

MÀSTER INTERNACIONAL EN PROGRAMARI LLIURE



The worldwide university



TFM
TREBALL FINAL DE MÀSTER
GESTOR CENTRALITZAT D'ACCESSOS

Autor: Jordi Blasco Planesas

Consultor: Francisco Javier Noguera Otero

16.01.2012



Introducció (I)

Què és un *administrador de sistemes* ?

És un professional dedicat al **manteniment** i **funcionament** d'un sistema informàtic i/o xarxa.



suport

instal·lació resolució
etc. d'incidències

supervisió *scripting*



manteniment



Introducció (II)

Objectiu actual: reducció de costos

- ✓ Incrementar el volum de negoci: més servidors a administrar
- ✓ Virtualització com a solució indispensable per determinats serveis
- ✓ Potenciació de serveis basats en GNU/Linux i UNIX sobre entorns Windows
- ✓ Ús d'eines centralitzadores d'administració de servidors
- ✓ Controlar la inversió en nombre d'administradors de sistemes



TEMPS



EFICIENTS



Introducció (III)

Factors comuns a tenir en compte :

- ✓ La majoria dels servidors utilitzen GNU/Linux i UNIX
- ✓ El principal protocol d'accés és SSH
- ✓ El conjunt d'usuaris que accedeixen als servidors GNU/Linux i UNIX



Gestor d'accessos



Objectius

- ✓ Gestionar tots els accessos als servidors GNU/Linux i UNIX
- ✓ Desvincular els usuaris de la gestió de contrasenyes dels servidors
- ✓ Facilitar la gestió de privilegis permanents i temporals
- ✓ Millorar la seguretat dels entorns
- ★ **Reduir el temps d'accés als servidors**



SSH (I)

El protocol SSH com a pedra angular del projecte :

- ✓ Permet l'accés a servidors remots a través de la xarxa
- ✓ Permet gestionar un servidor amb l'intèrpret de comandes
- ✓ Estableix túnel SSH entre servidors i xifra les dades transmeses
- ★ Permet establir **relacions de confiança**





SSH (II)

Què és una *relació de confiança* ?

- ✓ És un túnel SSH entre origen [usuari:servidor] i destí [usuari:servidor]
- ✓ L'autenticació s'estableix per mitjà de PKI: infraestructura de clau pública

Què possibilita ?

- ★ L'accés al servidor destí sense necessitat d'autenticació amb contrasenya



```
jordi@arrakis:~$ hostname
arrakis
jordi@arrakis:~$ ssh root@dune
root@dune:~$ hostname
dune
root@dune:~$
```



SSH (III)

Com es configura una *relació de confiança* ?

- ✓ És crea un parell de claus per l'usuari origen: pública PK i privada SK
- ✓ Es copia la PK de l'usuari origen dins `~/.ssh/authorized_keys` de l'usuari destí
- ✓ Es dóna d'alta el servidor destí dins `~/.ssh/known_hosts` de l'usuari origen
- ✓ S'habilita la validació amb PK dins `/etc/ssh/sshd_config` del servidor destí
- ✓ Es recarrega la configuració del dimoni `sshd` del servidor destí





El projecte



identificació

Accés d'usuaris a l'aplicació



usuaris

Gestió dels usuaris sobre els quals es defineixen accessos



Gestió dels servidors sobre els que s'hi concreten els accessos

Gestió dels accessos que s'estableixen entre usuaris i servidors



servidors

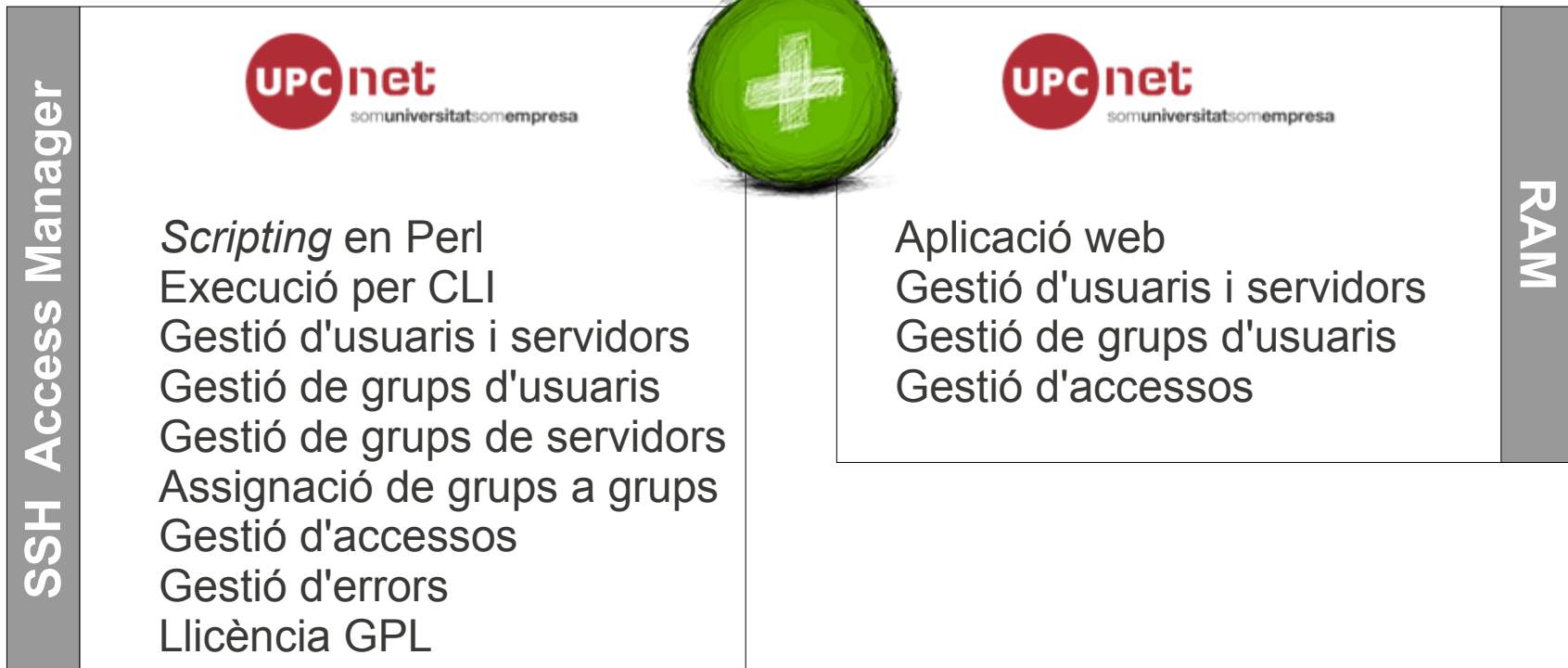
accessos





Continuïtat i evolució

nou projecte





Tecnologia i entorn



tecnologia

entorn

L



Ubuntu 10.04 server 32 bits

A



Apache HTTPd 2.2.14
Apache module PHP5 v5.3.2
Apache module for MySQL auth v4.3.9

M



MySQL Server 5.1.41

P



PHP5 v5.3.2
MySQL mòdul per PHP5 v5.3.2





Metodologia

basat
en *cascada* i *agile*

Anàlisi

Disseny

Codificació

Test

Implantació

Manteniment


Manteniment

Implementar les noves funcionalitats requerides pel client, així com mantenir les existents.





Estimació de costos

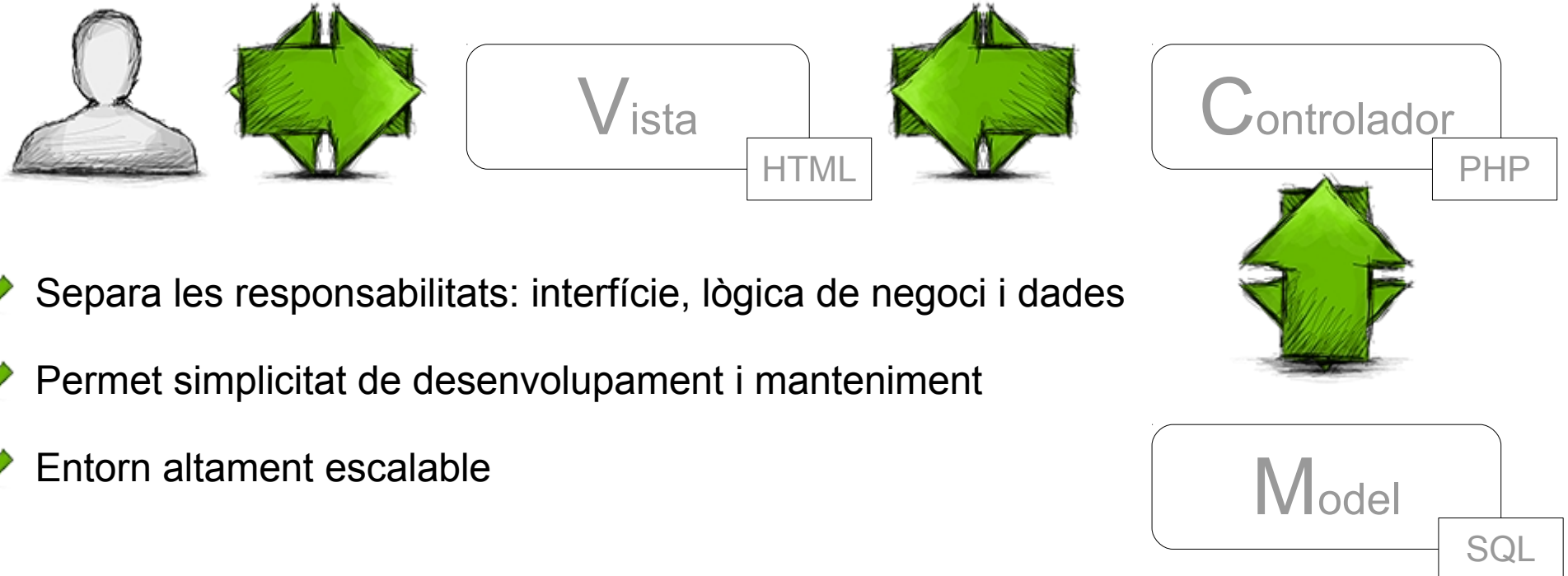
Anàlisi	10 h.	 <h2>Test</h2> <ul style="list-style-type: none"> ✓ Subsistema identificació : 1 h. ✓ Subsistema usuaris : 1 h. ✓ Subsistema servidors : 1 h. ✓ Subsistema accessos : 7 h.
Disseny	20 h.	
Codificació	120 h.	
Test	10 h.	
Implantació	10 h.	
Manteniment	0 h.	



Desenvolupament (I)

Què és el paradigma MVC ?

✓ És una separació lògica de l'aplicació en tres capes



✓ Separa les responsabilitats: interfície, lògica de negoci i dades

✓ Permet simplicitat de desenvolupament i manteniment

✓ Entorn altament escalable



Desenvolupament (II)

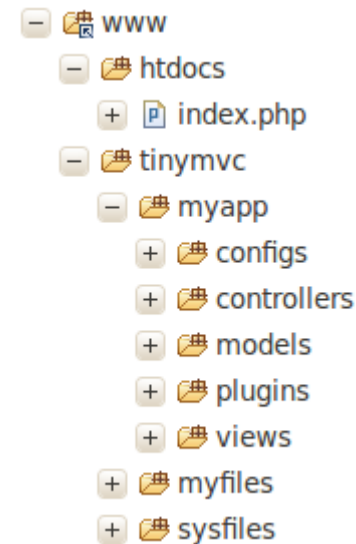
Com s'ha implementat el model MVC amb PHP?

- ✓ Framework PHP molt lleuger i senzill
- ✓ Necessitats ínfimes de recursos
- ✓ Corba d'aprenentatge ràpida



TinyMVC

<http://www.tinymvc.com>





Desenvolupament (III)



Subsistema d'identificació

Identificació usuari

! Validació a l'aplicació.

Username

Password

 Validar usuari  Canviar password

 [login](#)

Canvi de password.

! Canvi de password. Els camps marcats amb * són obligatoris

Username *

Password *

Nova password *

Confirmació password *

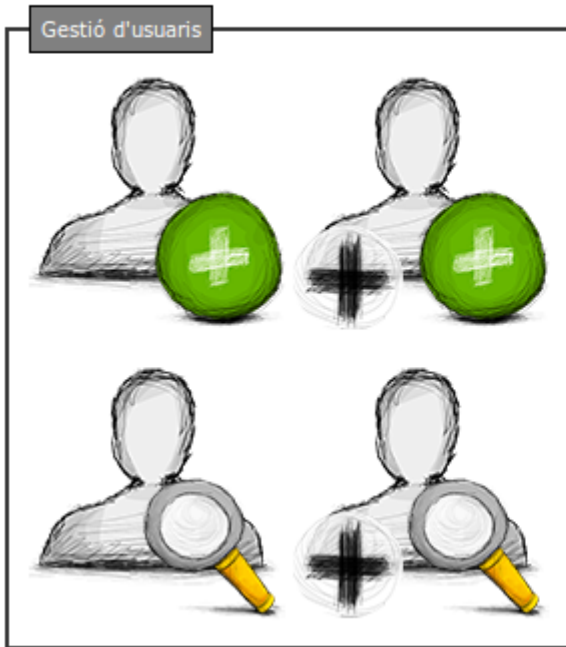
 Canviar password



Desenvolupament (IV)

Subsistema d'usuaris

Benvingut@ admin !



menu

Alta usuari → **menu - consulta usuaris**

Modificació usuari

Donar d'alta

Es pot *modificar* l'usuari i desar els canvis amb ✓ (els camps ✖ són obligatoris)

Usuaris

Nom → **menu - consulta grups**

Cognom

Modificació grup

Administrador

Es pot *modificar* el grup i desar els canvis amb ✓ o bé *eliminar-lo* amb -.

Confir

Descrip

Clau pí

Grups

jordi	grup individual	
Sistemes 1		

nnexió

licació

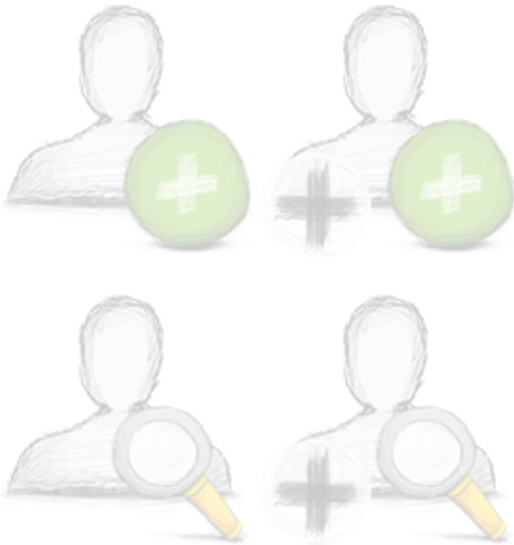


Desenvolupament (V)

Subsistema de servidors

Benvingut@ admin !

Gestió d'usuaris



menu - consulta servidors

Modificació servidor

! Es pot *modificar* el servidor i desar els canvis amb ✓ (els camps * són obligatoris)

menu - consulta grups

Modificació grup

! Es pot *modificar* el grup i desar els canvis amb ✓
o bé *eliminar-lo* amb -

Nom

Descripció

✓ Modificar grup - Eliminar grup

mozart	grup individual
Webservers	servidors web Apache HTTPd

✓ Modificar servidor - Eliminar servidor

connexió

aplicació

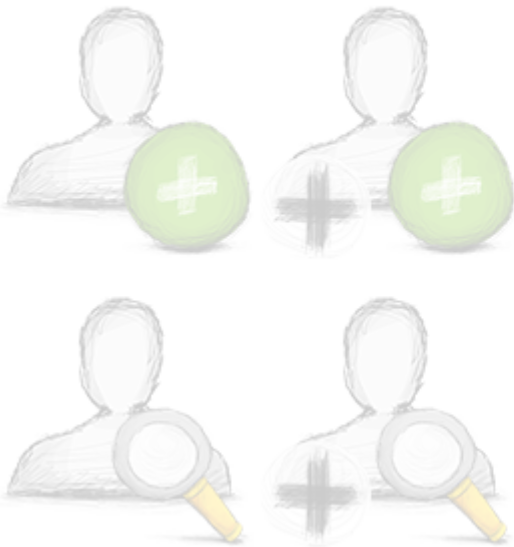


Desenvolupament (VI)

Subsistema de d'accessos

Benvingut@ admin !

Gestió d'usuaris





menu

Alta accés

! Donar d'alta un accés al sistema. Si no s'especifica data d'expiració, l'accés no caducarà.

menu - consulta accessos

Modificació accés

! Es pot *modificar* la data d'expiració de l'accés i desar els canvis amb  o bé *eliminar-lo* amb .

Agrupació d'usuaris


Agrupació de servidors

Data d'expiració (format: dd-mm-aa)

 **Modificar accés**  **Eliminar accés**

 **Afegir accés**  **Cancelar**

Desconnexió 

l'aplicació 



Desenvolupament (VII)

Auditoria

```
mysql> select * from Logs;
```

date	username	info
2012-01-21 22:17:16	admin	Alta grup usuari [Backoffice 1]
2012-01-21 22:17:33	admin	Alta grup usuari [Sistemes 1]
2012-01-21 22:19:37	admin	Alta usuari [jordi]
2012-01-21 22:19:37	admin	Alta grup usuari individual [jordi]
2012-01-21 22:19:37	admin	Associat usuari [jordi] a grup [Backoffice 1]
2012-01-21 22:20:00	admin	Modificat usuari [jordi]
2012-01-21 22:20:00	admin	Desassociat usuari [jordi] de tots els grups
2012-01-21 22:20:00	admin	Associat usuari [jordi] a grup [Backoffice 1]
2012-01-21 22:25:18	admin	Alta grup usuari [Backoffice 2]
2012-01-22 00:00:43	admin	Alta grup servidor [Correu]
2012-01-22 00:02:38	admin	Alta servidor [mozart1]
2012-01-22 00:02:38	admin	Alta grup servidor individual [mozart1]
2012-01-22 00:02:38	admin	Associat servidor [mozart1] a grup [Correu]
2012-01-22 00:02:53	admin	Alta servidor [mozart2]
2012-01-22 00:02:53	admin	Alta grup servidor individual [mozart2]
2012-01-22 00:02:53	admin	Associat servidor [mozart2] a grup [Correu]
2012-01-22 00:09:22	admin	Alta grup servidor [Webservers]
2012-01-22 00:20:34	admin	Alta acces grup usuari [jordi] a grup servidor [Correu]
2012-01-22 00:20:53	admin	Modificada data expiracio acces grup usuari [jordi] a grup servidor [Correu]



Conclusions

- ★ Es crea la base d'un projecte que millora l'eficiència d'una empresa
- ★ El projecte facilita la gestió d'accessos, així com incrementa la seguretat
- ★ La reducció de temps en tasques repetitives implica reducció de costos
- ★ És possible basar projectes de qualitat exclusivament en programari lliure
- ★ El *Màster en Programari Lliure* és útil per les necessitats del dia a dia