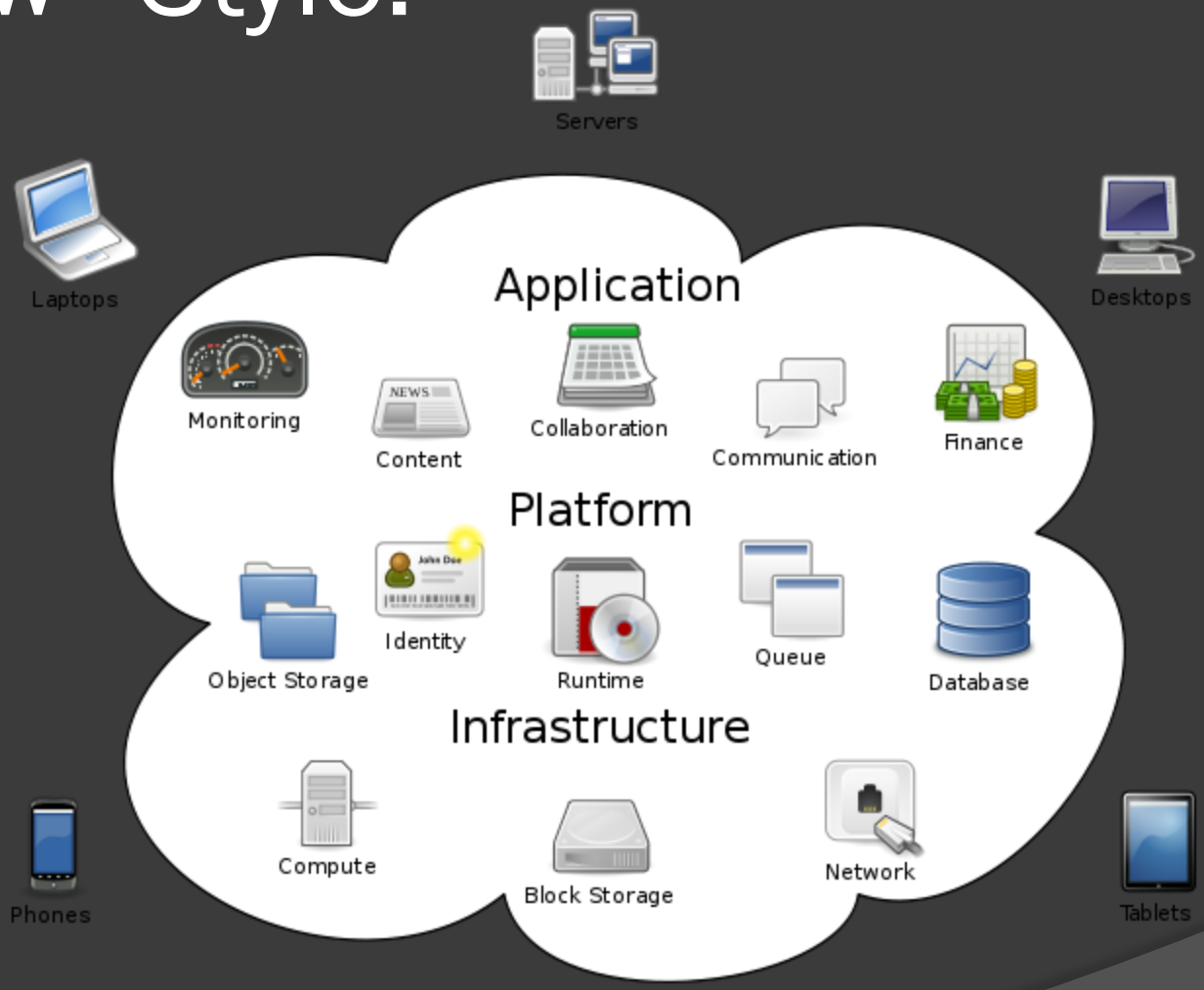
Utilizzando varie tipologie di unità di elaborazione (CPU), memorie di massa fisse o mobili come ram, dischi rigidi interni o esterni, Cd/DVD, chiavi USB, eccetera, un computer è in grado di elaborare, archiviare, recuperare programmi e dati.

“New” Style:

Nel caso di computer collegati in rete locale (lan) o geografica (wan) la possibilità di elaborazione/archiviazione/recupero può essere estesa ad altri computer e dispositivi remoti dislocati sulla rete stessa.

Sfruttando la tecnologia del *cloud computing* gli utenti collegati ad un *cloud provider* possono svolgere tutte queste mansioni, anche tramite un semplice internet browser. Possono, ad esempio, utilizzare software remoti non direttamente installati sul proprio computer e salvare dati su memorie di massa on-line predisposte dal provider stesso (sfruttando sia reti via cavo che senza fili).

“New” Style:


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Object Storage
Identity
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network
Phones
Tablets
Cloud Computing

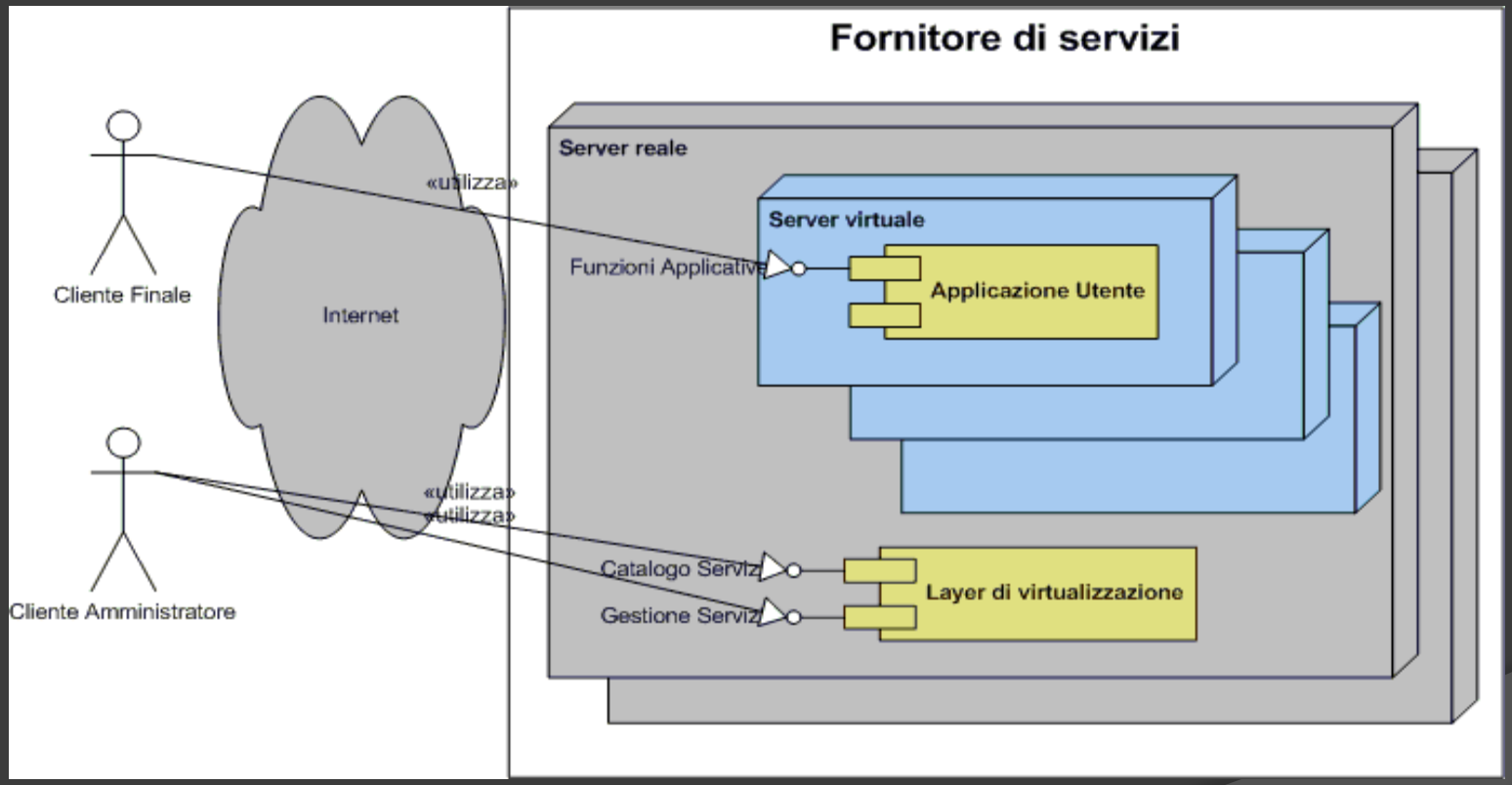
The Cloud... 3 tipi!

Nonostante il termine sia piuttosto vago e sembri essere utilizzato in diversi contesti con significati differenti tra loro, si possono distinguere tre tipologie fondamentali di *cloud Computing*:

- SaaS (*Software as a Service*) - Consiste nell'utilizzo di programmi in remoto, spesso attraverso un server web.

- PaaS (*Platform as a Service*) - È simile al SaaS, ma, invece che uno o più programmi singoli, viene eseguita in remoto una piattaforma software che può essere costituita da diversi servizi, programmi, librerie, etc.
- IaaS (*Infrastructure as a Service*) - Utilizzo di risorse hardware in remoto. Questo tipo di Cloud è quasi un sinonimo di Grid Computing, ma con una caratteristica imprescindibile: le risorse vengono utilizzate su richiesta o domanda al momento in cui un cliente ne ha bisogno, non vengono assegnate a prescindere dal loro utilizzo effettivo.

Chi e Come? Attori della nuvola



Chi e Come? Attori della nuvola

Casi d'uso:

- *Fornitore di servizi* (*cloud provider*)– Offre servizi (server virtuali, storage, applicazioni complete) generalmente secondo un modello "pay-per-use";

- *Cliente amministratore* – Sceglie e configura i servizi offerti dal fornitore, generalmente offrendo un valore aggiunto come ad esempio applicazioni software;

- *Cliente finale* – Utilizza i servizi opportunamente configurati dal cliente amministratore.

In determinati casi d'uso il cliente amministratore e il cliente finale possono coincidere. Ad esempio un cliente può utilizzare un servizio di storage per effettuare il backup dei propri dati, in questo caso il cliente finale provvede a configurare e utilizzare il servizio.

Pay per Use?

- Cloud computing typically does not involve long-term commitment to use the computing infrastructure. The vendor does not enforce long-term usage of services.
- Cloud computing does not involve any significant capital expenditure for the organization. Unlike traditional IT infrastructure, in cloud computing organizations just use the computing services without procuring it. In some sense cloud computing involves renting the computing resources instead of buying them.

Quando usare il Cloud?

- Availability of large computing infrastructure on need basis: Cloud vendors provide appearance of infinite computing infrastructure availability. This is available to organizations on need basis. This ensures that organizations do not need to set up servers for their peak requirements. As an example consider the official Wimbledon site. The site gets extremely high traffic in the two weeks when the championship happens. For this two weeks period this site will have high server usage. For rest of the year the site will need to only pay for the reduced usage. In general organizations do not need to bear the cost of computing infrastructure for their peak loads. The usage of computing resources can be increased or reduced on need basis, is called elastic computing.

Quando non usare il Cloud?

Sicurezza informatica e **privacy** degli utenti:

- Utilizzare un servizio di *cloud computing* per memorizzare dati personali o sensibili, espone l'utente a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle *Server Farms* di aziende che spesso risiedono in uno stato diverso da quello dell'utente. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.
- Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'utente, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.
- Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

Quando non usare il Cloud?

Continuità del servizio offerto: (anelli deboli della catena)

- Delegando a un servizio esterno la gestione dei dati e la loro elaborazione l'utente si trova fortemente limitato nel caso in cui i suddetti servizi non siano operativi (*out of service*). Un eventuale malfunzionamento inoltre colpirebbe un numero molto elevato di persone contemporaneamente dato che questi sono servizi condivisi. Anche se i migliori servizi di *cloud computing* utilizzano architetture ridondate e personale qualificato al fine di evitare malfunzionamenti dei sistema e ridurre la probabilità di guasti visibili dall'utente finale, non eliminano del tutto il problema. Bisogna anche considerare che tutto si basa sulla possibilità di avere una connessione Internet ad alta velocità sia in download che in upload e che anche nel caso di una interruzione della connessione dovuta al proprio Internet Service Provider/ISP si ha la completa paralisi delle attività.

Quando non usare il Cloud?

02 Settembre 2009

Gmail è stato irraggiungibile **dalle 12:30 p.m. PDT** (orario del pacifico, circa le **20:30 italiane**) per tornare attivo solo verso le 2:30 p.m., due ore dopo. I disserivizi creati sono stati ovviamente di vario tipo, andando a creare problemi non solo a chi utilizza gmail per il tempo libero o come casella personale, ma soprattutto a coloro che utilizzano Gmail come strumento di lavoro.

Google, attraverso il suo blog ufficiale nel corso della giornata ha così dato spiegazione dell'accaduto: *"As we now know, we had slightly underestimated the load which some recent changes (ironically, some designed to improve service availability) placed on the request routers -- servers which direct web queries to the appropriate Gmail server for response"*. Alla base di tutto quindi una stima errata circa le risorse di sistema ha reso completamente inaccessibile il popolare servizio di mail.

Quando non usare il Cloud?

Difficoltà di migrazione dei dati nel caso di un eventuale cambio del gestore dei servizi *cloud*:

- Non esistendo uno standard definito tra i gestori dei servizi un eventuale cambio di operatore risulta estremamente complesso. Tutto ciò risulterebbe estremamente dannoso in caso di fallimento del gestore dei servizi cui ci si è affidati

Crittografia:

- La crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente *crittogramma*.

Cifrario di Cesare:

- **sovrapposizione di due alfabeti :**

A B C D E F G H I L M N O P Q R S T U V Z
U V Z A B C D E F G H I L M N O P Q R S T

Facciamo un esempio concreto : come diventerebbe il seguente messaggio?
CIAO COME STAI ?

Cifrario di Cesare:

- **sovrapposizione di due alfabeti :**

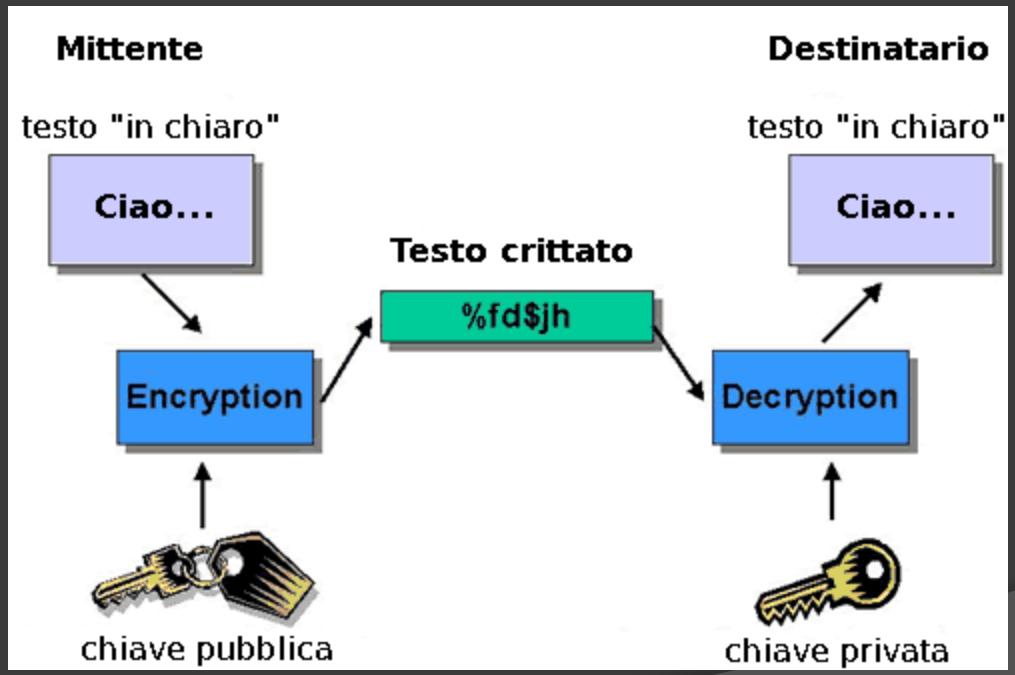
A B C D E F G H I L M N O P Q R S T U V Z
U V Z A B C D E F G H I L M N O P Q R S T

Facciamo un esempio concreto : come diventerebbe il seguente messaggio?
CIAO COME STAI ?

ZFUL ZLHB PQUF ?

Cifratura Simmetrica/Asimmetrica

- Simmetrica -> stessa chiave
- Asimmetrica Chiave Pubblica e Privata



Usiamo Cesare? Decisamente NO!

Le chiavi pubbliche si basano sulla creazione di un problema matematico molto difficile da risolvere senza informazioni, ma che con l'utilizzo di alcune informazioni (la chiave) diventa di semplice e rapida risoluzione. L'utente distribuisce pubblicamente il problema (la chiave pubblica) e tiene nascoste le informazioni aggiuntive (la chiave privata). Il problema viene utilizzato per mescolare i messaggi da trasmettere in modo da non renderli comprensibili.

Cifratura:

Tenuto conto della condivisione di risorse prevista nelle cloud, l'utilizzo di strumenti di cifratura dei dati assume un'importanza centrale nella valutazione delle misure di sicurezza implementate. La cifratura dovrebbe essere estensivamente utilizzata, ad esempio cifrando i dati:

- in transito all'interno e all'esterno della cloud;
- conservati all'interno dei database;
- archiviati sui supporti di backup.

Cifratura:

È opportuno valutare anche la possibilità di utilizzare un ulteriore livello di cifratura per i dati in memoria, per ridurre al minimo le possibili perdite di controllo sulla riservatezza dei dati stessi.

La cifratura, inoltre, può essere un valido strumento in due situazioni molto critiche del mondo cloud: il furto di dati e la cancellazione dei dati.

In molte legislazioni, un furto di dati cifrati non è soggetto agli obblighi di pubblicità che altrimenti dovrebbero essere svolti se i dati fossero in chiaro.

Per queste legislazioni, se i dati sono cifrati, è come se il furto di dati non fosse avvenuto.

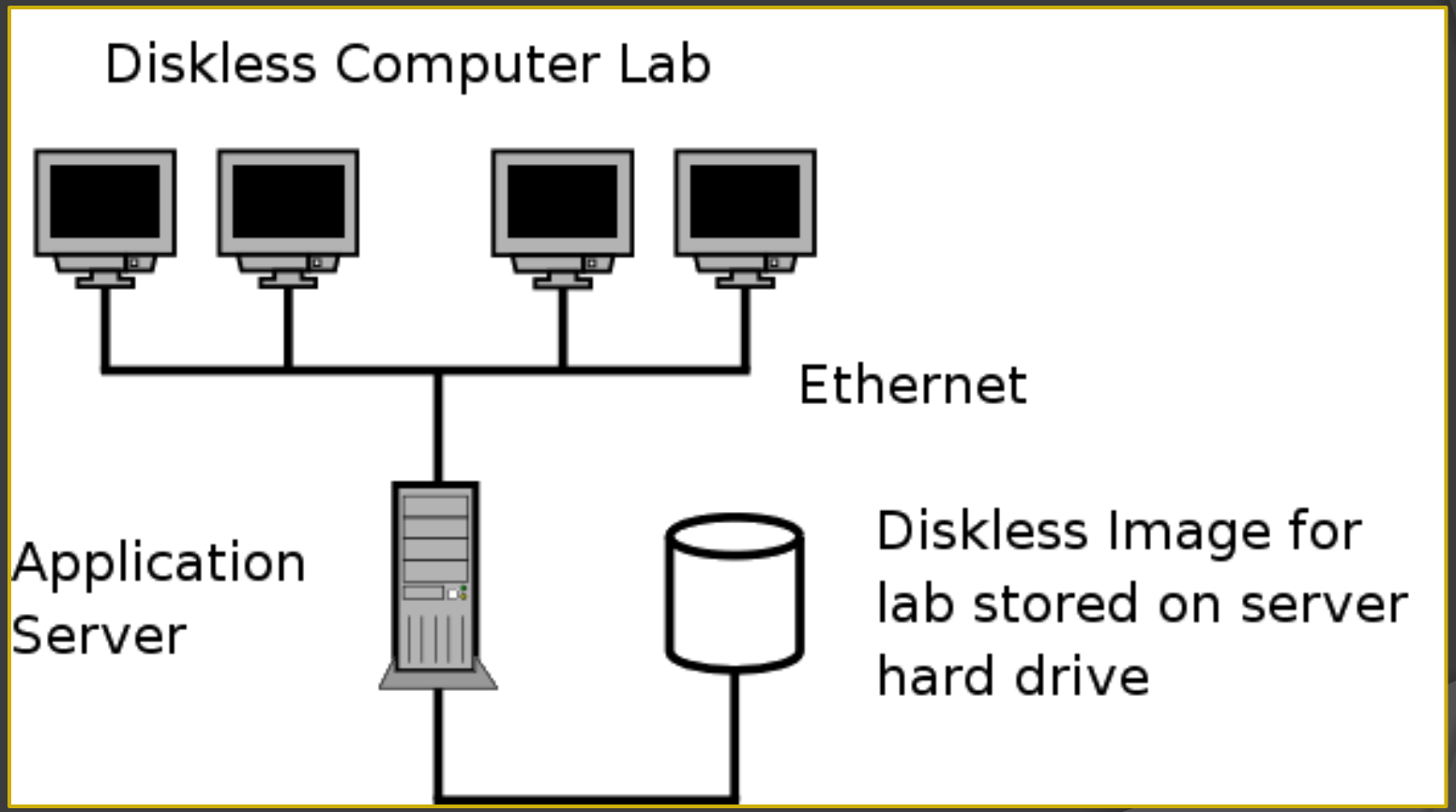
Fornitori?

- https://www.cloudsleuth.net/web/guest/global-provider-view

HomeMade...similCloud:

- DiskLess, ThinClient PC cosa sono ?
- Dove possiamo usarli ?
- Come si realizzano ?
- Quali vantaggi offrono ?

DiskLess:


Diskless Computer Lab
Ethernet
Application Server
Diskless Image for lab stored on server hard drive

DiskLess e ThinClient:

"PXE (Preboot eXecution Environment) is Intel's loosely defined standard for booting PCs over the network. A PXE-capable BIOS or boot ROM can download bootstrapping code and load an operating system over the network. Booting Linux with PXE is a straightforward way of starting a diskless workstation or appliance in a closed network . . .“

http://www.debian-administration.org/articles/478
http://en.wikipedia.org/wiki/Diskless_node

Vantaggi:

- *Access for all* If anything goes wrong with a piece of hardware, a user can just move over to the next cubicle and start right up where he or she left off with no loss of productivity. "You're talking seconds rather than hours for getting a user up and running on new hardware after a crash," says Seidner.

- *Seamless software transitions* Because everything is done at the server level, there's no need to install software on separate machines or individually upgrade applications. "Everything is done behind the scenes, without disturbing users. This dramatically reduces hardware maintenance costs and keeps employees productive during major software transitions," says Seidner.

- *Enhanced security* One of the biggest security risks for the enterprise network is unauthorized downloads of programs or content from the Internet. That simply can't happen with thin clients. Likewise, because all antivirus and anti-spam protection exists at the server level, IT management needn't be concerned about security breaches on individual machines. Finally, data residing on the server is much easier to back up and protect against loss or theft -- a prime concern when individual users keep important data on their own personal hard drives.

Domande? Chiarimenti? Proposte?