

El directorio corporativo centro de la identidad digital

El servidor de Fedora

Victoriano Giralt

Servicio Central de Informática
Universidad de Málaga

Jornadas Tecnológicas
inFORMANdo
11 de diciembre de 2007



La Identidad es escurridiza en el mundo digital



©Peter Steiner. The New Yorker, 5 de julio de 1993



¿Es tan importante la identidad?

vamos al cine ...



Índice

- 1 La identidad y su gestión
- 2 El directorio, almacén de identidad
- 3 Servidores de directorio



Parte I

La identidad y su gestión



La identidad y su gestión

1 ¿Qué es la Gestión de Identidad (IdM)?

- Definiciones
- Procesos
- Funciones



La identidad y su gestión

- 1 ¿Qué es la Gestión de Identidad (IdM)?
 - Definiciones
 - Procesos
 - Funciones
- 2 La Edad de Piedra de la Gestión de Identidad



La identidad y su gestión

- 1 ¿Qué es la Gestión de Identidad (IdM)?
 - Definiciones
 - Procesos
 - Funciones
- 2 La Edad de Piedra de la Gestión de Identidad
- 3 Hacia una mejor IdM
 - Conceptos
 - Enfermedad
 - Cura



La identidad y su gestión

- 1 ¿Qué es la Gestión de Identidad (IdM)?
 - Definiciones
 - Procesos
 - Funciones
- 2 La Edad de Piedra de la Gestión de Identidad
- 3 Hacia una mejor IdM
 - Conceptos
 - Enfermedad
 - Cura
- 4 Nuevas funciones
 - Visión general
 - Provisión
 - Incorporando IdM en aplicaciones
 - Demandas



La identidad y su gestión

- 1 ¿Qué es la Gestión de Identidad (IdM)?
 - Definiciones
 - Procesos
 - Funciones
- 2 La Edad de Piedra de la Gestión de Identidad
- 3 Hacia una mejor IdM
 - Conceptos
 - Enfermedad
 - Cura
- 4 Nuevas funciones
 - Visión general
 - Provisión
 - Incorporando IdM en aplicaciones
 - Demandas



Definición de IdM

De qué va todo esto

Tenemos que saber de lo que estamos hablando



Definición de IdM

De qué va todo esto

Tenemos que saber de lo que estamos hablando

- ¿Qué es la gestión de identidad?



Definición de IdM

De qué va todo esto

Tenemos que saber de lo que estamos hablando

- ¿Qué es la gestión de identidad?

“La gestión de identidad es el conjunto de procesos de negocio, y su infraestructura de soporte, para la creación, uso y mantenimiento de identidades electrónicas.”

The Burton Group (gabinete de investigación especializada en infraestructura de TI para las empresas)



Definición de IdM

De qué va todo esto

Tenemos que saber de lo que estamos hablando

- ¿Qué es la gestión de identidad?

“La gestión de identidad es el conjunto de procesos de negocio, y su infraestructura de soporte, para la creación, uso y mantenimiento de identidades electrónicas.”

The Burton Group (gabinete de investigación especializada en infraestructura de TI para las empresas)

- La gestión de identidad, en este sentido, se conoce, a veces, como “Gestión de identidad y acceso” (IAM, *Identity and Access Management*)



Terminología común en IdM

Qué significan todos estos *palabros*

Es importante entender la terminología del negocio



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- Digital Id

Identidad digital

Los trocitos de información de identidad que existen en los sistemas de TI de la organización a la que pertenece una persona.

La identidad **debe** ser única en cada entorno.



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- AuthN
- Digital Id

Autenticación

Proceso que permite verificar la identidad de un individuo, por cualquier método, sean electrónicos o físicos.

Esta prueba de identidad también se conoce como credenciales.



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- AuthR
- AuthN
- Digital Id

Autorización

Proceso que valida los derechos del usuario sobre un determinado recurso y, normalmente, los hace valer.

A veces aparece como AuthS (inglés británico) o AuthZ (inglés americano).



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- **AAI**
- AuthR
- AuthN
- Digital Id

Infraestructura de Autenticación y Autorización

Un conjunto de sistemas coordinados que permite a las organizaciones colaborar en el intercambio de datos de identidad para controlar el acceso a los servicios por sus respectivos miembros.



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- **IdP**
- AAI
- AuthR
- AuthN
- Digital Id

Proveedor de **Id**entidad

También conocido como fuente de identidad.
La organización que tiene toda la información necesaria para identificar a un individuo, sea una persona, un sistema o un servicio.



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- SP
- IdP
- AAI
- AuthR
- AuthN
- Digital Id

Proveedor de Servicios

También conocido como consumidor de identidad. Alguien que necesita conocer la identidad de un individuo y, probablemente, alguna otra información asociada, para permitir el acceso a un recurso.



Terminología común en IdM

Qué significan todos estos *palabras*

Es importante entender la terminología del negocio

- SoR
- SP
- IdP
- AAI
- AuthR
- AuthN
- Digital Id

Sistema de Registro

Los sistemas que recogen datos sobre los individuos, esto es, aquellos a través de los cuales pasan a formar parte de la organización. Por ejemplo: la nómina o el sistema de matrícula.



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María”



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo”



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (*AuthN*)



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (*AuthN*)
- ”Quiero entregar unos trabajos“



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (*AuthN*)
- ”Quiero entregar unos trabajos“
😊 (AuthR: Permitir a María usar los servicios a los que tiene derecho)



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (*AuthN*)
- ”Quiero entregar unos trabajos“
😊 (AuthR: Permitir a María usar los servicios a los que tiene derecho)
- ”Ya puestos me gustaría cambiar mi nota de Física del cuatrimestre pasado“



IdM con ejemplos

María, la alumna

Veamos a María usando algunos sistemas de la Universidad

- “¡Hola! Soy María” (*Identidad*)
- “y aquí están mi usuario y clave para demostrarlo” (*AuthN*)
- ”Quiero entregar unos trabajos“
😊 (AuthR: Permitir a María usar los servicios a los que tiene derecho)
- ”Ya puestos me gustaría cambiar mi nota de Física del cuatrimestre pasado“
😞 (AuthR: Evitar que haga cosas que no debe)



Algunas preguntas comunes

a diversos entornos de IdM

Este conjunto de preguntas se deben hacer en muchos entornos de IdM.



Algunas preguntas comunes

a diversos entornos de IdM.

Este conjunto de preguntas se deben hacer en muchos entornos de IdM.

- ¿Las personas que usan los servicios son quien dicen ser?
- ¿Pertenece a nuestra comunidad?
- ¿Tienen permiso?
- ¿Su privacidad está protegida?



Algunas preguntas comunes

a diversos entornos de IdM.

Este conjunto de preguntas se deben hacer en muchos entornos de IdM.

- ¿Las personas que usan los servicios son quien dicen ser?
- ¿Pertenece a nuestra comunidad?
- ¿Tienen permiso?
- ¿Su privacidad está protegida?

Huele a asuntos no estrictamente técnicos por aquí.



Funciones básicas de IdM

las que necesita cualquier sistema

Hay tres funciones que todo sistema debe prestar



Funciones básicas de IdM

las que necesita cualquier sistema

Hay tres funciones que todo sistema debe prestar

- AuthN: Verificar la identidad de los individuos que intentan acceder a un servicio o recurso



Funciones básicas de IdM

las que necesita cualquier sistema

Hay tres funciones que todo sistema debe prestar

- AuthN: Verificar la identidad de los individuos que intentan acceder a un servicio o recurso
- AuthR: Asegurar que el individuo posee los permisos necesarios para lo que quiere hacer



Funciones básicas de IdM

las que necesita cualquier sistema

Hay tres funciones que todo sistema debe prestar

- AuthN: Verificar la identidad de los individuos que intentan acceder a un servicio o recurso
- AuthR: Asegurar que el individuo posee los permisos necesarios para lo que quiere hacer
- Log: Llevar un registro de accesos a los recursos o servicios



En la Edad de Piedra

las tribus estaban aisladas

En una organización que no ha despertado a la IdM



En la Edad de Piedra

las tribus estaban aisladas

En una organización que no ha despertado a la IdM

- Cada aplicación hace las funciones de IdM por sí misma



En la Edad de Piedra

las tribus estaban aisladas

En una organización que no ha despertado a la IdM

- Cada aplicación hace las funciones de IdM por sí misma
- Lista de usuarios, credenciales, si estás en la lista, entras
AuthN = AuthR



En la Edad de Piedra

las tribus estaban aisladas

En una organización que no ha despertado a la IdM

- Cada aplicación hace las funciones de IdM por sí misma
- Lista de usuarios, credenciales, si estás en la lista, entras
AuthN = AuthR
- Existen identificadores nacionales de escaso valor local



Una forma mejor de IdM

curando el síndrome de las pegatinas amarillas

IAM es una capa de middleware
al servicio de múltiples aplicaciones,
que necesita expandir el conjunto de funciones básicas



Una forma mejor de IdM

curando el síndrome de las pegatinas amarillas

IAM es una capa de middleware
al servicio de múltiples aplicaciones,
que necesita expandir el conjunto de funciones básicas

- Reflejar: Mantener los cambios en los datos institucionales desde los cambios en los SoR y otros componentes de la IdM



Una forma mejor de IdM

curando el síndrome de las pegatinas amarillas

IAM es una capa de middleware
al servicio de múltiples aplicaciones,
que necesita expandir el conjunto de funciones básicas

- Reflejar: Mantener los cambios en los datos institucionales desde los cambios en los SoR y otros componentes de la IdM
- Unir: Establecer y mantener la identidad de la persona entre SoR



Una forma mejor de IdM

curando el síndrome de las pegatinas amarillas

IAM es una capa de middleware al servicio de múltiples aplicaciones, que necesita expandir el conjunto de funciones básicas

- Reflejar: Mantener los cambios en los datos institucionales desde los cambios en los SoR y otros componentes de la IdM
- Unir: Establecer y mantener la identidad de la persona entre SoR
- Credencial: expedir credenciales digitales a las personas de la comunidad



Fragmentación de Identidad

el cáncer de la gestión de identidad

Hay dos puntos básicos para diagnosticar la enfermedad



Fragmentación de Identidad

el cáncer de la gestión de identidad

Hay dos puntos básicos para diagnosticar la enfermedad

- Para una persona concreta de la comunidad,
¿conocemos la entrada en el almacén de datos de cada sistema que tiene pedacitos de su identidad?



Fragmentación de Identidad

el cáncer de la gestión de identidad

Hay dos puntos básicos para diagnosticar la enfermedad

- Para una persona concreta de la comunidad, ¿conocemos la entrada en el almacén de datos de cada sistema que tiene pedacitos de su identidad?
- ¿Cuántos sistemas pueden crear una "persona"? más de uno ⇒ fragmentación de identidad



La Unión

tenemos un remedio para el cáncer (en IdM)

El mejor remedio para la fragmentación de identidad es



La Unión

tenemos un remedio para el cáncer (en IdM)

El mejor remedio para la fragmentación de identidad es:
La Unión



La Unión

tenemos un remedio para el cáncer (en IdM)

El mejor remedio para la fragmentación de identidad es:

La Unión

Para aplicarlo, necesitamos lógica de negocios que



La Unión

tenemos un remedio para el cáncer (en IdM)

El mejor remedio para la fragmentación de identidad es:

La Unión

Para aplicarlo, necesitamos lógica de negocios que

- Establezca los registros que corresponden a la misma persona



La Unión

tenemos un remedio para el cáncer (en IdM)

El mejor remedio para la fragmentación de identidad es:

La Unión

Para aplicarlo, necesitamos lógica de negocios que

- Establezca los registros que corresponden a la misma persona
- Mantenga esa unión de identidad frente a los cambios en los datos almacenados en los sistemas



Acceso a la Información de Identidad

Implementando La Unión

Para poder implementar La Unión,
necesitamos acceso a la información de identidad



Acceso a la Información de Identidad

Implementando La Unión

Para poder implementar La Unión,
necesitamos acceso a la información de identidad

- Alguna vendrá del Directorio Corporativo por reflejo de los SoR



Acceso a la Información de Identidad

Implementando La Unión

Para poder implementar La Unión,
necesitamos acceso a la información de identidad

- Alguna vendrá del Directorio Corporativo por reflejo de los SoR
- A otros pedacitos llegaremos por puentes de identidad

Nº regsitro	ID Sist. A	ID Sist. B	ID Sist. C	ID Sist. D
3a104e59	fperez32	86443	pacop	864164
8c2f916d	mgomez1	45209	mariag	752731



Si no puedes integrar, *federa* otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad
es



Si no puedes integrar, *federa* otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad
es: *La Federación*



Si no puedes integrar, *federa* otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad
es: *La Federación*
La Gestión de Identidad Federada



Si no puedes integrar, *federa* otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad
es: *La Federación*

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones



Si no puedes integrar, *federa*

otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad es: *La Federación*

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos



Si no puedes integrar, *federa*

otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad es: *La Federación*

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos
- Por medio de acuerdos inter-institucionales



Si no puedes integrar, *federa*

otra forma de curar la fragmentación de identidad

El segundo mejor remedio para la fragmentación de identidad es: *La Federación*

La Gestión de Identidad Federada

- Se basa en la infraestructura de Gestión de Identidad de una o más organizaciones
- Para autenticar y pasar información relativa a la autorización a los proveedores de servicios o los servidores recursos
- Por medio de acuerdos inter-institucionales
- Facilitados por la pertenencia a una federación



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas

- **Gest. Afil.:** Gestionar la información de afiliación y los grupos



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas

- Gest. Afil.: Gestionar la información de afiliación y los grupos
- **Gest. Priv.:** Gestionar privilegios y permisos a nivel de sistemas y recursos



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas

- Gest. Afil.: Gestionar la información de afiliación y los grupos
- Gest. Priv.: Gestionar privilegios y permisos a nivel de sistemas y recursos
- **Provisión**: Empujar la información de IAM hacia los sistemas y servicios según se requiera



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas

- Gest. Afil.: Gestionar la información de afiliación y los grupos
- Gest. Priv.: Gestionar privilegios y permisos a nivel de sistemas y recursos
- Provisión: Empujar la información de IAM hacia los sistemas y servicios según se requiera
- **Envío**: Facilitar información de control de acceso y autorización a los servicios en tiempo de ejecución



El conjunto extendido de funciones básicas

una nueva visión requiere nuevas formas de hacer las cosas

Esta nueva forma de hacer IdM requiere funciones nuevas

- Gest. Afil.: Gestionar la información de afiliación y los grupos
- Gest. Priv.: Gestionar privilegios y permisos a nivel de sistemas y recursos
- Provisión: Empujar la información de IAM hacia los sistemas y servicios según se requiera
- Envío: Facilitar información de control de acceso y autorización a los servicios en tiempo de ejecución
- **AuthR**: Independizar de la AuteNticación las decisiones de permitir o denegar el uso



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*

- Exportándoles información reformateada de manera que la puedan entender



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*

- Exportándoles información reformateada de manera que la puedan entender
- Usando un API de la aplicación



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*

- Exportándoles información reformateada de manera que la puedan entender
- Usando un API de la aplicación
- o con trucos que escriben en su almacén de datos



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*

- Exportándoles información reformateada de manera que la puedan entender
- Usando un API de la aplicación
- o con trucos que escriben en su almacén de datos



Provisión

Llevando la información de identidad a donde se necesita

Este es un proceso que se encarga de colocar la identidad en aplicaciones *con carácter*

- Exportándoles información reformateada de manera que la puedan entender
- Usando un API de la aplicación
- o con trucos que escriben en su almacén de datos

El cambio es inexorable, así que éste es un proceso sin fin



Integración de aplicaciones e IdM

trayendo las aplicaciones al futuro

Hay dos formas de integrar las aplicaciones y la IdM



Integración de aplicaciones e IdM

trayendo las aplicaciones al futuro

Hay dos formas de integrar las aplicaciones y la IdM

- Para las aplicaciones domesticadas:
Dotárlas de todas las funciones de IdM



Integración de aplicaciones e IdM

trayendo las aplicaciones al futuro

Hay dos formas de integrar las aplicaciones y la IdM

- Para las aplicaciones domesticadas:
Dotárlas de todas las funciones de IdM
- Para las aplicaciones con *carácter de fábrica*:
Acercarse a más de medio camino provisionando



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*
- Cumplir con un número creciente de leyes



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*
- Cumplir con un número creciente de leyes
- Aumentar el nivel de seguridad frente a nuevas amenazas sin fin



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*
- Cumplir con un número creciente de leyes
- Aumentar el nivel de seguridad frente a nuevas amenazas sin fin
- Servir poblaciones nuevas (insertar aquí las de cada uno)



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*
- Cumplir con un número creciente de leyes
- Aumentar el nivel de seguridad frente a nuevas amenazas sin fin
- Servir poblaciones nuevas (insertar aquí las de cada uno)
- Más peticiones de nuevos servicios y nuevas combinaciones de ellos



Requisitos

antiguos, nuevos, y alguno más

Qué se le está pidiendo a la gente de TI

- Alta y baja automática de cuentas
- Acceso a registros de personal por imperativo legal
- Servicios de *ventanilla única*
- Cumplir con un número creciente de leyes
- Aumentar el nivel de seguridad frente a nuevas amenazas sin fin
- Servir poblaciones nuevas (insertar aquí las de cada uno)
- Más peticiones de nuevos servicios y nuevas combinaciones de ellos
- Interés creciente en el e-Negocio



Requisitos

antiguos, nuevos, y alguno más

Parece que nos sobrepase



Requisitos

antiguos, nuevos, y alguno más

Parece que nos sobrepase
Lo *hace*



Requisitos

antiguos, nuevos, y alguno más

Parece que nos sobrepase

Lo *hace*

Y todos y cada uno de los puntos anteriores
tiene su cara de Gestión de Identidad



La IdM es una ayuda

al rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda



La IdM es una ayuda

al rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM



La IdM es una ayuda

al rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM
- Reduciendo la complejidad del ecosistema TIC



La IdM es una ayuda

al rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM
- Reduciendo la complejidad del ecosistema TIC
la complejidad como fricción \Rightarrow recursos malgastados



La IdM es una ayuda

al rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM
- Reduciendo la complejidad del ecosistema TIC
la complejidad como fricción \Rightarrow recursos malgastados
- Mejorando la experiencia del usuario



La IdM es una ayuda

a la rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM
- Reduciendo la complejidad del ecosistema TIC
la complejidad como fricción \Rightarrow recursos malgastados
- Mejorando la experiencia del usuario
- Permitiendo la especialización funcional



La IdM es una ayuda

a la rescate a los pobres profesionales de las TIC

Una capa completa de IdM ayuda

- Mejorando la escalabilidad:
Automatización de procesos de IdM
- Reduciendo la complejidad del ecosistema TIC
la complejidad como fricción \Rightarrow recursos malgastados
- Mejorando la experiencia del usuario
- Permitiendo la especialización funcional
Los programadores se pueden dedicar a
la funcionalidad específica de la aplicación



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
Materias primas en sistemas



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
Materias primas en sistemas
- Integración



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
 - Materias primas en sistemas
- Integración
 - Subsistemas en sistemas completos



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
 - Materias primas en sistemas
- Integración
 - Subsistemas en sistemas completos
 - Múltiples sistemas en ecosistemas



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
 - Materias primas en sistemas
- Integración
 - Subsistemas en sistemas completos
 - Múltiples sistemas en ecosistemas
- Todos estamos pasando de la construcción a la integración



Evolución de la IdM

desde la construcción a la integración

La forma de hacer las cosas está cambiando

- Construcción
 - Materias primas en sistemas
- Integración
 - Subsistemas en sistemas completos
 - Múltiples sistemas en ecosistemas
- Todos estamos pasando de la construcción a la integración
- y es más fácil con código y estándares abiertos



Funciones de IdM

el conjunto ampliado

<i>Reflejar</i>	información interesante
<i>Unir</i>	la identidad entre SoR
<i>Credencial</i>	NetID, otros
<i>Gest. Afil/Grupos</i>	información de AuthR
<i>Gest. Privilegios</i>	más información de AuthR
<i>Provisión</i>	Llevar la información de AuthNR a las aplic.
<i>Enviar</i>	Inf. de AuthR a las aplicaciones a demanda
<i>Autenticar</i>	las pretensiones de identidad
<i>Autorizar</i>	las decisiones de acceso (permitir / denegar)
<i>Registrar</i>	para auditar, contabilizar, diagnosticar, ...



Las mismas funciones en diferentes cajas

Finalmente ...



Las mismas funciones

en diferentes cajas

Finalmente ...

- **Vuestra infraestructura de IdM puede diferir de la mia**



Las mismas funciones

en diferentes cajas

Finalmente . . .

- Vuestra infraestructura de IdM puede diferir de la mia
- pero, en alguna parte, de algún modo se hacen las funciones de IdM



Las mismas funciones

en diferentes cajas

Finalmente . . .

- Vuestra infraestructura de IdM puede diferir de la mia
- pero, en alguna parte, de algún modo se hacen las funciones de IdM



Las mismas funciones

en diferentes cajas

Finalmente . . .

- Vuestra infraestructura de IdM puede diferir de la mía
- pero, en alguna parte, de algún modo se hacen las funciones de IdM
- Podemos comparar nuestras soluciones mirando las diferentes formas de empaquetar las funciones



Parte II

El directorio, almacén de identidad



El directorio

- 6 Definiciones
 - Elementos
 - Esquema



El directorio

- 6 Definiciones
 - Elementos
 - Esquema

- 7 Características
 - Singularidades
 - Indizado



Las cosas claras desde el principio

LDAP **NO** es un directorio



Las cosas claras desde el principio

LDAP **NO** es un directorio
es un protocolo
para acceder al directorio



Las cosas claras desde el principio

LDAP **NO** es un directorio
es un protocolo
para acceder al directorio
X.500 *ES* el directorio



Las cosas claras desde el principio

LDAP **NO** es un directorio
es un protocolo
para acceder al directorio
X.500 **ES** el directorio

No huyais



Las cosas claras desde el principio

LDAP **NO** es un directorio
es un protocolo
para acceder al directorio
X.500 **ES** el directorio

No huyais no voy a resucitar el OSI



Las cosas claras desde el principio

LDAP **NO** es un directorio
es un protocolo
para acceder al directorio
X.500 **ES** el directorio

No huyais no voy a resucitar el OSI

Nos quedamos con que

LDAP = sistema de directorio accesible por LDAP



Qué es un directorio

desde varios puntos de vista

Lingüística

Según el D.R.A.E.

Directorio

5. m.

Guía en la que figuran las personas de un conjunto, con indicación de diversos datos de ellas, como su cargo, sus señas, su teléfono, etc.



Qué es un directorio

desde varios puntos de vista

Informática

Directorio

Objetos de información organizados jerárquicamente. Como:

- Sistemas de almacenamiento
- El sistema de nombres de dominios (DNS)
- X.500, *e/* Directorio



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas

- Una persona



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas

- Una persona
- Una organización



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas

- Una persona
- Una organización
- Un departamento



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas

- Una persona
- Una organización
- Un departamento
- Un nodo de red



Qué es una *Entrada*

Una entrada es *simplemente* un objeto individual almacenado en el directorio

Ejemplos de entradas

- Una persona
- Una organización
- Un departamento
- Un nodo de red
- La descripción de un código de clasificación



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser

- Univaluados. Un único par con un nombre por entrada.



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser

- Univaluados. Un único par con un nombre por entrada.
- Multivaluados. Múltiples pares del mismo nombre.



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser

- Univaluados. Un único par con un nombre por entrada.
- Multivaluados. Múltiples pares del mismo nombre.
- Operacionales. Gestionados por el servidor.



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser

- Univaluados. Un único par con un nombre por entrada.
- Multivaluados. Múltiples pares del mismo nombre.
- Operacionales. Gestionados por el servidor.

Ejemplos de atributos



Qué es un *Atributo*

Un atributo es un par nombre valor de una característica de un objeto almacenado en una entrada del directorio.

Los atributos pueden ser

- Univaluados. Un único par con un nombre por entrada.
- Multivaluados. Múltiples pares del mismo nombre.
- Operacionales. Gestionados por el servidor.

Ejemplos de atributos

- Los apellidos
- Una dirección IP
- Un número de teléfono
- createTimestamp



Qué es una *ObjectClass*

Una *objectClass* (clase de objetos)
es una forma de agrupar lógicamente los atributos que
pueden tener las entradas



Qué es una *ObjectClass*

Una *objectClass* (clase de objetos)
es una forma de agrupar lógicamente los atributos que
pueden tener las entradas
Según la definición de la clase, los atributos son



Qué es una *ObjectClass*

Una *objectClass* (clase de objetos) es una forma de agrupar lógicamente los atributos que pueden tener las entradas

Según la definición de la clase, los atributos son

- Requeridos. El atributo **debe** estar.



Qué es una *ObjectClass*

Una *objectClass* (clase de objetos) es una forma de agrupar lógicamente los atributos que pueden tener las entradas

Según la definición de la clase, los atributos son

- Requeridos. El atributo **debe** estar.
- Opcionales. El atributo **puede** estar (o *no*).



Qué es una *ObjectClass*

Una `objectClass` (clase de objetos) es una forma de agrupar lógicamente los atributos que pueden tener las entradas

Según la definición de la clase, los atributos son

- Requeridos. El atributo **debe** estar.
- Opcionales. El atributo **puede** estar (o *no*).

Ejemplos de `objectClasses`



Qué es una *ObjectClass*

Una objectClass (clase de objetos) es una forma de agrupar lógicamente los atributos que pueden tener las entradas

Según la definición de la clase, los atributos son

- Requeridos. El atributo **debe** estar.
- Opcionales. El atributo **puede** estar (o *no*).

Ejemplos de objectClasses

- Person
- inetNode
- schacLinkageIdentifiers



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores
- Si los atributos son requeridos o no



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores
- Si los atributos son requeridos o no
- Los tipos de las clases



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores
- Si los atributos son requeridos o no
- Los tipos de las clases

Base = Solo para heredar



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores
- Si los atributos son requeridos o no
- Los tipos de las clases

Base = Solo para heredar

Estructural = la clase principal de un objeto



El Esquema

la constitución del directorio

El esquema define el contenido de un directorio

- La organización de los atributos en clases
- Los valores de los atributos
- La forma de ordenar los valores
- La forma de buscar los valores
- Si los atributos son requeridos o no
- Los tipos de las clases

Base = Solo para heredar

Estructural = la clase principal de un objeto

Auxiliar = para atributos extra



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

Esquema

SGBD relacional

No existe un
esquema estándar

directorio LDAP

Estándares
internacionales
para personas y
organizaciones



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

Esquema
Organización

SGBD relacional

Una entidad lógica
almacenada en
varias tablas

directorio LDAP

Una entidad lógica
Un objeto
Un nodo = entrada



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Nueva tabla o
varios campos

Esquema
Organización
Varios valores

directorio LDAP

Todos en un atributo
Tantos como hagan falta



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Conjunto limitado

Esquema

Organización

Varios valores

Tipos de datos

directorio LDAP

Número ilimitado
por medio de sintáxis



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Reglas de comparación fuera del modelo de datos.
Implementado en los programas

Esquema
Organización
Varios valores
Tipos de datos
Comparación

directorio LDAP

Reglas de comparación en el modelo de datos.
Definido con el esquema



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Los cambios del esquema requieren gran esfuerzo.
Afectan a la lógica de programa

Esquema
Organización
Varios valores
Tipos de datos
Comparación
Flexibilidad

directorio LDAP

Modificaciones del esquema granulares
Hasta nivel de entrada.
Otro atributo →
otra objectClass

Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Acceso por red
no estándar

Esquema
Organización
Varios valores
Tipos de datos
Comparación
Flexibilidad
Acceso

directorio LDAP

Acceso por red estándar:
LDAP
Fácil distribución de
datos en la Red



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Mecanismos de
AuthN
sólo propietarios

Esquema
Organización
Varios valores
Tipos de datos
Comparación
Flexibilidad
Acceso
AuthN

directorio LDAP

Varios mecanismos de
AuthN estándar
que funcionan por la red



Singularidades de los directorios

un modelo más cercano al mundo real

Los SGBD mejor conocidos son los relacionales.
Describiremos los directorios LDAP por comparación

SGBD relacional

Solo propietarios
Muy complicados

Esquema
Organización
Varios valores
Tipos de datos
Comparación
Flexibilidad
Acceso
AuthN
Réplica

directorio LDAP

Protocolos estándar
incluidos en el diseño



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente



Indizado del directorio

preparándose para encontrar las entradas

- El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente
- Más índices ⇒ búsquedas más rápidas



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices ⇒ búsquedas más rápidas
- Más índices ⇒ actualizaciones más lentas



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices \Rightarrow búsquedas más rápidas
- Más índices \Rightarrow actualizaciones más lentas
- Qué atributos indizar



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices \Rightarrow búsquedas más rápidas
- Más índices \Rightarrow actualizaciones más lentas
- Qué atributos indizar
- Cómo indizarlos



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices \Rightarrow búsquedas más rápidas
- Más índices \Rightarrow actualizaciones más lentas
- Qué atributos indizar
- Cómo indizarlos, depende del esquema



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices ⇒ búsquedas más rápidas
- Más índices ⇒ actualizaciones más lentas
- Qué atributos indizar
- Cómo indizarlos, depende del esquema
 - igualdad



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices ⇒ búsquedas más rápidas
- Más índices ⇒ actualizaciones más lentas
- Qué atributos indizar
- Cómo indizarlos, depende del esquema
 - igualdad
 - presencia



Indizado del directorio

preparándose para encontrar las entradas

El LDAP está optimizado para lectura
Por tanto es vital indizar adecuadamente

- Más índices ⇒ búsquedas más rápidas
- Más índices ⇒ actualizaciones más lentas
- Qué atributos indizar
- Cómo indizarlos, depende del esquema
 - igualdad
 - presencia
 - subcadena



Parte III

Servidores de directorio



Servidores de directorio

8 Fundamentos de OpenLDAP



Servidores de directorio

- 8 Fundamentos de OpenLDAP
- 9 Fundamentos del Fedora Directory Server



Servidores de directorio

- 8 Fundamentos de OpenLDAP
- 9 Fundamentos del Fedora Directory Server
- 10 Seleccionando un Servidor de Directorio OpenSource



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido (flames > /dev/null)



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido (flames > /dev/null)
- Incómodo de administrar



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido (flames > /dev/null)
- Incómodo de administrar
casi cualquier operación requiere un rearranque



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido (flames > /dev/null)
- Incómodo de administrar
casi cualquier operación requiere un rearranque
- El esquema y los ACIs no se replican



Fundamentos de OpenLDAP

OpenLDAP ha servido muy bien a la comunidad mucho tiempo
Se merece un respeto

- Fácil y rápido de instalar
- Cualquier sabor de Linux o BSD tiene un paquete

pero ...

- No es el más rápido (flames > /dev/null)
- Incómodo de administrar
casi cualquier operación requiere un rearranque
- El esquema y los ACIs no se replican,
una pesadilla para escalar



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad

pero ...



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad

pero ...

- no es fácil de configurar



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad

pero ...

- no es fácil de configurar, más



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad

pero ...

- no es fácil de configurar, más,
¿quién dijo que ésto es un trabajo sencillo?



Fundamentos del FDS

Aunque lo han abierto recientemente, no es un recién llegado

- Robusto y muy rápido
- Excelente escalabilidad
- Mantiene las mayores instalaciones LDAP del mundo
- Réplica con Multi-master, gran fiabilidad
- Prácticamente no hay que rearrancar, gran estabilidad
- Puede replicar el esquema y los ACIs, más escalabilidad
- Puede sincronizar con AD, buena interoperabilidad

pero ...

- no es fácil de configurar, más,
¿quién dijo que ésto es un trabajo sencillo?



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor: OpenLDAP



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor: OpenLDAP
- Instalación pequeña con un par de réplicas



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor: OpenLDAP
- Instalación pequeña con un par de réplicas:
FDS u OpenLDAP



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor: OpenLDAP
- Instalación pequeña con un par de réplicas:
FDS u OpenLDAP
- Para cualquier cosa mayor



FDS vs OpenLDAP

cuál debemos elegir

La respuesta es, como siempre, “Depende”

- Instalación pequeña con un solo servidor: OpenLDAP
- Instalación pequeña con un par de réplicas:
FDS u OpenLDAP
- Para cualquier cosa mayor: FDS



Algunos URLs

Wikipedia <http://en.wikipedia.org/wiki/Ldap>

OpenLDAP <http://www.openldap.org/>

Fedora DS <http://directory.fedoraproject.org/>

RFCs <http://www.rfc-editor.org/rfcsearch.html>
buscar LDAP

OpenLDAP Admin Guide <http://www.openldap.org/doc/admin23/>

RedHat DS Admin Guide <http://www.redhat.com/docs/manuals/dir-server/ag7.1/adminTOC.html>

FDS Docs <http://directory.fedoraproject.org/wiki/Documentation>

Why FDS <http://www.enterprisenetworkingplanet.com/netos/article.php/3622486>

