

INTRODUCCIÓN AL SERVICIO DE DIRECTORIOS

AWS/AMS
Febrero 2021



ADAS ILLA
IESE
SEP ESTEVE TERRADA
SEP ESTEVE TERRADA ILLA
IESE SEP ESTEVE TERRADA ILLA

ieesteveterradas.com

1. ¿Qué es el Servicio de directorio?

Los directorios son un **tipo específico de bases de datos** con un propósito también específico: almacenar la información sobre un objeto (individuo, recurso de red, documento...).

Su papel es **clave** en cualquier organización que quiera tener la **información** sobre sus empleados, usuarios de red, etc., catalogada y accesible desde multitud de aplicaciones.

Además, el uso de un servicio de directorio facilita la **gestión de la identidad de los usuarios** de los sistemas de información en una organización.

En este núcleo formativo estudiaremos los conceptos básicos de los directorios, su diseño y su implantación.



1. ¿Qué es el Servicio de directorio?

Un **directorio** es una estructura jerárquica que organiza y almacena datos acerca de elementos. Es un tipo concreto de base de datos.

Un **servicio de directorio** es una plataforma que proporciona métodos para gestionar y almacenar los datos que contiene el directorio.

Un servicio de directorio permite la búsqueda de valores a partir de un determinado nombre (o identificador), de forma similar a lo que hace un diccionario.

Aunque el concepto de directorio se relacione con datos, bien cierto es que existen varias diferencias entre un servicio de directorio y una base de datos:



1. ¿Qué es el Servicio de directorio?

- ❑ En los directorios se realizan muchas más lecturas de datos que escrituras.
- ❑ Los directorios pueden modificar más fácilmente el diseño de las "entidades" que albergan.
- ❑ En cambio en una base de datos cambiar el diseño de ésta a posteriori puede ser más complejo.
- ❑ Los datos de los directorios suelen estar distribuidos y replicados con mayor frecuencia que en bases de datos.
- ❑ Los directorios permiten, en general, consultas simples, y no consultas que requieran la fusión de datos provenientes de varias tablas (consultas join de las bases de datos).

1.2 Tipos de Servicios de Directorio

Un tipo sencillo de directorios es el que está incluido en **aplicaciones de software**, como por ejemplo las libretas de direcciones.

Un paso más allá sería que esta aplicación de libreta de direcciones funcionara como una aplicación informática independiente, o quizás fuera un elemento más del sistema operativo. En este caso, sería preciso establecer **un estándar de intercambio de información** para que los demás programas pudieran hacer uso de esta libreta de direcciones.

Un ejemplo de estos sistemas sería **el LDIF** (LDAP, data interchange format) el cual es utilizado como medio habitual de exportación de datos de libreta de direcciones a un fichero de texto imprimible.



1.2 Tipos de Servicios de Directorio

Esta aplicación podría ser una aplicación de red ejecutándose en un servidor. De este modo, la información de los contactos estaría disponible para todos los equipos clientes que consultaran al servidor. En este caso, sería necesario establecer un protocolo de comunicaciones a nivel de aplicación para poder realizar distintas operaciones:

- Consultas sobre la información de un contacto.
- Mensaje de error en caso de que no se encontrara el contacto.
- Opcionalmente, un protocolo de identificación del usuario.
- Operaciones de alta, baja y modificación de contactos sólo ejecutables por un usuario con permisos de administrador, etc.

Los **directorios de sistemas operativos en red** almacenan datos de recursos de una red. Algunos ejemplos son **el Active Directory de Microsoft**.



1.2 Tipos de Servicios de Directorio

Ejemplo:

Otro ejemplo de directorio de propósito específico es el sistema de nombres para Internet.

El acceso a servicios basados en Internet se realiza mediante conexiones o envío de datagramas hacia una determinada dirección IP. El sistema DNS resuelve, a partir de un nombre, cuál es la dirección IP del recurso.

Así como DNS se puede ver como un servicio de directorio tanto específico, los hay de propósito general.

Este es el caso del **servicio LDAP**. Aunque en ciertos casos su uso se remite a tener información sobre los usuarios de una serie de servicios en red (permitiendo, por ejemplo, el acceso a múltiples servicios mediante un único usuario y contraseña), LDAP permite definir soluciones para un amplio espectro de escenarios.



IES
ESTEBÉ TERRADAS ILLA
TERRADAS ILLA
SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA
TERRADAS ILLA

jesesteveterradas.com

1.3 Espacio de nombres

ESPACIO DE NOMBRES:

En los servicios de directorio, cada objeto está identificado mediante un nombre.

El identificador de objeto debe ser un nombre único dentro del servicio de directorio.

Además de identificar objetos, los identificadores también pueden identificar grupos de objetos, con lo cual se puede diseñar una estructura jerárquica.

Veamos a continuación algunos ejemplos de espacios de nombres:



jesesteveterradas.com

1.3 Espacio de nombres

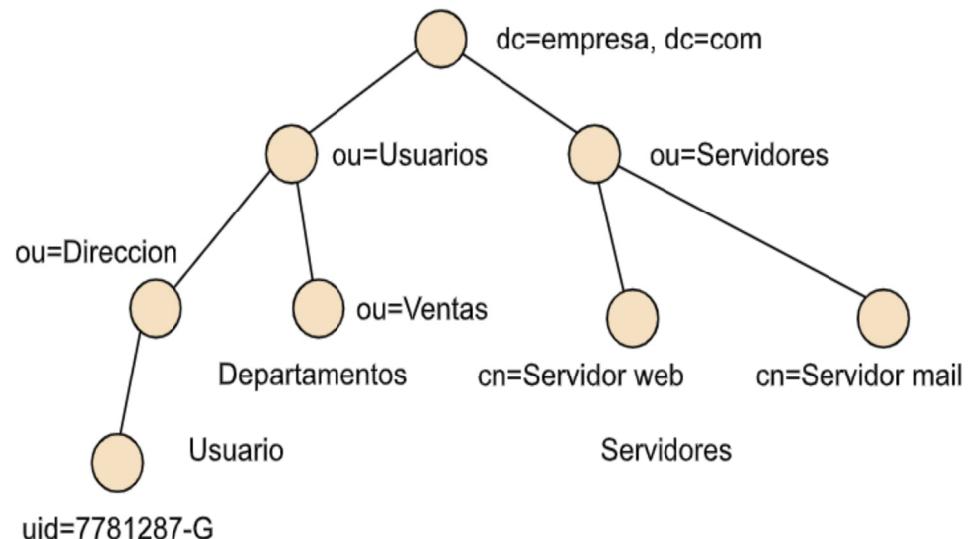
- Sistema DNS: En un sistema DNS, el espacio de nombres permite identificar únicamente a un equipo conectado a Internet. De hecho, varios nombres pueden apuntar a un mismo equipo. Para identificar un equipo dentro del espacio de nombres, el DNS se ayuda de una estructuración jerárquica iniciada en el dominio '.', que es el dominio raíz.
- Sistema LDAP: El sistema de nombres que usa LDAP permite la organización de los objetos de forma jerárquica.

En la siguiente figura se puede observar como es un ejemplo de directorio LDAP:

Ejemplo de directorio LDAP

En la figura siguiente se puede observar un ejemplo de directorio LDAP.

Ejemplo de espacio de nombres de un directorio basado en LDAP



Espacio de nombres

En esta organización (*empresa.com*) hay definidos dos grupos de objetos: los usuarios y los servidores. Los usuarios se dividen en departamentos. Como veremos más adelante, LDAP y otras implementaciones derivadas permiten la agrupación de elementos y crear una jerarquía. LDAP no fija ninguna jerarquía ni ningún número determinado de niveles: el espacio de nombres permite dar flexibilidad para adaptarse a multitud de usuarios.

Cada objeto se plasma como una **entrada de directorio**. En el ejemplo hay un total de ocho entradas. Cada entrada tiene un nombre *distinguished name* (DN). Por ejemplo, la organización tiene como DN dc=empresa, dc=com.

Cada entrada de directorio está compuesta por una serie de **atributos**, cada uno de ellos describe varios aspectos del objeto que la entrada identifica. En el ejemplo se define un usuario. Este objeto podría tener los atributos descritos en la tabla siguiente.

Ejemplo de directorio LDAP



Ejemplo de una entrada LDAP

Atributo	Valor
objectclass	person
cn	José María López García Pepe López García
sn	López García
telephoneNumber	1789
mail	josem.lopez@empresa.com
jpegPhoto	nU6KNyVIYS817zVdf5YKF1FrNb...

Ejemplo de directorio LDAP



IES ESTEBÉ TERRADAS ILLA
SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA

jesesteveterradas.com

Ejemplo directorio LDAP

La definición de qué **atributos** forman parte del directorio se conoce como el **esquema** del directorio. A continuación se explica el significado de los anteriores atributos:

- **objectclass**. Especifica a qué clase pertenece el objeto.
- **Common name (cn)**. Nombre del usuario, puede tener más de un valor. En este caso, se considera nombre del usuario tanto José María, como Pepe.
- **Surname (sn)**. Es el apellido del usuario.
- **telephoneNumber**. Como su nombre indica, sirve para almacenar el número de teléfono del usuario.
- **mail**. Almacena la dirección de correo electrónico.
- **jpegPhoto**. Contiene una pequeña imagen del usuario.

En LDAP cada objeto se identifica mediante un nombre, el ***distinguished name (DN)***, formado por varios atributos y sus valores.



1.4 Operaciones de cliente

En este subapartado definimos las operaciones más frecuentes a nivel de interacción de un cliente con un servicio de directorio:

□ Operaciones de interrogación:

La operación de **búsqueda** (*search*) permite buscar en el directorio y obtener información de las entradas.

La herramienta puede ser mediante la línea de comandos, como **ldapsearch**.

```
ldapsearch -h ldap.ejemplo.com -s sub -b "ou=ingenieros" "(cn~=Juan Prados)"
```

En este caso se busca en el servidor ldap.ejemplo.com, dentro del apartado de ingenieros, la entrada correspondiente a un tal Juan Prados. La herramienta ldapsearch ha realizado una consulta al servicio de directorio que no ha precisado de una conexión autenticada o, lo que es lo mismo, ha usado una conexión anónima.



jesesteveterradas.com

1.4 Operaciones de cliente

- Operaciones de actualización: LDAP dispone de cuatro operaciones de actualización de datos: añadir, borrar, modificar y renombrar/mover.
- Operaciones de autenticación: La conexión a un directorio no está exenta de las implicaciones en la seguridad del propio servicio de directorio.

Por ejemplo, puede ser que la consulta de información sea pública para cualquier usuario, mientras que la modificación sea sólo posible para ciertos usuarios con rol de administradores del servicio de directorio.

Para realizar una conexión (operación bind), se especifica el DN de quien realiza la conexión. Se puede usar una contraseña para autenticación, así como distintos métodos de seguridad.

1.4 Operaciones de cliente

- Acceso desde otras aplicaciones: Otra forma en la que se encuentra disponible LDAP es como interfaz para implementar programas (API). De este modo, por ejemplo, en lenguaje C es posible usar funciones contra un servicio de directorio LDAP, como ldap_search(), ldap_bind(), ldap_add(), etc.



IES ESTEBÉ TERRADAS ILLA
SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA
TERRADAS ILLA

jesesteveterradas.com

2. Diseño del directorio

El espacio de nombres es un elemento estrechamente ligado con la organización de los objetos que incluye el directorio. En LDAP los objetos se identifican mediante una serie de valores específicos de atributos, en principio uno para cada nivel del espacio de nombres.

Será necesario tener claro qué elementos conviene almacenar para cada entrada, es decir, **cuáles serán los atributos que definirán los objetos del directorio.**

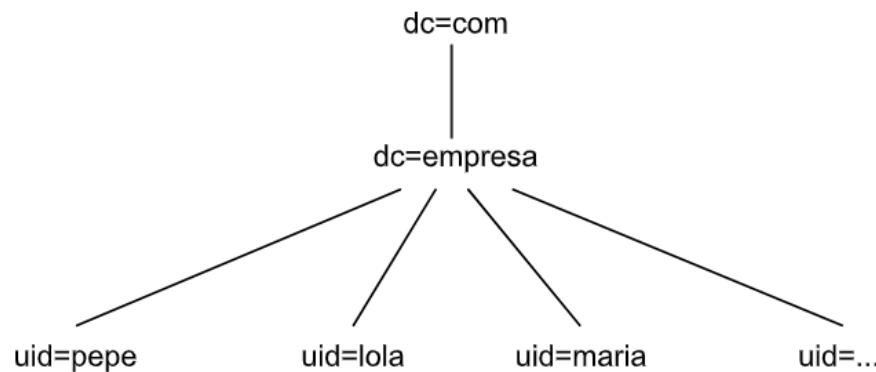
- Elección del sufijo:** lo importante es que el sufijo (el nombre de la parte "raíz" del árbol del directorio) identifique únicamente la organización. Se podría escoger la recomendación de la RFC 2247. En ella se especifica que es conveniente mapear en DN del directorio con el nombre DNS que la organización tenga asignado.

2. Diseño del directorio

□ Estructura del directorio plano:

El espacio de nombres más simple sería un espacio de nombres plano, por ejemplo, sin departamentos ni grupos de usuarios.

La figura siguiente muestra un espacio de nombres plano.

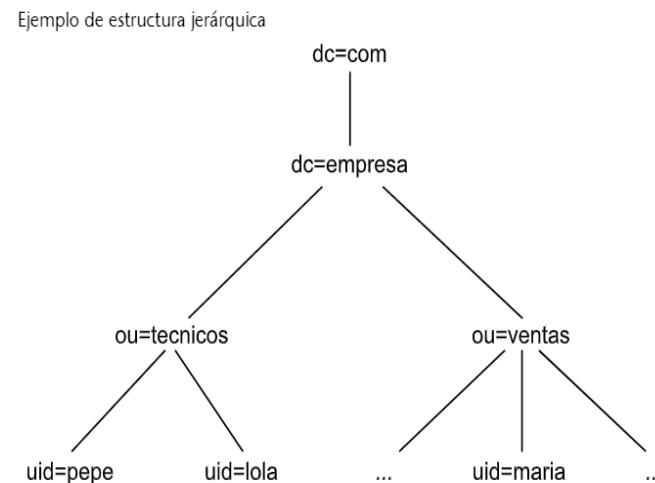


2. Diseño del directorio

Estructura del directorio jerarquizado:

En organizaciones que contemplan departamentos o distintos perfiles de usuarios, se aconseja crear unidades organizacionales (identificadas con el atributo "ou").

Además, distribuir los recursos en grupos puede ser útil, por ejemplo, para temas de control de acceso a recursos.



2. Diseño del directorio

Identificación de objetos en el directorio:

El último elemento que analizaremos sobre el diseño del espacio de nombres tiene que ver con la identificación de los objetos dentro del directorio.

Tal y como hemos visto, las restricciones que impone LDAP a la hora de identificar objetos son dos:

- El RDN de una entrada se formará a partir de un atributo (o más de uno, aunque no es recomendable).
- En RDN debe ser único entre las entradas "hermanas" (aquellas que penden del mismo padre en la estructura).

Aunque solamente haya establecidas estas dos restricciones, se aconseja en general que la identificación de los objetos (en especial cuando se trata de personas o usuarios) se haga a través **de un identificador único**.



2. Diseño del directorio

Esquema del directorio (schema):

- ✓ Hasta ahora hemos hablado de objetos en el sentido amplio de la palabra. Hemos visto que un directorio contiene entradas con sus distintos atributos.
- ✓ Una entrada representa a un objeto cuya información es almacenada en el directorio. Y se puede entrever que las entradas pueden ser de varios tipos: individuos, recursos, grupos, etc.

El **esquema del directorio** es la definición de qué tipos de objeto guarda un directorio y qué atributos se utilizan para su definición.

- ✓ Las implementaciones de servicios de directorio ya suelen incluir sus propias definiciones de esquema.
- ✓ En el decurso de este subapartado vamos a tratar los conceptos de **atributo** y **clase**, esenciales en la definición del esquema del directorio.

2. Diseño del directorio

Atributos:

Los atributos sirven directamente para guardar información (nombre de persona, número de teléfono, fotografía, etc.).

Para definir un atributo en LDAP, es preciso contar con una serie de información:

- Un nombre que identifica al atributo que se define. En caso de LDAP, ya hay algunos nombres estándar definidos (common name, telephoneNumber,etc.), algunos de ellos con una abreviatura también conocida (por ejemplo, "cn" para common name). LDAP no distingue entre mayúsculas y minúsculas.
- Un OID (identificador de objeto) que también identifique al atributo. Los OID son cadenas de números que permiten localizar de forma precisa un objeto de datos. Los OID también definen un espacio de nombres con una jerarquía.



Descripción de algunos de los atributos más habituales en LDAP

Atributo	Descripción
<i>cn, commonName</i>	Nombre del objeto. Si el objeto es una persona, sirve para especificar su nombre completo
<i>sn, surname</i>	Apellido de una persona
<i>serialNumber</i>	Número de serie de un dispositivo o recurso
<i>c, countryName</i>	Nombre del país usando dos caracteres, tal y como especifica la ISO 3166
<i>st, stateOrProvinceName</i>	Nombre del estado, provincia, comunidad autónoma, etc.
<i>street, streetAddress</i>	Dirección postal (calle, número, etc.)
<i>o, organizationName</i>	Nombre de la organización
<i>ou, organizationalUnitName</i>	Nombre del departamento u otra unidad organizacional



IES
ESTEVE TERRADAS
Illa
TERRADAS ILLA
SEP ESTEVE TERRADAS
Illa TERRADAS ILLA SEP ESTEVE

jesesteveterradas.com

<i>title</i>	Título de la persona dentro de una organización (presidente, director, etc.)
<i>description</i>	Descripción del objeto, de forma comprensible para los humanos
<i>postalCode</i>	Código postal
<i>telephoneNumber</i>	Número de teléfono
<i>preferredDeliveryMethod</i>	Descripción de cómo quiere una persona que se le entregue información (por ejemplo, por fax o e-mail)
<i>member</i>	Se trata de un DN que indica de quién es miembro el objeto en el árbol del directorio
<i>uid, userid</i>	Identificador de usuario, en general usado para autenticarse en un servicio o sistema



IE
ADASTILLA
SEP ESTEVE TERRA
SEP ESTEVE TERRADAS I ILLA
SEP ESTEVE TERRADAS I ILLA
TERRADAS I ILLA

jesesteveterradas.com

2. Diseño del directorio

Clase de objeto:

Una vez los atributos han sido definidos, se pueden utilizar clases de objetos para definir cómo son las entradas del directorio.

Una clase de objeto es un atributo de una entrada. Especifica los atributos que puede tener la entrada.

Un identificador de clase de objeto es un valor único que identifica una clase de objeto.

Para definir una clase de objeto, se debe especificar su identificador de objeto, un nombre, un nombre alternativo, una subclase, un tipo de clase de objeto, una lista de atributos debe contener y una lista de atributos puede contener o conjuntos de atributos, y una descripción.





3. Implementaciones de servicio de directorio

3. Implementacion de servicio de directorio

Después de realizar una aproximación teórica al concepto, diseño y usos de los servicios de directorio, y de haber estudiado el sistema LDAP, vamos a estudiar dos casos concretos de implementación:

- **El Active Directory:** Si Windows NT usaba el NetBIOS como mecanismo primario de comunicación de red (y el WINS como base de datos de nombre de objetos de red), el Active Directory requiere el uso de TCP/IP, así como del servicio DNS.
- **El OpenLDAP:** OpenLDAP es una implementación de un servicio de directorio basado en LDAP bajo la filosofía de software libre y código abierto. El proyecto OpenLDAP es quien se encarga de su desarrollo y sus productos se hallan disponibles en multitud de distribuciones GNU/Linux.

3. Implementacion de servicio de directorio

- **El OpenLDAP:** El servidor `slapd` ejecuta las funciones de servicio de directorio. Se encarga de interaccionar con el backend (almacén de datos) correspondiente.

OpenLDAP permite la replicación de contenidos. Actualmente, se utilizan los términos de proveedor y consumidor de actualizaciones. Esto permite definir mejores reglas de actualización, haciendo posible que un servidor pueda actuar de proveedor o bien de consumidor en función de la necesidad.

El motor de sincronización para OpenLDAP es **syncrepl**, que usa como protocolo el **LDAPSync**.

4. Conceptos relacionados

Una vez que disponemos de una idea global del concepto de directorio, es conveniente que hagamos un repaso de la terminología que vamos a emplear cuando hablamos de Servicios de directorio:

- Dominio:** Un Dominio es una **colección de objetos** dentro del directorio que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un **bosque**, cada uno de ellos con su propia colección de objetos y unidades organizativas.
- Objeto:** La palabra Objeto se utiliza como nombre genérico para referirnos a cualquiera de los componentes que forman parte del directorio, como una impresora o una carpeta compartida, pero también un usuario, un grupo, etc.

Nota: Como veremos más adelante, las características específicas de cada tipo de objeto quedarán definidas en el Esquema de la base de datos



4. Conceptos relacionados

En general, los objetos se organizan en tres categorías:

- q Usuarios: identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración.
- q Recursos: que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus privilegios. Por ejemplo, carpetas compartidas, impresoras, etc.
- q Servicios: que son las diferentes funciones a las que los usuarios pueden tener acceso. Por ejemplo, el correo electrónico.

IMPORTANTE

Definición de usuario:

Desde un punto de vista informático, un usuario es un conjunto de permisos y de privilegios sobre determinados recursos.

En este sentido, un usuario no tiene que ser, necesariamente, una persona.

4. Conceptos relacionados

Controlador de dominio: Un Controlador de dominio (domain controller) contiene la **base de datos de objetos del directorio para un determinado dominio**, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control.

En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.



RECUERDA
Cuando instalamos Active Directory en un ordenador con Windows Server 2008, convertimos a ese ordenador en un Controlador de dominio.

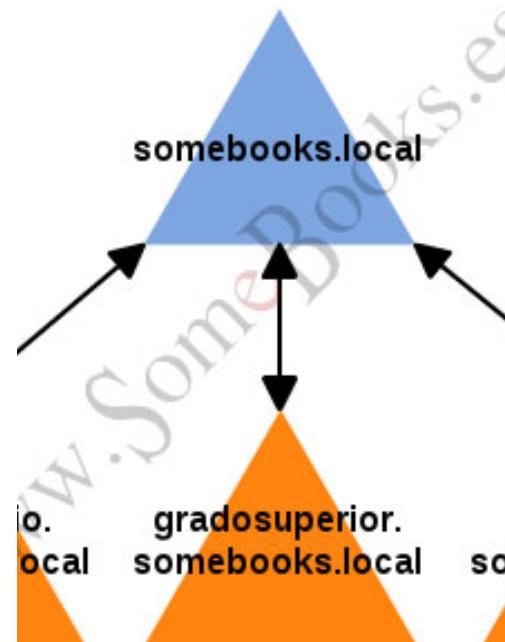
4. Conceptos relacionados

Árboles:

Un Árbol es simplemente una **colección de dominios** que dependen de una raíz común y se encuentran organizados como una determinada jerarquía.

De esta forma, sabremos que los dominios somebooks.es e informatica.somebooks.es forman parte del mismo árbol, mientras que sliceoflinux.com y somebooks.es no.

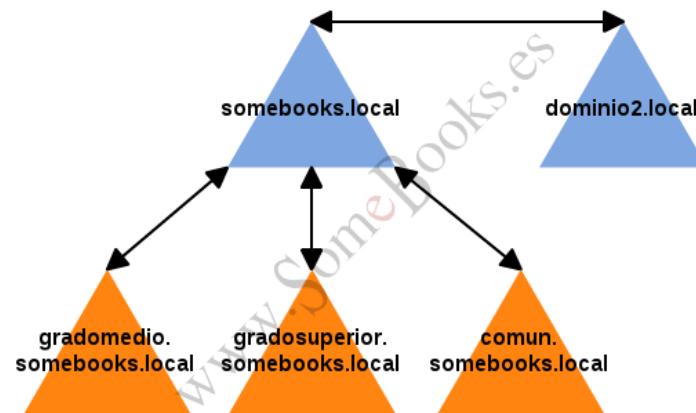
El objetivo de crear este tipo de estructura es fragmentar los datos del Directorio Activo, replicando sólo las partes necesarias y ahorrando ancho de banda en la red.



4. Conceptos relacionados

Bosque:

Un bosque es una agrupación de varios dominios Active Directory y posee un único esquema. El primer dominio instalado en un bosque se llama dominio raíz del bosque. Varios árboles de dominio cuyo espacio de nombres no es continuo representan un bosque.



alias *m* Entrada que en realidad enlaza con otra entrada del directorio.

atributo *m* Parte de la entrada destinada a guardar una pieza de información, como por ejemplo un apellido o un número de teléfono.

base *f* En la operación de búsqueda especifica, desde qué entrada u objeto se quiere empezar a buscar información.

búsqueda *f* Operación básica de interrogación al servicio del directorio, mediante la cual se obtiene información conforme una serie de criterios.

DAP (directory access protocol) *m* Sistema primitivo de implementación y gestión de directorios, basado en la especificación X.500.

directorio *m* Tipo especializado de base de datos jerárquica que organiza y almacena datos acerca de elementos (entradas de directorio).

distinguished name (DN) *m* Relación de DN relativos que identifican únicamente una entrada en un directorio LDAP.

DN relativo *m* Atributo y su valor que identifican a una entrada para un nivel en concreto del árbol del directorio.

esquema *m* Definición de qué tipos de objeto guarda un directorio y los atributos usados en la definición de los objetos.

Glosario



IES ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA
IES SEP ESTEBÉ TERRADAS ILLA

jesesteveterradas.com

Glosario

esquema *m* Definición de qué tipos de objeto guarda un directorio y los atributos usados en la definición de los objetos.

LDAP (*Lightweight DAP*) *f* Interfaz entre clientes de directorio y sistemas DAP, que luego evolucionó hacia un servicio de directorio.

objectclass *m* Atributo de una entrada de directorio basado en LDAP que especifica a qué clase pertenece la entrada (por ejemplo, "person").

servicio de directorio *m* Plataforma que proporciona métodos para gestionar y almacenar los datos que contiene el directorio.

sufijo *m* DN para la raíz del árbol de directorio.

user identifier *m* Atributo específico para guardar el "login" de un usuario de un sistema informático.



IES ESTEBÉ TERRADAS ILLA
IES ESTEBÉ TERRADAS ILLA
IES ESTEBÉ TERRADAS ILLA
IES ESTEBÉ TERRADAS ILLA

jesesteveterradas.com



Protocol d'Accés al Servei de Directori als sistemes Windows

SISTEMES MICROINFORMÀTICS EN XARXA

M4. UF1. INSTAL·LACIÓ I ADMINISTRACIÓ DE SO OPERATIUS EN XARXA PROPIETARIS



[jesesteveterradas](http://jesesteveterradas.com).com

Windows Server Active Directory

► CONTINGUTS

- ▶ Conceptes bàsics d'Active Directory
 - ▶ Introducció
 - ▶ Estructura
 - ▶ Topologia de xarxa
- ▶ Webgrafia i/o material

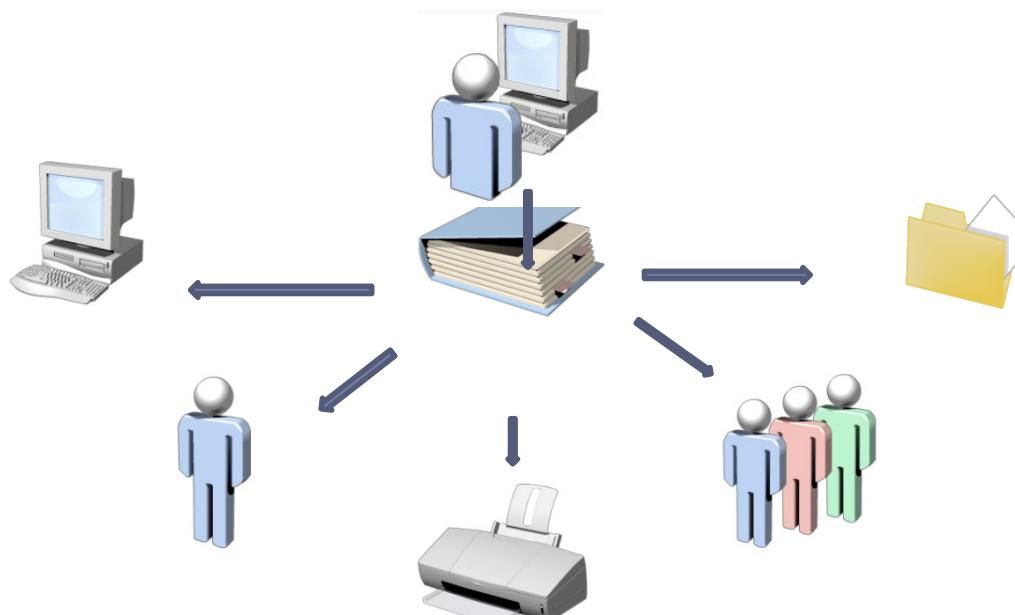


jesesteveterradas.com

Conceptes bàsics d'Active Directory

► INTRODUCCIÓ (I)

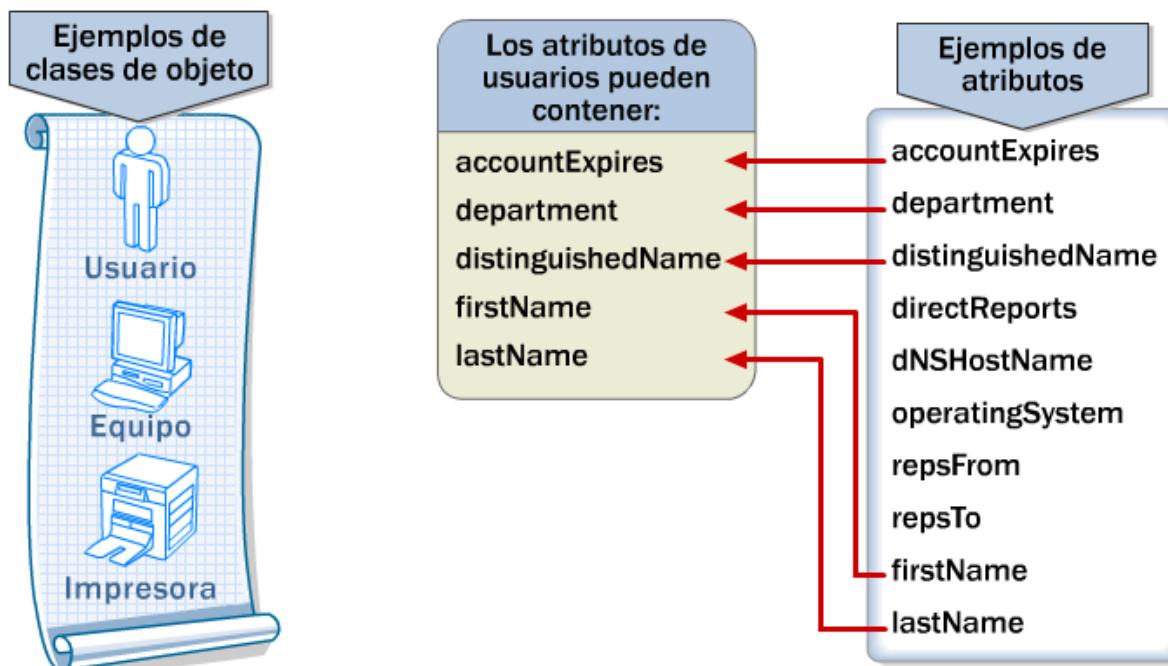
- ▶ Active Directory és el servei de directori utilitzat en Windows Server
- ▶ Un servei de directori emmagatzema informació sobre tots els recursos de la xarxa, com usuaris, grups, equips, arxius, impressores i aplicacions.
- ▶ A més, proporciona tots els serveis que fan que la informació estigui disponible i sigui útil.



Conceptes bàsics d'Active Directory

► INTRODUCCIÓ (II)

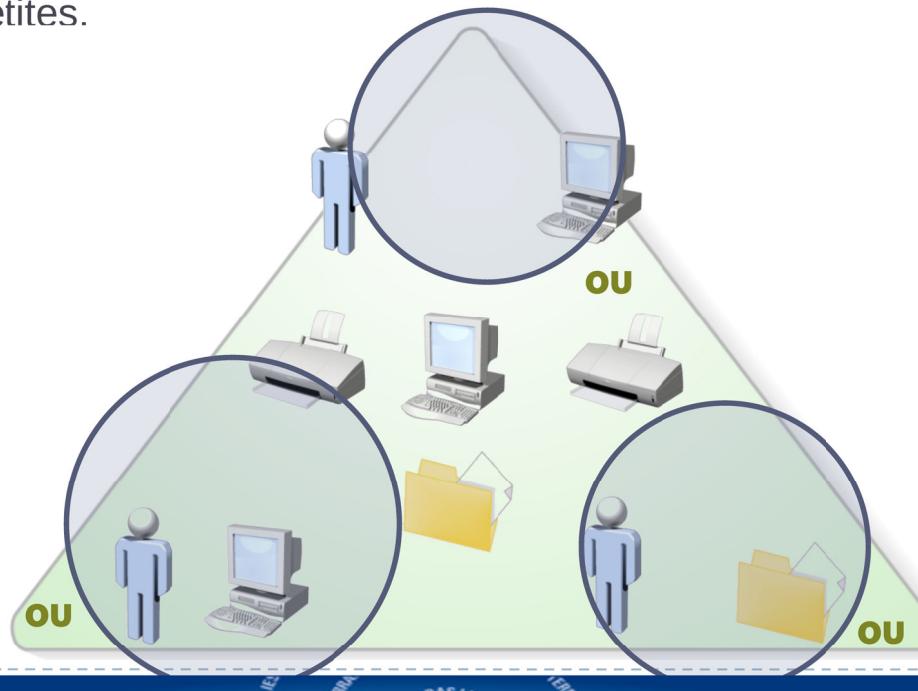
- ▶ Active Directory emmagatzema informació sobre els diferents objectes en una estructura jeràrquica.
- ▶ Cada objecte té atributs, com el nom d'usuari, cognom i direcció de correu; o número i ubicació de les impressores actives, la combinació dels quals fa que defineixi de forma única cadascun d'aquests objectes.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (I)

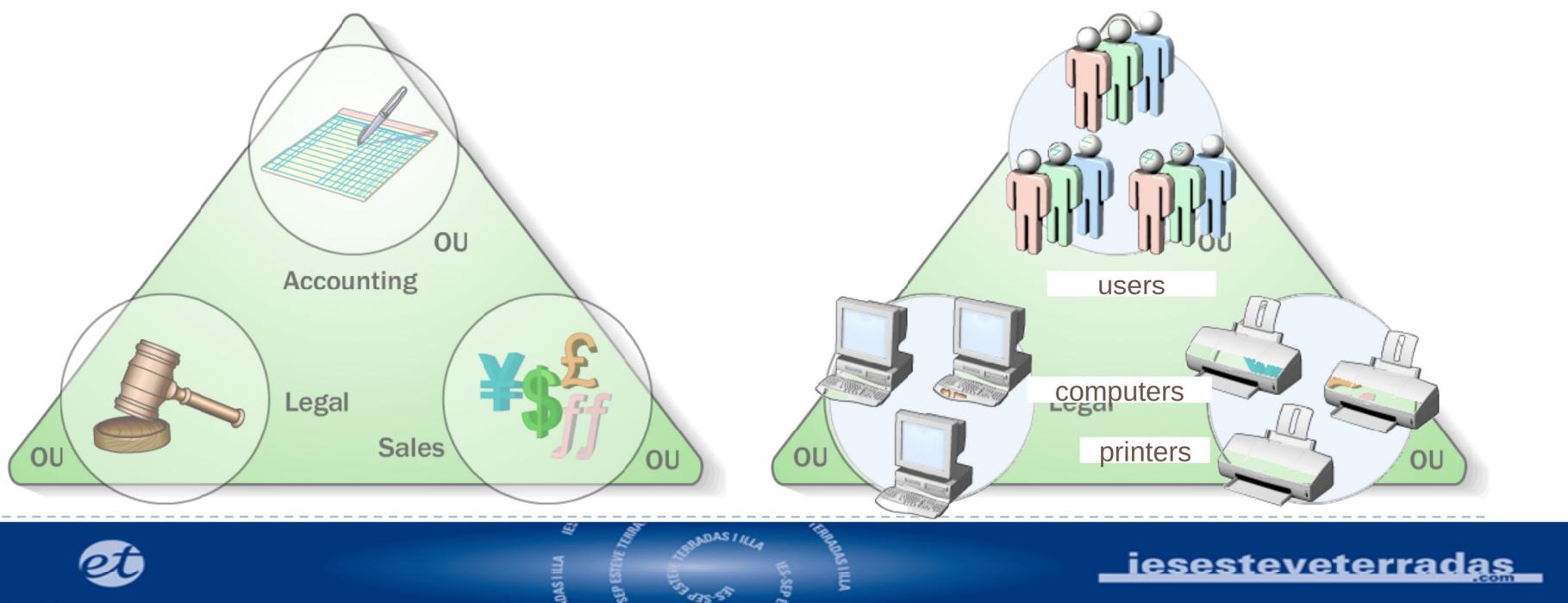
- ▶ Els objectes es mantenen en un domini que és la unitat bàsica de la organització i seguretat d'Active Directory.
- ▶ En un domini, els objectes s'organitzen en contenidors lògics anomenats unitats organitzatives o OU.
- ▶ Mitjançat les OU, es pot crear una jerarquia que repliqui l'estructura d'una organització. I el que és més important, es poden delegar algunes responsabilitats administratives a unitats més petites.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (II)

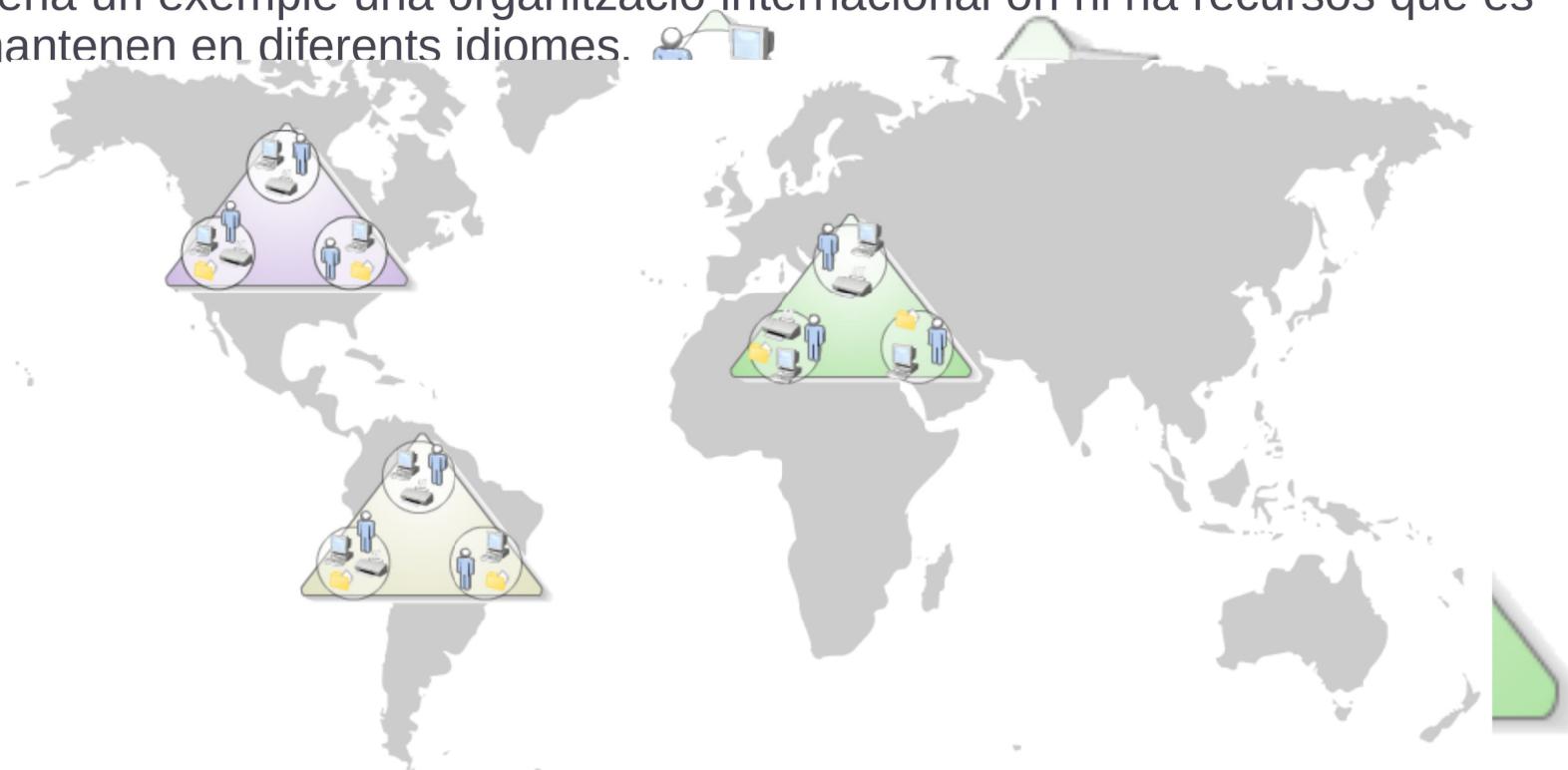
- ▶ Les OU poden seguir diferents models jeràrquics segons la utilitat que vulguem donar.
- ▶ Podem trobar OU organitzades segons la unitat empresarial o segons el tipus d'objectes que conté.
- ▶ A més a més, les OU és poden niar unes dintre de les altres facilitant encara més la seva administració a través de regles administratives i de seguretat aplicades sobre una OU primària.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (III)

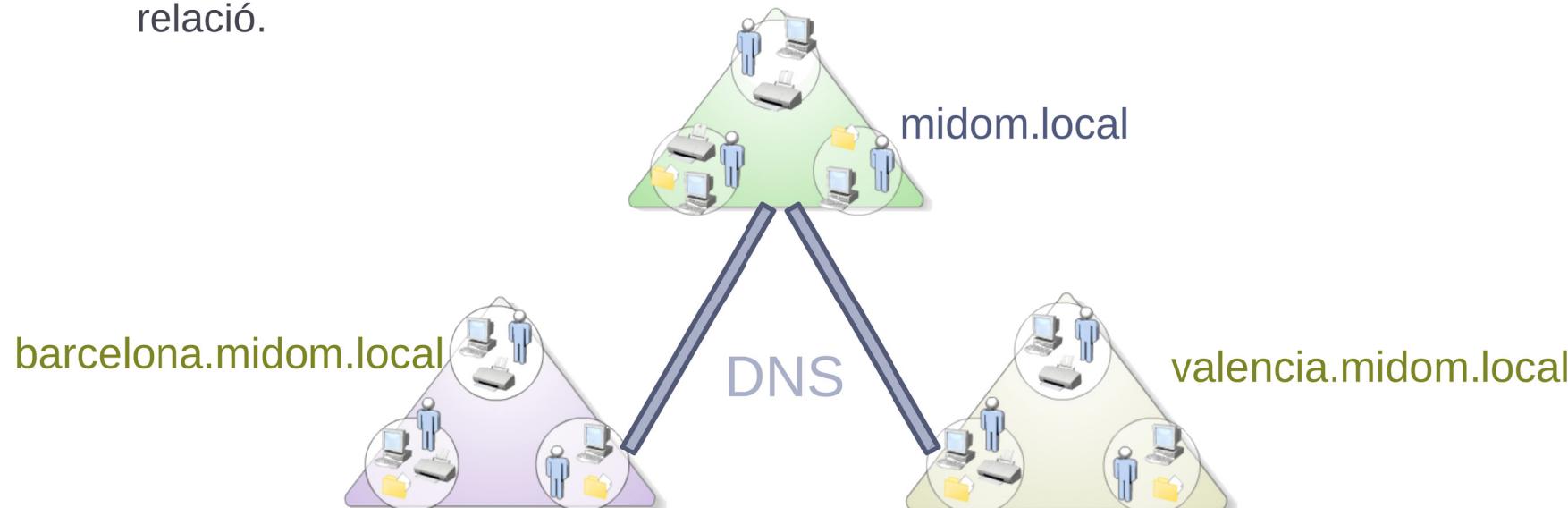
- Tot i que les OU són útils per delegar responsabilitats administratives en un domini, els dominis múltiples són útils en xarxes on l'administració es realitza per diferents autoritats.
- Seria un exemple una organització internacional on hi ha recursos que es mantenen en diferents idiomes.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (IV)

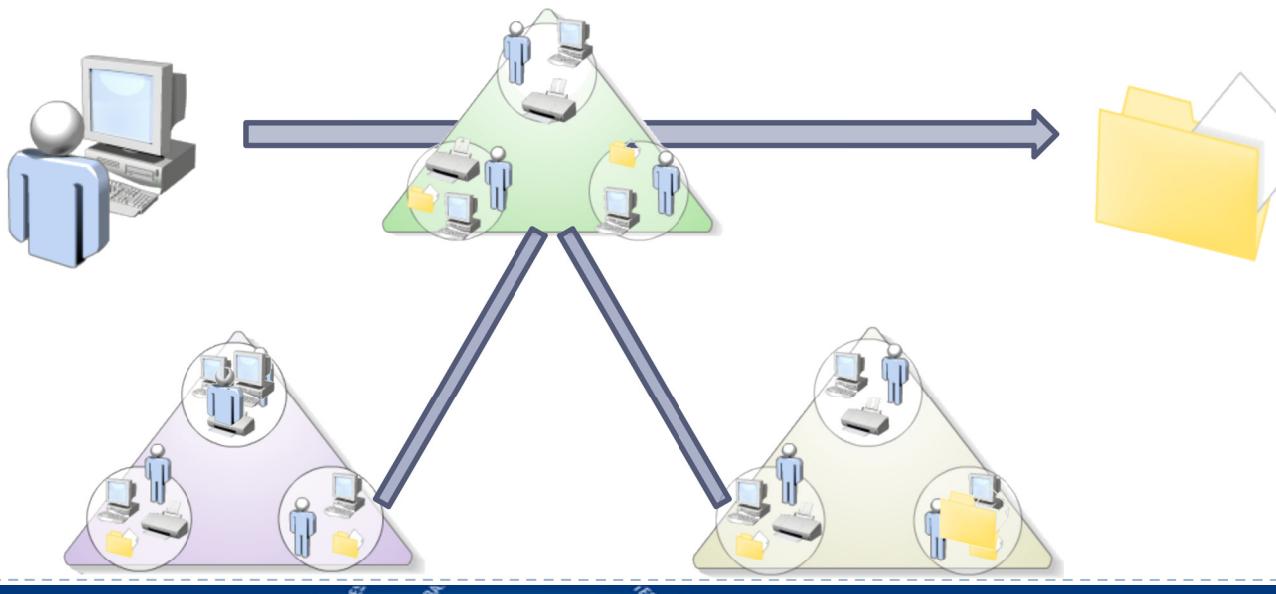
- Els dominis múltiples poden formar un arbre de dominis. El domini arrel es crea el primer i serà el domini principal dels dominis secundaris agregats sota ell.
- A cada domini d'un arbre se li assigna un nom mitjançant el Sistema de Noms de Domini jeràrquic o DNS. Quan anem agregant dominis al arbre, el nom del domini secundari s'agrega al nom del domini principal, reflectint així la seva relació.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (V)

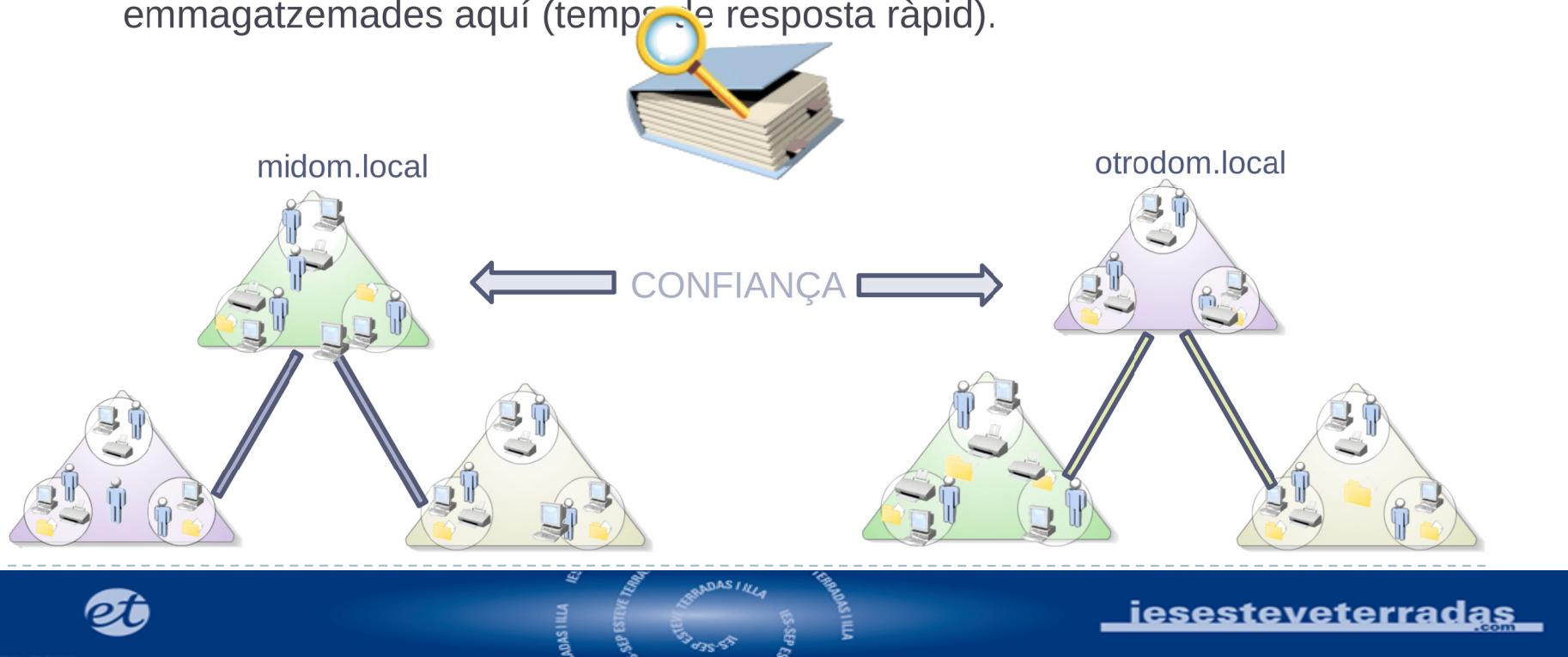
- ▶ Perquè els recursos de xarxa estiguin globalment disponibles pels usuaris, de manera predeterminada Active Directory afegeix dominis transparentment a través de relacions de confiança transitiva.
- ▶ Les relacions de confiança fan que els recursos d'un domini estiguin disponibles per a usuaris d'altres dominis, sempre és clar, que no tinguin l'accés restringit.
- ▶ La relació transitiva significa que les relacions de confiança es poden estendre automàticament a altres dominis del arbre.



Conceptes bàsics d'Active Directory

► ESTRUCTURA (VI)

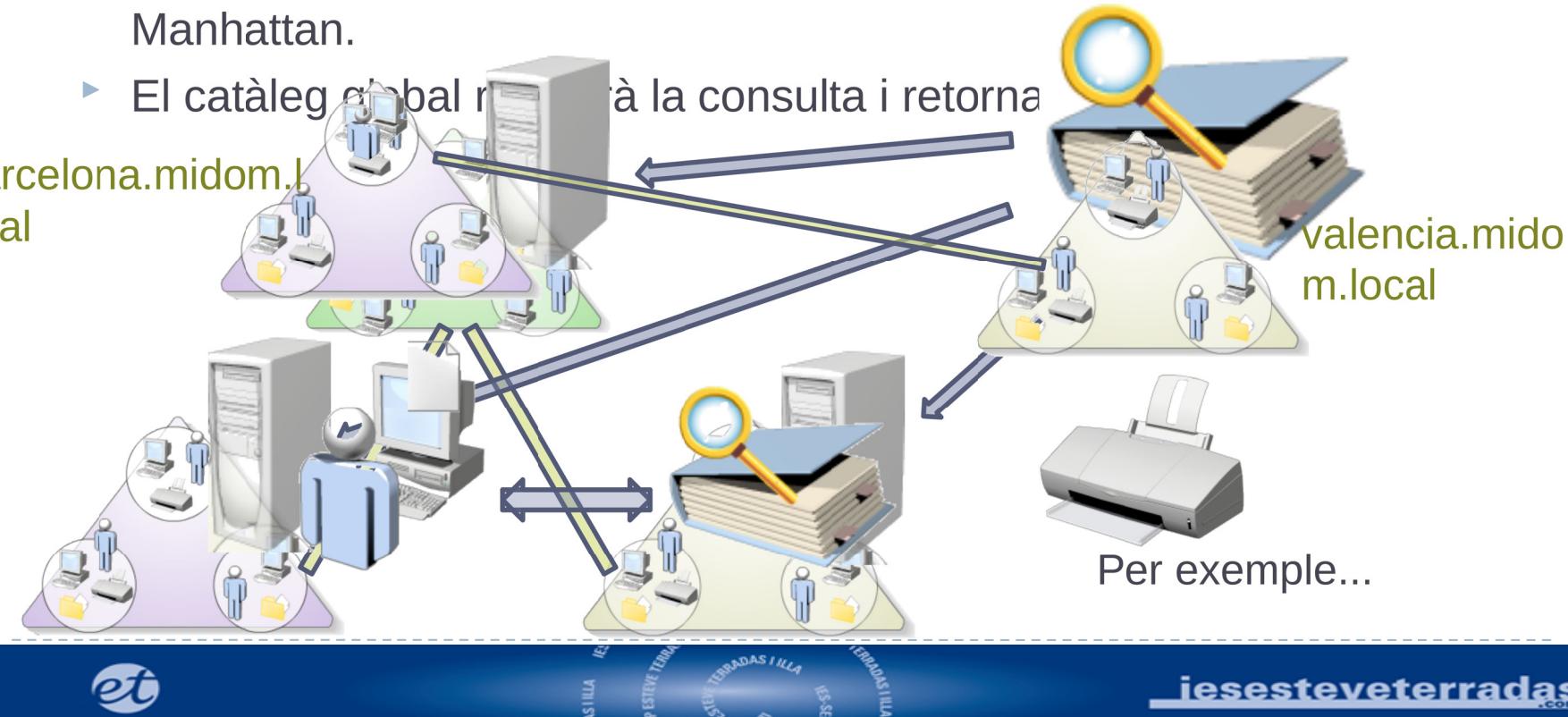
- ▶ El model d'arbre de dominis múltiples es pot estendre fins crear un bosc d'arbres en organitzacions en les que calgui mantenir estructures separades.
 - ▶ Els arbres d'un bosc comparteixen: relacions de confiança transitives entre dominis del bosc, esquema comú i un catàleg global general.
 - ▶ Tots els objectes de directori de la empresa estan representats en el catàleg global (es poden localitzar), però tant sols un subconjunt de les propietats són emmagatzemades aquí (temp de resposta ràpid).



Conceptes bàsics d'Active Directory

► ESTRUCTURA (VII) – Exemple

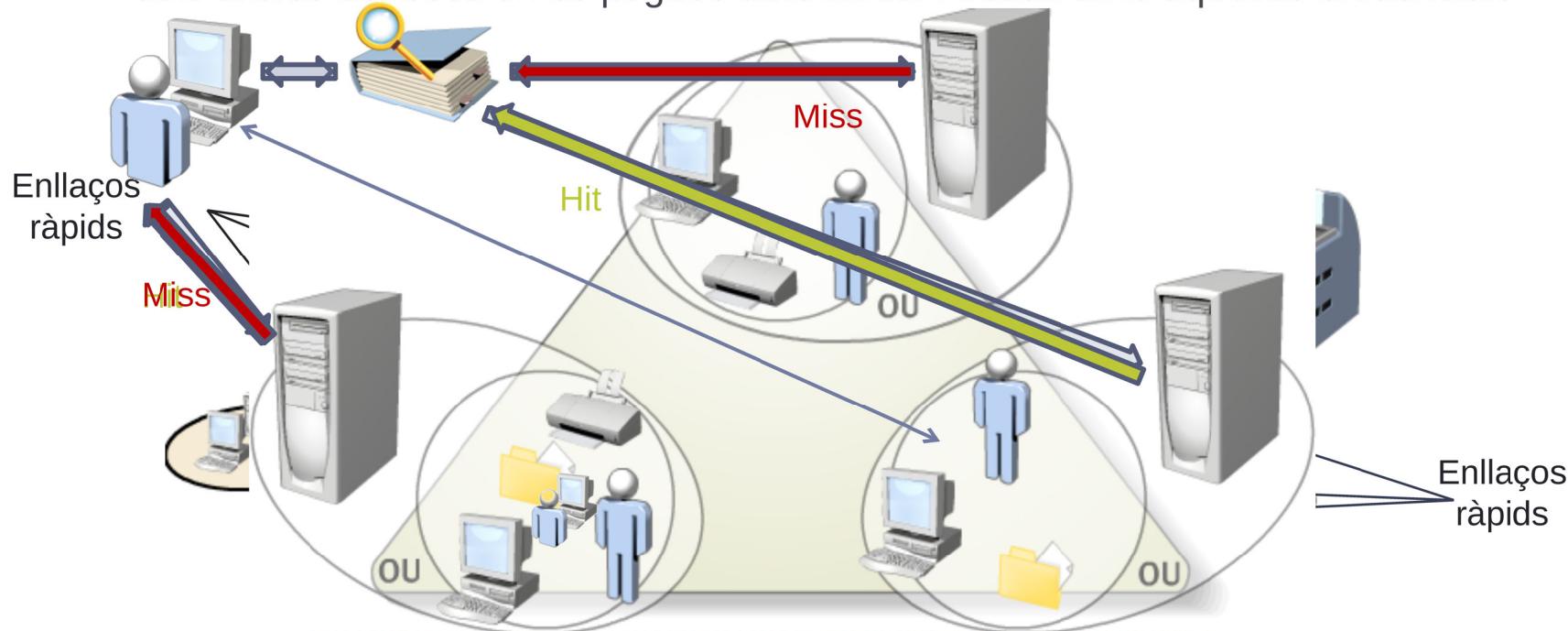
- ▶ Un empleat de l'oficina de Barcelona vol enviar una copia impresa a la subsidiària de New York.
 - ▶ Consultarà el catàleg global d'Active Directory per buscar una impressora a la segona planta de l'oficina de la 7th Avenue en Manhattan.
 - ▶ El catàleg global resoldrà la consulta i retorna



Conceptes bàsics d'Active Directory

► TOPOLOGIA DE XARXA (II) – Exemple

- Un usuari vol iniciar sessió, Windows Server intentarà trobar un controlador de domini en el mateix lloc del usuari per validar la seva petició.
- En cas de trobar-lo farà l'inici ràpidament i sense saturar de càrrega el catàleg global.
- Si no es dona una resposta positiva, cercaria al catàleg global un domini en algun dels arbres del bosc on es pogués autentificar l'usuari amb aquelles credencials.

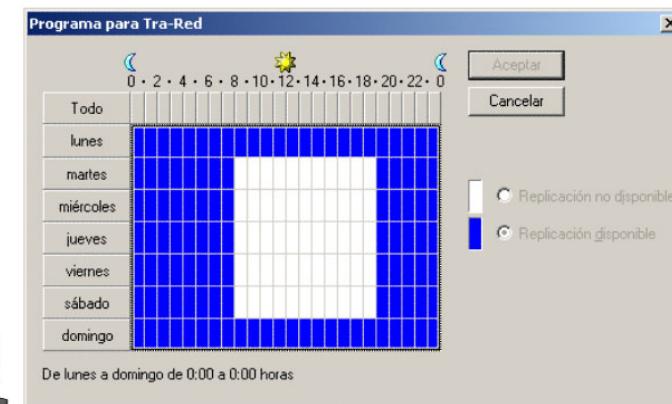
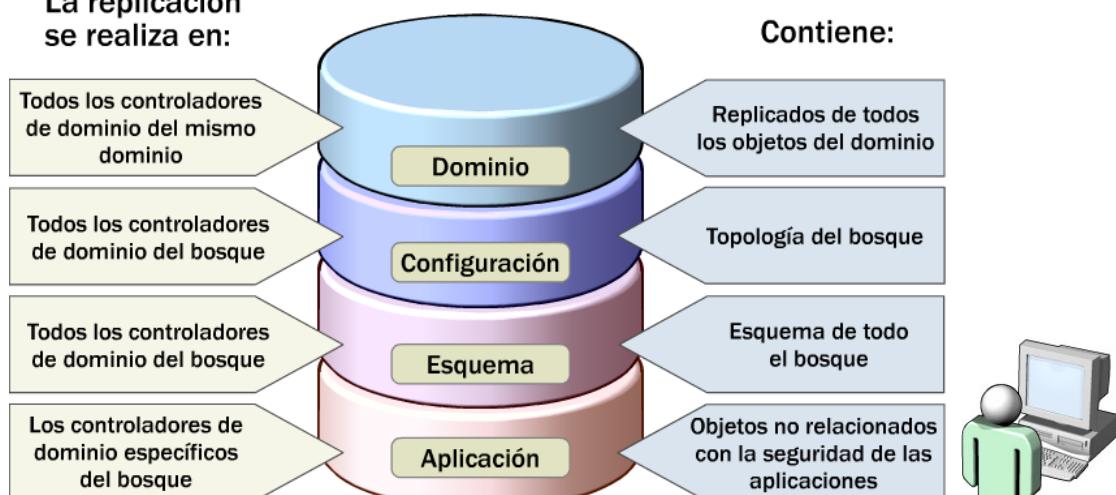


Conceptes bàsics d'Active Directory

► TOPOLOGIA DE XARXA (III)

- ▶ Cada lloc contindrà com a mínim un controlador de domini que executarà Active Directory i farà les funcions de replicació de la informació.
- ▶ Així amb una gestió acurada dels llocs segons l'enllaç (ràpid o lent) farà disminuir la latència, o temps que es triga en replicar un canvi d'un controlador de domini en la resta.
- ▶ Per exemple: replicar entre llocs units per enllaços lents només a determinades hores.

La replicación se realiza en:



Webgrafia i/o material

- ▶ <http://www.tech-faq.com/active-directory.html>
- ▶ <http://technet.microsoft.com/en-us/library/bb727030.aspx>
- ▶ http://delreguero.com/wordpress/wp-content/uploads/ASO/otros/01_intro_infraestruct_DA/media08_1.htm



jesesteveterradas.com

añadir Linux AD net ads tutorial

dominio patosa.com

Controlador de dominio
winser2012AD → 172.16.0.201
cliente linux
clienteWin2012 → 172.16.0.110

Lo primero de todo le ponemos nombre a la maquina:

hostnamectl set-hostname clienteWin2012

instalamos resolvconf para poder establecer el controlador de dominio como DNS y que no nos lo machaque otro programa

apt install resolvconf

y configuramos nuestro DNS

cat /etc/resolvconf/resolv.conf.d/head

domain patosa.com
search patosa.com
nameserver 172.16.0.201
nameserver 8.8.8.8

cat /etc/resolv.conf

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
domain patosa.com
search patosa.com
nameserver 172.16.0.201
nameserver 8.8.8.8
nameserver 192.168.0.1
```

iniciamos servicio, por defecto estará habilitado pero no levantado

systemctl status resolvconf.service

systemctl start resolvconf.service

comprobamos que ha modificado nuestro archivo </etc/resolv.conf>

modificamos el archivo </etc/hosts>

cat /etc/hosts

```
127.0.0.1 localhost
127.0.1.1 clienteWin2012.patosa.com clienteWin2012
172.16.0.201 winser2012AD.patosa.com winser2012AD
```

The following lines are desirable for IPv6 capable hosts

```
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Establecemos ip estatica:

cat /etc/network/interfaces

```
auto lo
iface lo inet loopback
```

```
auto enp0s3
iface enp0s3 inet static
address 172.16.0.110/24
```

reiniciamos la red:

systemctl restart networking

comprobamos la ip

ip address

comprobamos que podemos acceder al controlador de dominio

ping winser2012AD

actualizamos lista paquetes

apt update

instalamos software necesario:

apt-get -y install ntp vim ntpdate winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user

If your computer gets IP address information from a DHCP server on the network, the DHCP server may also on the network. This requires a change to your smb.conf file so that DHCP-provided WINS settings will au

The dhcp-client package must be installed to take advantage of this feature.

Modify smb.conf to use WINS settings from DHCP?

<Yes>

no queremos recuperar información de ningun DHCP

Nos preguntará sobre la configuración de kerberos:

Configuring Kerberos Authentication

When users attempt to use Kerberos and specify a principal or user name without specifying what administrative Kerberos realm that principal belongs to, the system appends the default realm. The default realm may also be used as the realm of a Kerberos service running on the local machine. Often, the default realm is the uppercase version of the local DNS domain.

Default Kerberos version 5 realm:

PATOSA.COM

<Ok>

ponemos nuestro dominio patosa.com en mayúsculas

También nos preguntará por el kerberos server (nuestro controlador de dominio)

Configuring Kerberos Authentication

Enter the hostnames of Kerberos servers in the PATOSA.COM Kerberos realm separated by spaces.

Kerberos servers for your realm:

winser2012AD.patosa.com

<Ok>

igual cuando nos pregunte por el kdc server

editamos /etc/ntp.conf
cambiamos todos los pool por:
pool winser2012AD.patosa.com

service ntp restart

modificamos nuestro fichero de configuración de kerberos:

cp /etc/krb5.conf /etc/krb5.conf_original

Lo editamos y dejamos como sigue:

```
[libdefaults]
default_realm = PATOSA.COM
dns_lookup_realm = true
dns_lookup_kdc = true
renew_lifetime = 7d

[realms]
PATOSA.COM = {
    kdc = winser2012AD.PATOSA.COM:88
    admin_server = winser2012AD.PATOSA.COM:464
    default_domain = PATOSA.COM
}

[domain_realm]
.PATOSA.COM = winser2012AD.PATOSA.COM
PATOSA.COM = winser2012AD.PATOSA.COM

[appdefaults]
pam = {
    debug = true
}
```

```

ticket_lifetime = 36000
renew_lifetime = 36000
forwadable = true
krb4_convert = false
}
[login]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

```

comprobamos que nos podemos autenticar con un usuario del active directory:

kinit administrador

Password for administrador@PATOSA.COM:

Si no nos da error, es que ha ido todo bien.

Si ejecutamos klist, comprobamos que se nos ha creado un ticket:

klist

Ticket cache: FILE:/tmp/krb5cc_0

Default principal: administrador@PATOSA.COM

Valid starting Expires Service principal

02/03/21 07:32:04 02/03/21 17:32:04 krbtgt@PATOSA.COM@PATOSA.COM

renew until 09/03/21 07:31:38

modificamos la configuracion de nuestro samba:

cp /etc/samba/smb.conf /etc/samba/smb.conf_original

dejamos la sección [global] como sigue:

```

[global]
workgroup = PATOSA
security = ADS
realm = PATOSA.COM
encrypt passwords = yes
idmap config * : backend = tdb
idmap config * : range = 2000-3000
winbind trusted domains only = no
winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes
winbind refresh tickets = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
idmap uid = 2000-29999
idmap gid = 2000-29999
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
winbind refresh tickets = yes

```

winbind nss info = rfc2307

modificamos el archivo nsswitch.conf

cat /etc/nsswitch.conf

```

passwd: compat winbind
group: compat winbind
shadow: compat winbind
gshadow: files
.
.
.
```

Es posible que al reiniciar los servicios de samba

service smbd restart

service nmbd restart

service winbind restart

nos aparezca el siguiente error:

cat /var/log/samba/log.smbd

ERROR: failed to setup guest info.

resolucion

groupadd nobody

net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type= builtin

Successfully added group nobody to the mapping db as a wellknown group

nos unimos al dominio

net join ads -U administrador

es posible que nos aparezca el error:

Failed to join domain: failed to find DC for domain ads - {Operation Failed} The requested operation was unsuccessful.

en ese caso ejecutamos:

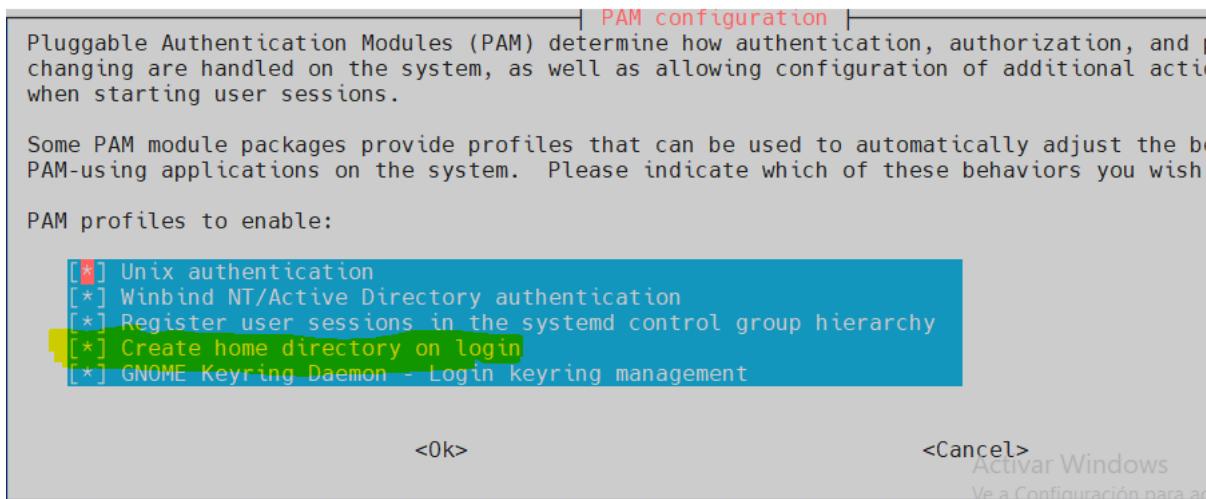
```
net join ads -U administrador -S winser2012AD.patosa.com
```

podemos ir a nuestro controlador de dominio y comprobar que nos ha creado la maquina

```
root@clienteWin2012:~# wbinfo -g
could not obtain winbind interface details: WBC_ERR_WINBIND_NOT_AVAILABLE
could not obtain winbind domain name!
failed to call wbcListGroups: WBC_ERR_WINBIND_NOT_AVAILABLE
Error looking up domain groups
```

ejecutamos:

```
pam-auth-update
```



reiniciar los servicios de samba

```
service smbd restart
```

```
service nmbd restart
```

```
service winbind restart
```

wbinfo -g

```
winrmremotewmiusers_
```

equipo del dominio

controladores de dominio

administradores de esquema

administradores de empresas

wbinfo -u

administrador

invitado

krbtgt

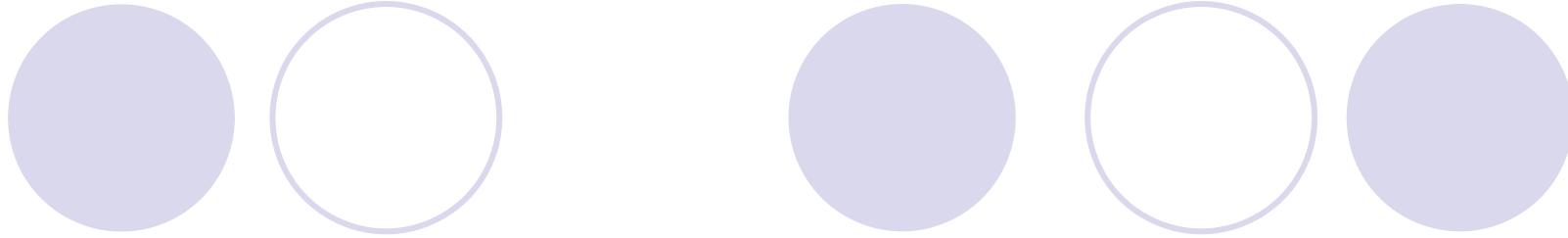
jernesto

usuariodomnio

en estos momento es muy probable que no nos deje loguearnos en modo grafico, rebotamos la máquina y probamos:



Autenticació centralitzada amb tecnologia LDAP



El problema de l'Administració d'Identitats

El problema d'Administració de Identitats

- Cada usuari té múltiples identitats en la empresa
- Múltiples administradors per a cada usuari
- No existeix un mètode segur per a compartir les identitats d'usuaris entre ambients linux, UNIX® i Windows®
- No existeix un únic punt de administració per a cada usuari

Costos en Seguretat i Taula d'Ajuda



- **Un usuari promig utilitza 5+ claus**
- **55% dels usuaris escriu la clau en paper al menys una vegada**
- **9% de tots els usuaris escriuen en paper totes les claus**
- **51% de tots els usuaris requereixen ajuda de TI per què oblidien la seva clau**
- **25% de tots els consultats a les taules d'ajuda estan relacionades amb claus**

Procés Tradicional de Maneig d'Identitats



Username: brucem
Password: hockey1



Solaris



Username: bmackay
Password: hockey1



Windows



Username: brucem
Pass: hockey1

AIX

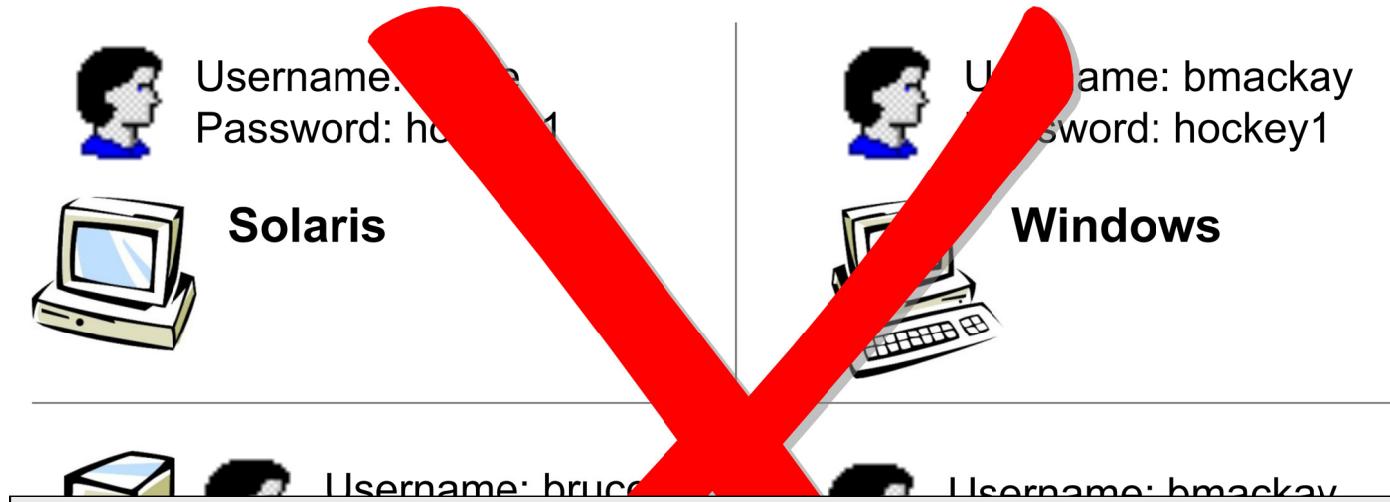


Username: bmackay
Password: hockey1



Linux

Procés Tradicional de Maneig d'Identitats



Problema:

- 4 noms d'usuaris diferents
- 4 eines de Admin. diferents
- 4 llocs diferents on es guarden les claus

Autenticació Tradicional

- /etc/passwd
- NIS
- PAM/NSS

Autenticació /etc/passwd

```
login: juana  
Password: ***
```

```
getpwnam("juana")
```

```
crypt()
```

```
strcmp()
```

/etc/passwd
/etc/shadow

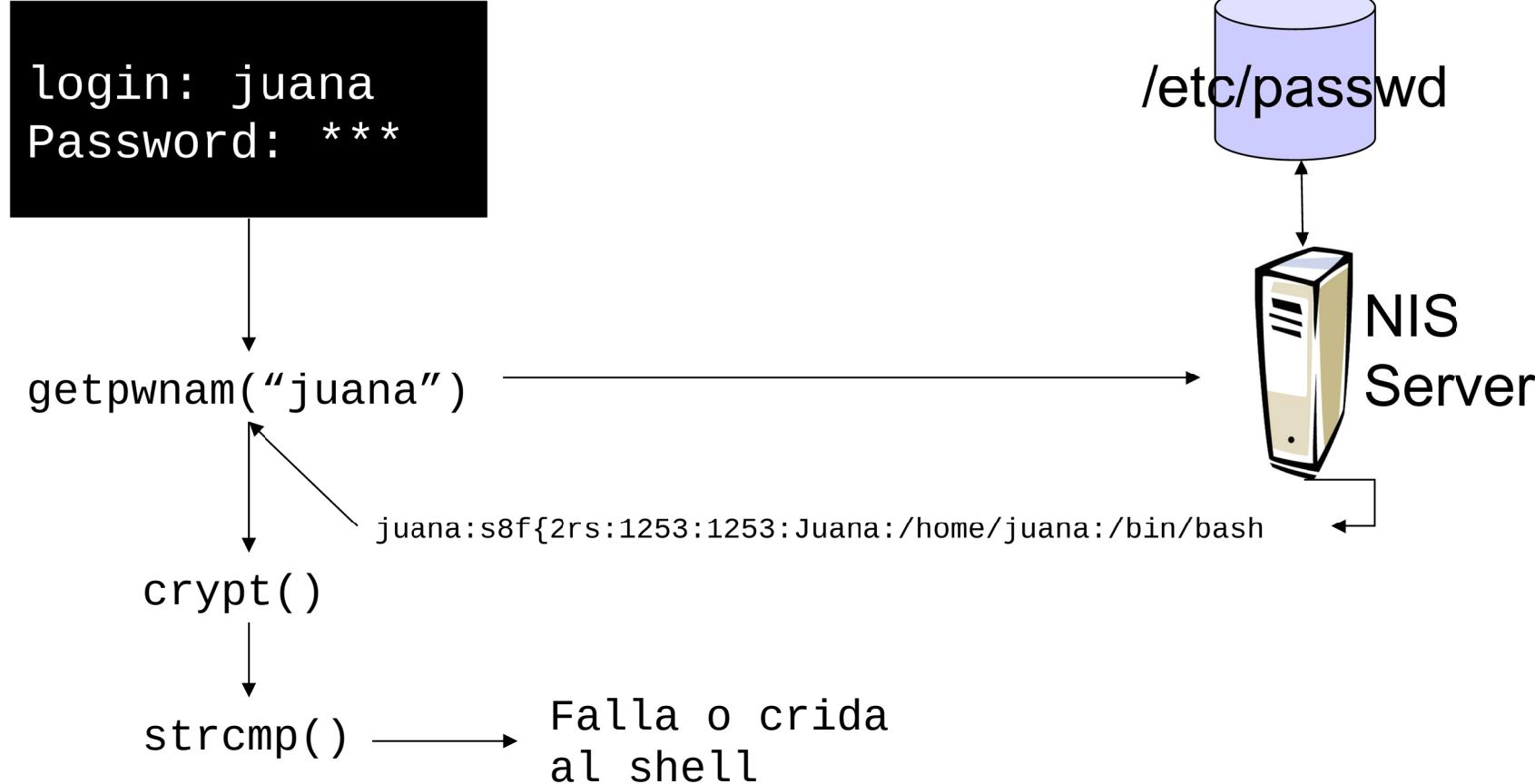
juana:w8f{2rs:1253:1253:Juana la loca:/home/juana:/bin/bash

Falla o crida
el shell del
usuari

/etc/passwd Pros/Contres

- Avantatges:
 - Molt simple
- Desavantatges:
 - Dissenyat per a autenticació local
 - Cada màquina ha de tenir l'arxiu /etc/passwd
 - El mateix arxiu ha de replicar-se per a les comptes comuns
 - /etc/passwd no és extensible

Network Information System NIS



NIS Pros/Contres

Avantatges:

- Permet distribuir l'arxiu mestre /etc/passwd i /etc/shadow entre diferents servidors
- Compatible amb la majoria de Unix/linux

Desavantatges :

- Molts furats de seguretat
- Canvis en eines administratives
- Incompatible amb sistemes diferents a UNIX
- No treballa en mode desconectat

Name Service Switch (NSS)

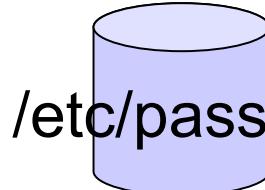
```
login: juana  
Password: ***
```

getpwnam()

/etc/nsswitch.conf

jdoe:s8f{2rs:1253:1253:Juana:/home/juana:/bin/bash

/etc/passwd

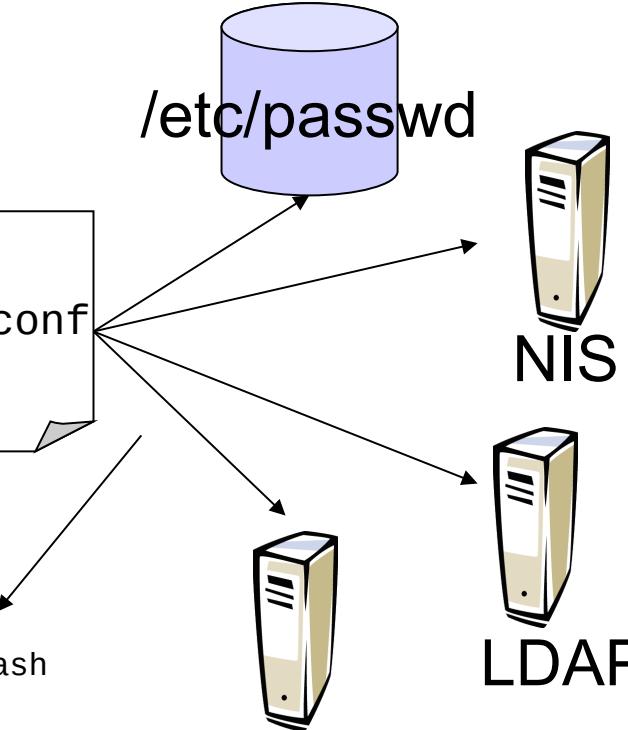


NIS



LDAP

SQL



NSS Pros/Contres

Avantatges:

- Permet que una entrada de /etc/passwd s'obtingui de qualsevol font
- 100% transparent a les aplicacions

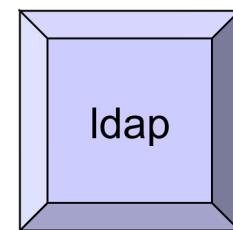
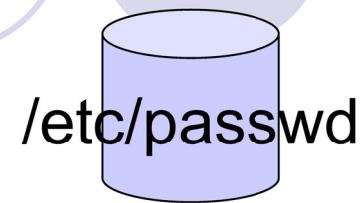
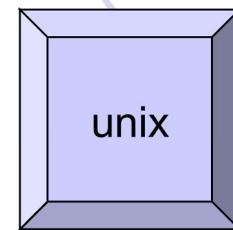
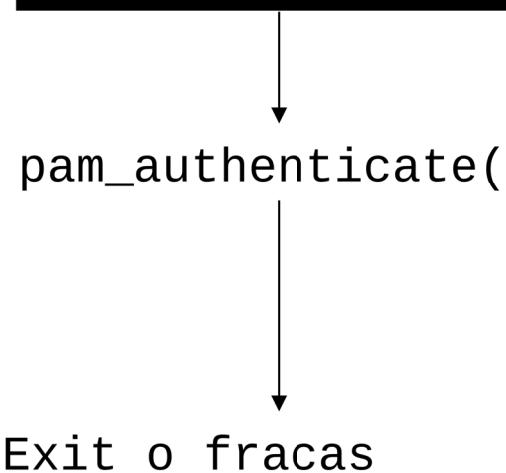
Desavantatges:

- No disponible en tots els Unix/Linux
- Quan es busca en múltiples fonts de dades la sincronització és un problema

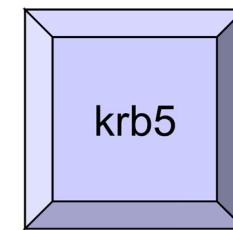
Pluggable Authentication Modules

PAM

```
login: juana  
Password: ***
```



LDAP



Kerberos

PAM Pros/Contres

Avantatges:

- Permet autenticar directament contra qualsevol font de dades
- Fàcilment configurable segons /etc/pam.d
- Aplicacions PAM no necessiten “mecanismes específics” de codi per a autenticar-se

Desavantatges:

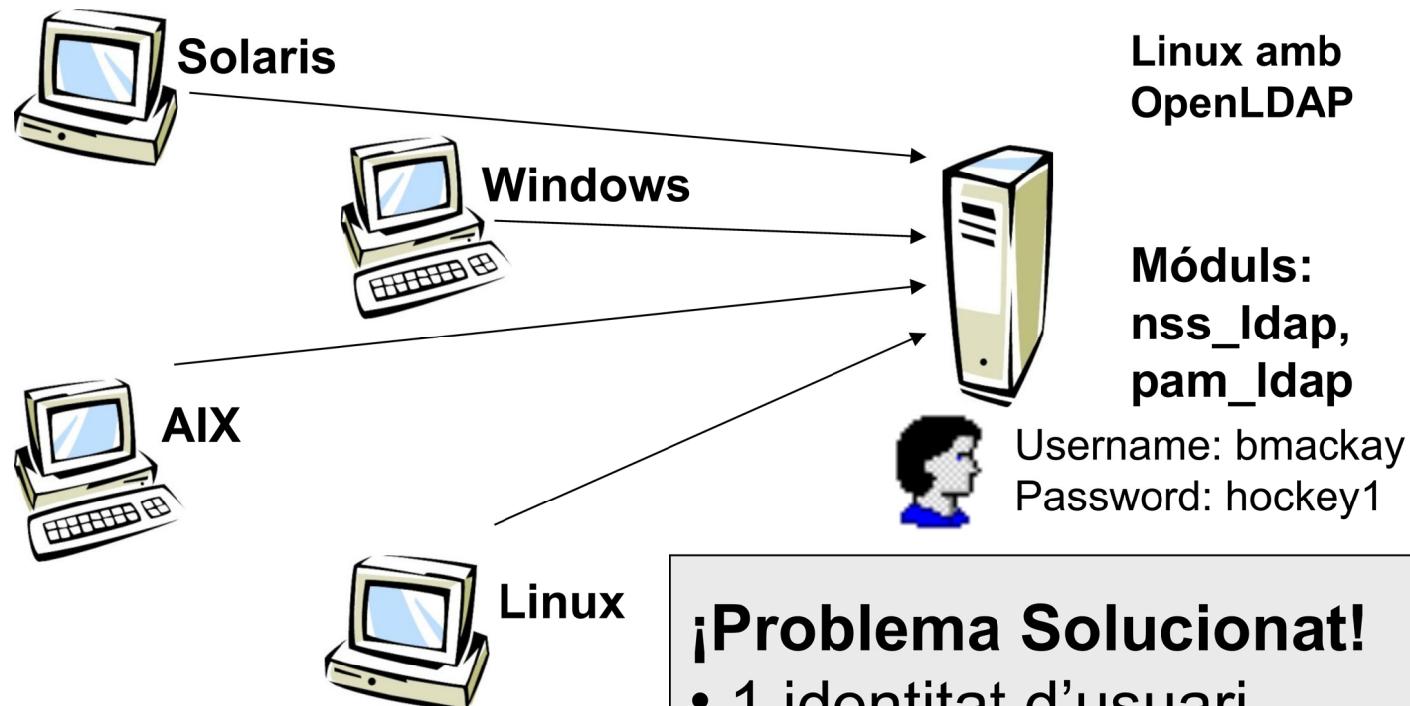
- Les utilitats i serveis per a autenticar-se han de ser “PAM enabled” (es a dir escrits en PAM API)



RFC2307

Proposta amb OpenLDAP i PAM_LDAP

Proposta amb OpenLDAP



¡Problema Solucionat!

- 1 identitat d'usuari
- 1 eina d'Admin.
- 1 emmagatzematge de claus

Ambients Ideals

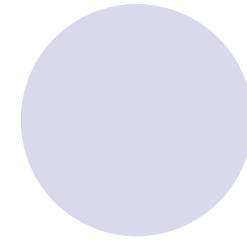
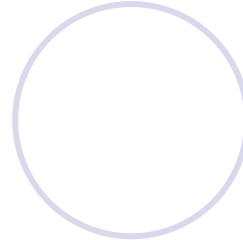
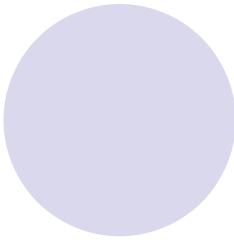
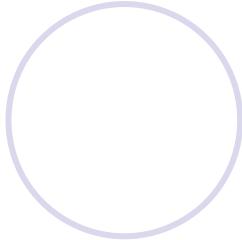
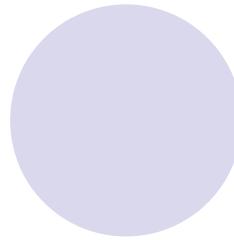
- Utilització d'un ambient mixt UNIX i Windows
- Cerca d'un ambient heterogeni segur
- Canvis o rotació de personal
- Maneig de 50+ usuaris UNIX/Linux

Missatges Claus

- Estableix una única identitat per a usuaris UNIX, Linux i Windows
- Proveeix alt nivell de seguretat en la xarxa (SSL i Kerberos)
- Centralitza l'administració d'identitats de usuaris UNIX, Linux i Windows
- Brinda suport per a múltiples plataformes
- S'integra en forma transparent en les estacions de treball dels usuaris

Casos d'exit

- Guardia di Finanza: 3,000 usuaris
- UK Ministry Of Defense: 1,600 usuaris que accedeixen a varies aplicacions, incloent una d'estadístiques de tripulació aérea
- Dynatronics - EEUU: Autenticant 40 usuaris que accedeixen aplicacions contables en Linux



● LDAP

Què és LDAP?

- Es un protocol lleuger d'accés a directoris que permet gestionar informació jeràrquica per a mantenir-la actualitzada i disponible en la xarxa
- LDAP = Lightweight Directory Access Protocol
- És una versió simplificada del pesat X.500 DAP protocol del modelo OSI de 1990

Què és LDAP?

- LDAP va néixer en Julio de 1993 amb el RFC 1487 (RFC 1777)
- La informació es guarda en una BD de tipus jeràrquica
- El promig de lectura en la BD es major a la d'escriptura

Perquè serveix LDAP?

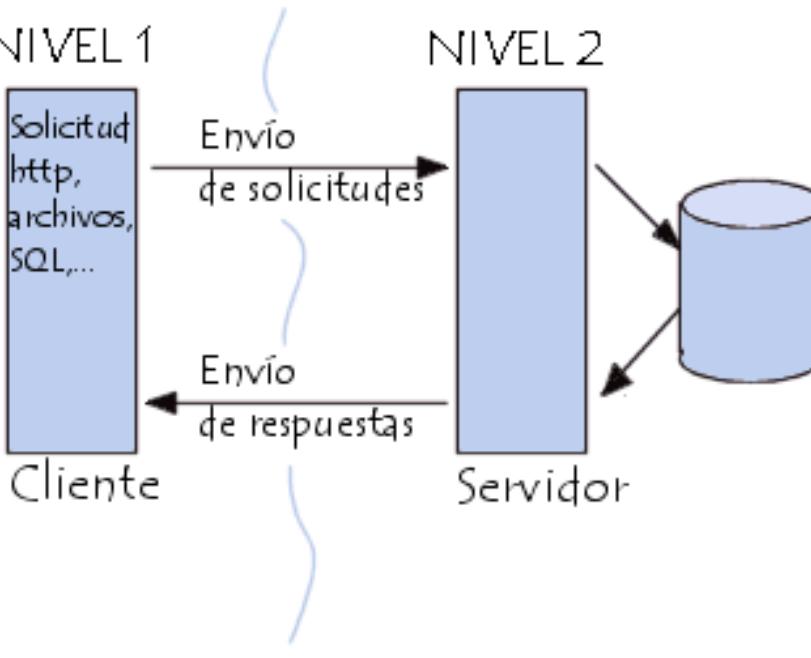
- Si ets un administrador: es pot administrar de forma centralitzada usuaris, grups, dispositius
- Pots aïllar les aplicacions dels directoris ex: correu electrònic
- Si ets un IT manager: Et permet renunciar a estar amarrat a un sol proveïdor i/o sistema operatiu
- Disminueix costos. Baixa el TCO (*Total Cost of Ownership*) al reduir el total de diferent directoris que es necessiten administrar

Perquè serveix LDAP?

- Si ets un desenvolupador: Et permet renunciar a estar amarrat a un sol proveïdor i/o sistema operatiu
- Estalvia temps de desenvolupament ja que no ha de desenvolupar un altre vegada el seu propi sistema de directoris per a usuaris, grups, objectes, etc

Arquitectura

- Es basa en l'arquitectura client servidor de dos nivells
- És un proc
- Hi ha dos tipus de serveis: tics i els dinàmics
- Offline dades que ajuden a la funcionalitat. Directori de televisió, servei de notícies, llibreries, biblioteques, etc



Arquitectura

- Online directoris:
- Canvien de forma dinàmica, han de ser flexibles, ha de ser segurs i han de personalitzar-se al gust de l'usuari
- Han de ser actualitzat per l'usuari propietari de la informació
- Ex: Directori d'empleats en una empresa per a localitzar-les quan canvien les seves dades de tel, fax, etc, directori d'hotels per als que passa un funcionari, etc

Productes Comercials

- Netscape's Directory Server
- Innosoft Distributed Directory Server
- Lucent Technologies Internet Directory Server
- Sun Microsystem's Directory services
- IBM's DSSeries LDAP Directory
- Microsoft Active Directory server
- Novell Suse Open Exchange - Mail
- SCOoffice Server - Mail
- Tarantella – Broker d'aplicacions

Competidores

- iPlanet de Netscape
- eDirectory de Novell
- Novell directory
- Active directory de Microsoft

Website: www.openldap.org

- Software en format rpm o font es pot obtenir de www.openldap.org:
- És heretat de la versió 3.3 de la Univ.Michigan
- A Julio de 2010 la versió actual és la OpenLDAP 2.4.23

Format de presentació

- LDIF: Format de representació de dades
- Codi ASCII que es pot passar com missatges d'e-mail (8 bit clean)
- Una entrada LDIF està formada per varies línies
- Inicia amb la paraula “DN”, seguit del nom únic que identifica la línia ó entrada en la BD

Format de presentació

- El registre DN ha d'ocupar una sola línia
- Després segueixen els atributs de l'entrada
- Cada atribut ha d'anar en una línia diferent
- Cada atribut ha d'estar seguit pel signe ":" i a continuació el seu valor

Exemple

- dn:**o=Acis,c=CO**
- o:Acis
- objectclass:organization
- dn: **cn=Juana, o=Acis, c=CO**
- cn: Juana
- sn: Zamora
- telephoneNumber: 781 784 7547
- objectclass:inetOrgPerson

Explicació

- Dn: significa distinguished (Distinguit)
- ObjectClass: (Tipus d'objecte)
- Cn: significa Common name (Nom Comú)
- Sn: significa surname (Cognom)
- Telephonenumber: (Número de tel)
- Uid: Compte de l'usuari
- userPassword: Clau de l'usuari
- Mail: (e-mail de l'usuari)

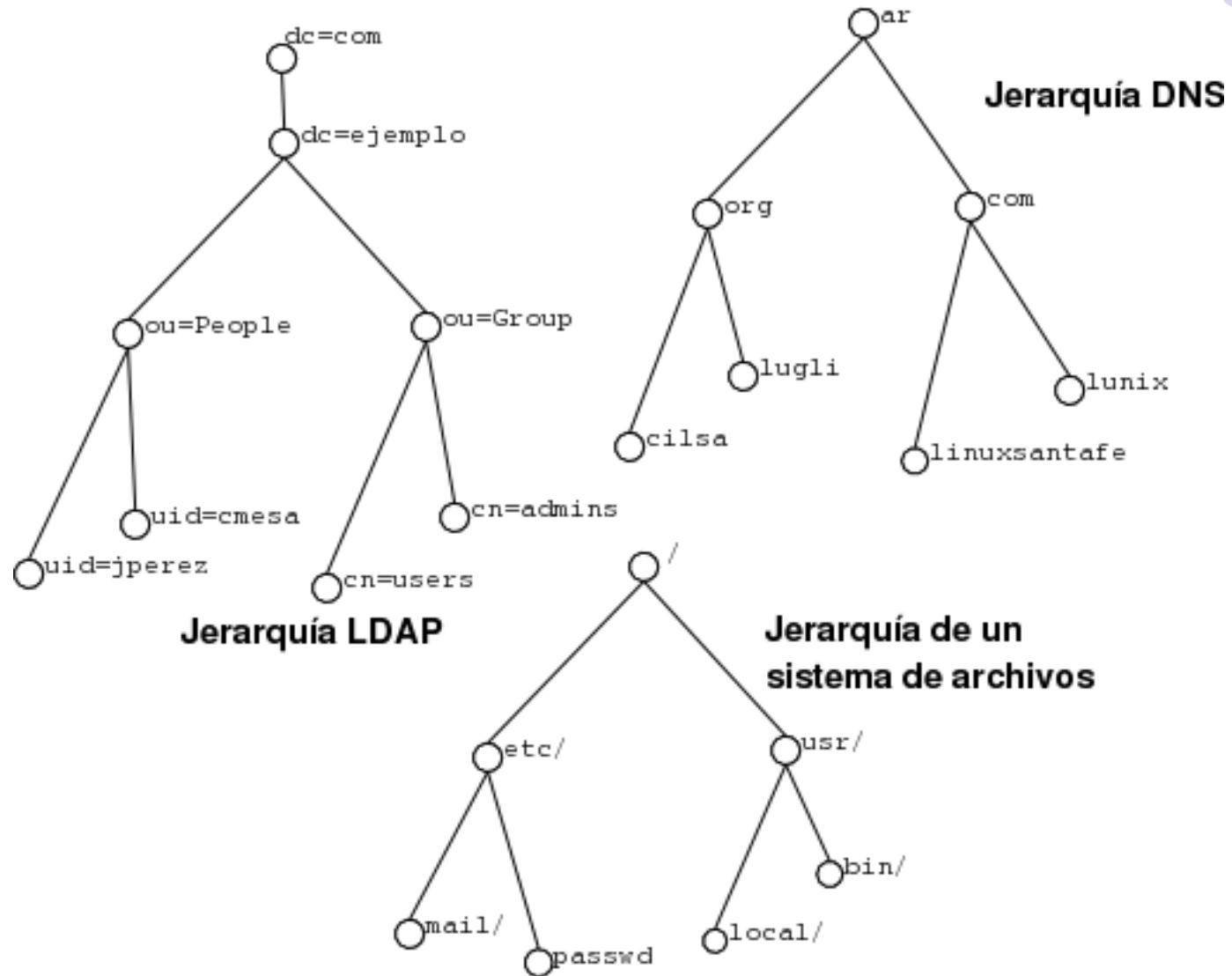
Explicació

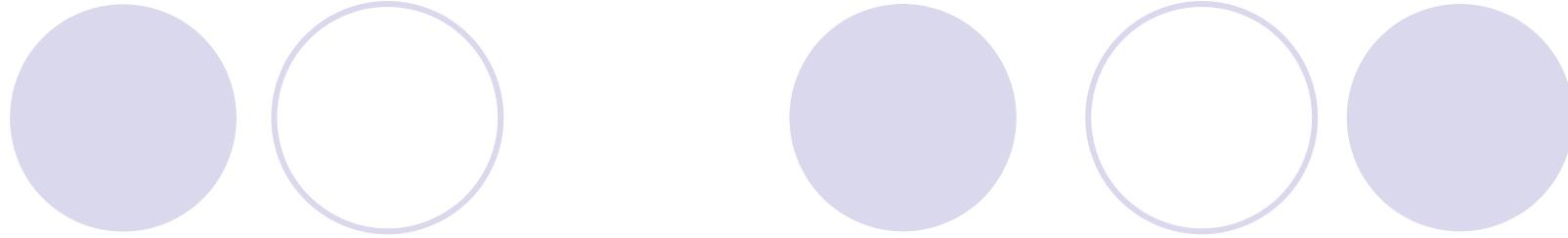
- Description: (Descripció de l'objecte)
- O: Significa organization (Nom de l'empresa)
- C: significa country (país)
- És a dir primer és té un tipus d'atribut i després el valor de l'atribut

Explicació

- El significat de cada atribut està definit en els arxius de tipus “schema” residents en el directori: /etc/openldap/schema/core.schema, /etc/openldap/schema/cosine.schema, /etc/openldap/schema/inetorgperson.schema

Exemple





- Arxius de configuració

Arxius de configuració: slapd

- El procés servidor en binari de ldap es diu: slapd
- Escolta pel port tcp 389
- slapd significa: Stand-alone LDAP Daemon

Configuració

- El shell d'arrencada /etc/init.d/ldap crida al servei slapd i aquest a la vegada busca l'arxiu de configuració /etc/openldap/slapd.conf
- Ambient per defecte /etc/openldap/ldap.conf
- Directori de dades: /var/lib/openldap

Arxius de configuració: slapd.conf

- # Indica els atributs i objectes que LDAP pot manejar per cada registre
- Include /etc/openldap/schema/core.schema
- Include /etc/openldap/schema/cosine.schema
- Include /etc / openldap / schema / inetorgperson.schema
- # Permet compatibilidad amb l'antiga versió 2
– Falla en RH 9.x
- allow bind_v2

Arxius de configuració: slapd.conf

- # Tipus de xifrat en els passwords dels usuaris
- password-hash {Format}
- # On format pot ser algun algoritme de xifrat simètric com: {SSHA}, {SHA}, {SMD5}, {MD5}, {CRYPT}, {CLEARTEXT}

Slapd.conf

- # Indica el format de la base de dades
- database ldbm
- # Esta és la base de la clau principal
- suffix o=Acis, c=CO
- # És el directori on resideix els arxius de la base de dades LDAP
- directory /var/lib/ldap

Slapd.conf

- # Aquest és la base del registre per a l'administrador
- rootdn cn=root, o=Acis, c=CO
- # Aquest és el password de l'administrador
- rootpw {SSHA}msyaU45hcXmiq8ahe9OkewOCKKA4A5EY

Slapd.conf

- La clau de l'usuari administrador es pot xifrar amb la comanda:

```
# slappasswd -h Format > arxiu
```

- On Format pot ser algun algoritme de xifrat simètric:
- {SSHA}, {SHA}, {SMD5}, {MD5}, {CRYPT}, {CLEARTEXT}

Slapd.conf

- Nota: Mai utilitzis {CLEARTEXT} donat que si un intrús veu l'arxiu pla pot coneixer la clau de l'administrador.
- Es recomana en canvia l'algoritm més fort {SSHA}

/etc/openldap/ldap.conf

- L'arxiu client /etc/openldap/ldap.conf ha d'estar configurat de la següent forma:
 - HOST 127.0.0.1
 - BASE o=Acis, c=CO
 - PORT 389

Arxiu de dades: ldif

- dn: o=Acis,c=CO
- o: Acis
- postalAddress: Calle 93 con 13A
- objectclass: organization
- dn: cn=Juana, o=Acis, c=CO
- cn: Juana
- sn: Zamora
- description: Soport en Windows
- uid: acarvaja
- userPassword:{SSHA}msyaU45hcXmiq8ahe9OkewOCKKA4A5EY
- displayname: Armando Carvajal - sistemes
- mail: acarvaja@acis.org.co
- carLicense: 77036182
- homePhone: 571 528 3101
- objectclass:inetOrgPerson

Comandes:

- Consultar si “openldap” esta instal·lat:
rpm –q openldap
- Hacer backup de la base de dades en format LDIF:
slapcat –l backup.ldif
- Pujar les dades fets per un backup en format LDIF:
slapadd –l backup.ldif

Comandes:

- Per a generar un password xifrat de tipus hash:
slappasswd –h metode de xifrat
- Per a xifrar el password del client al servidor:
stunnel –c –d 389 –r localhost:636

Altres comandes:

- Per a veure tots els registres de la BD:
#ldapsearch -x -b 'o=Acis,c=CO' 'objectclass=*'
- Per a veure els usuaris de la BD:
#ldapsearch -x -b 'o=Acis,c=CO' 'uid='*
- Per a addicionar registres des de l'arxiu bd.ldif:
#ldapadd -x -D 'uid=acarvaja,o=Acis,c=CO' -W -f
bd.ldif



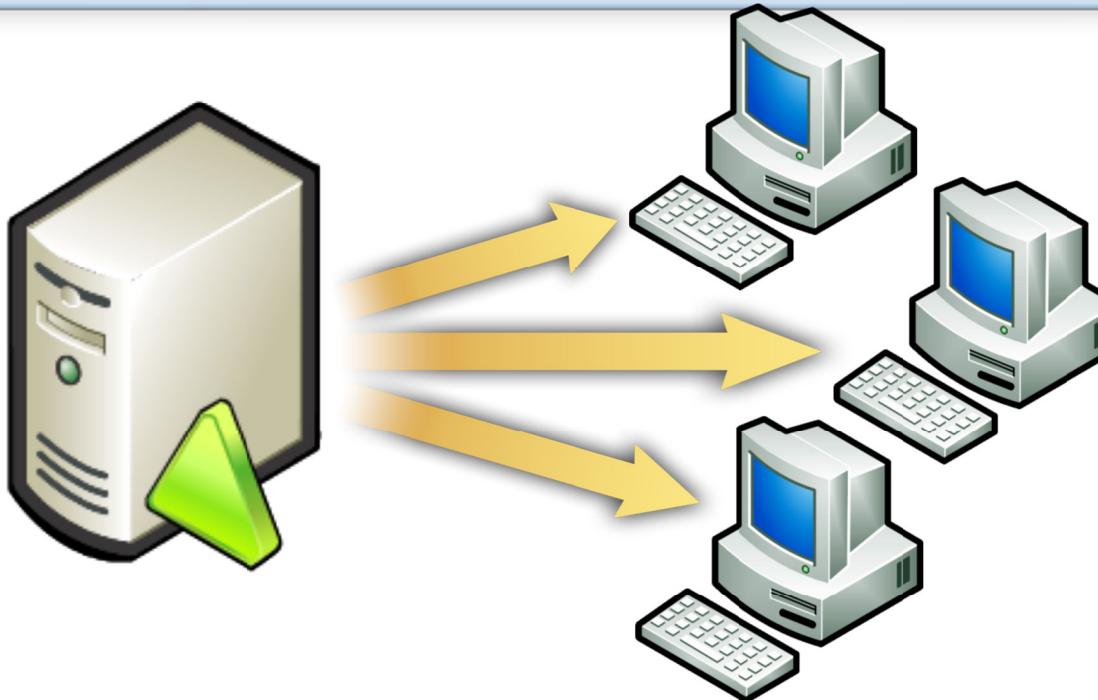
Webgrafia i/o material

- wwwldapguru.com
- www.openldap.org
- Bibliografia
 - Understanding And Deploying LDAP Directory Services, Timothy A. Howes Ph.D, New Riders, 1999, Netscape Communications Corporation, First Edition
 - Implementing LDAP, Marck Wilcox, Editorial Wrox

Implementació de directives de grup (GPO)



Què és la Group Policy Object?

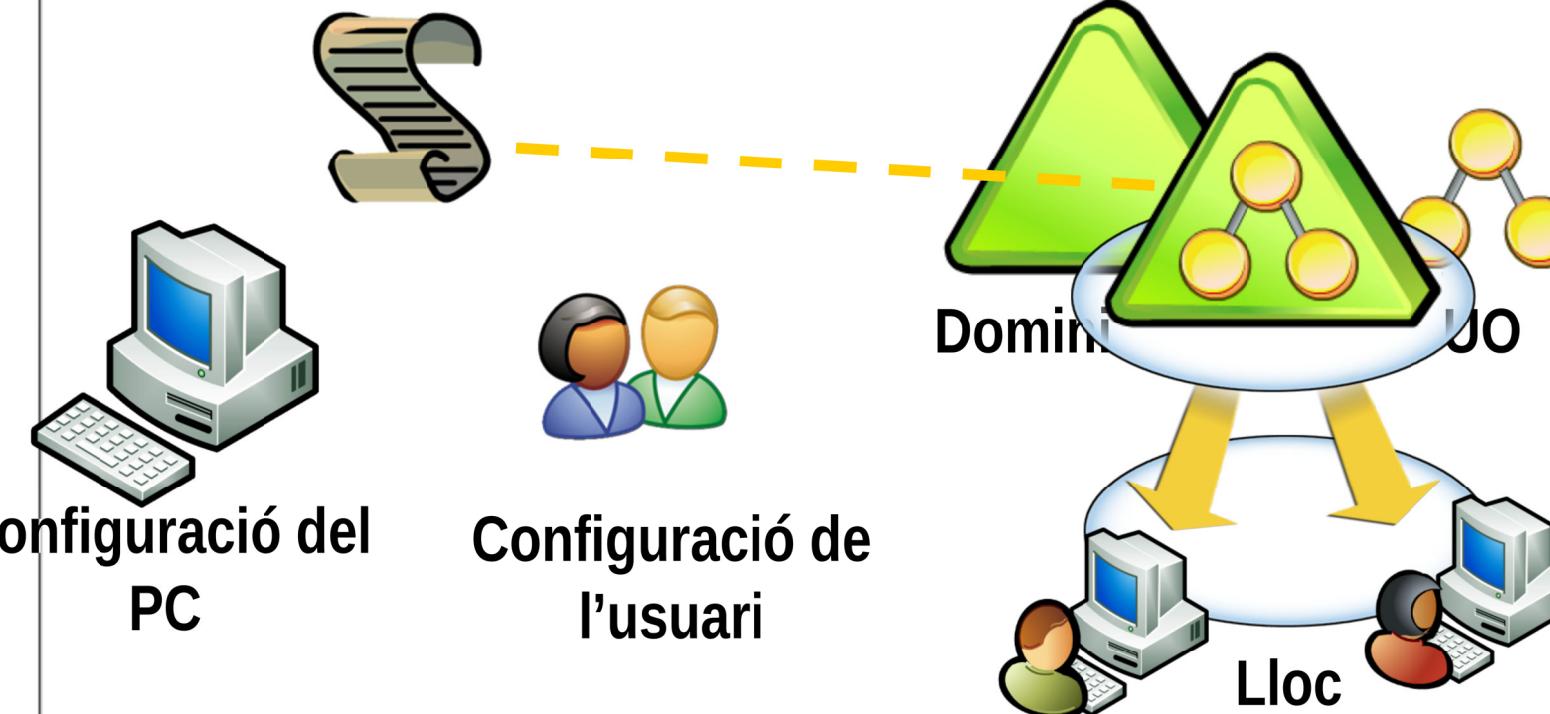


- Administrar els ambients de usuari i PC
- Aplicar polítiques d'equips
- Simplificar les tasques administratives
- Implementar configuracions de seguretat

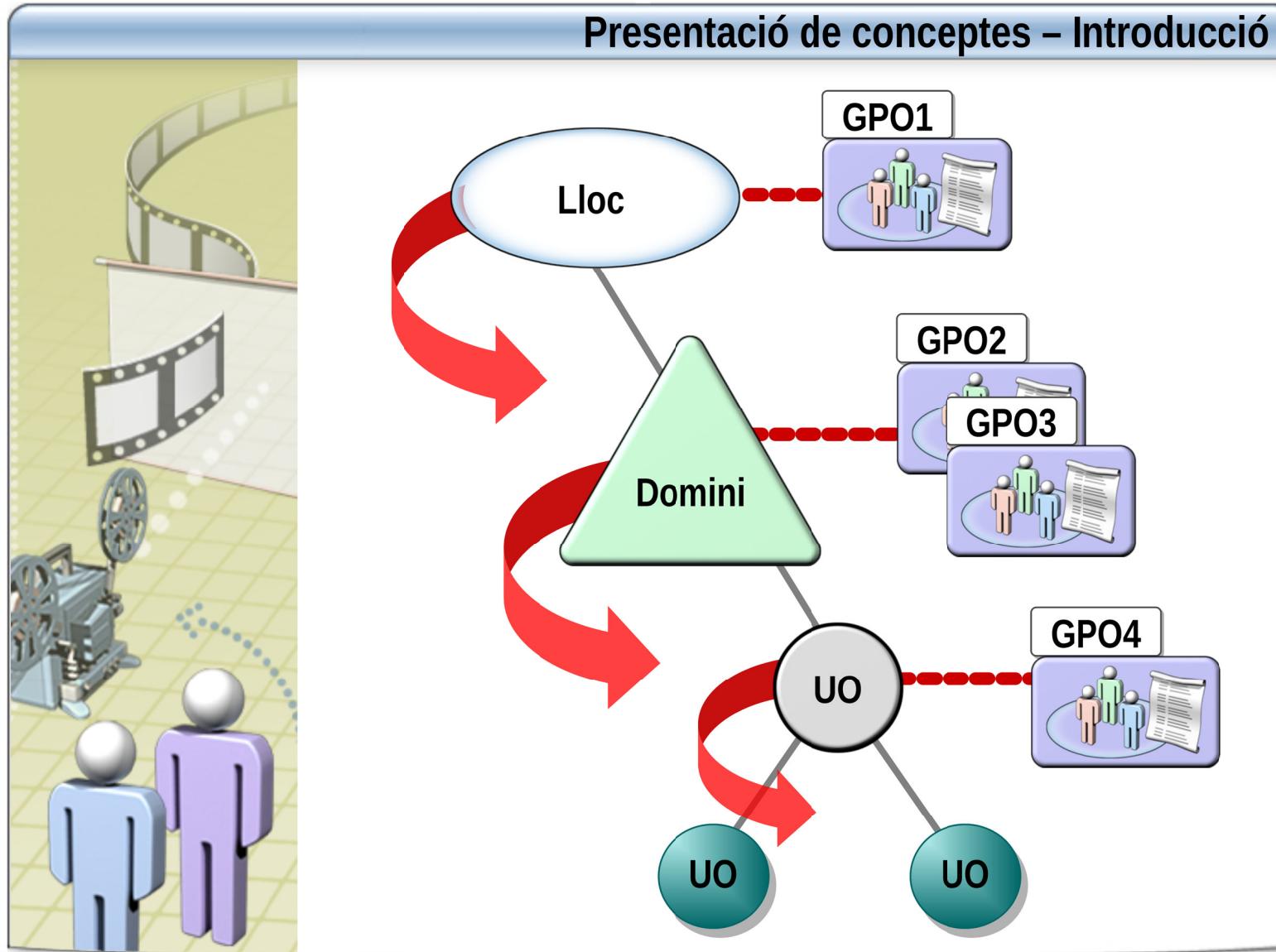
Termes de la Política de Grup

Objecte de la Política
de grup

Abast de la
administració



Creació i configuració de GPO



Quan s'aplica la Política de Grup?



Engegada i apagada



Conexió i desconexió

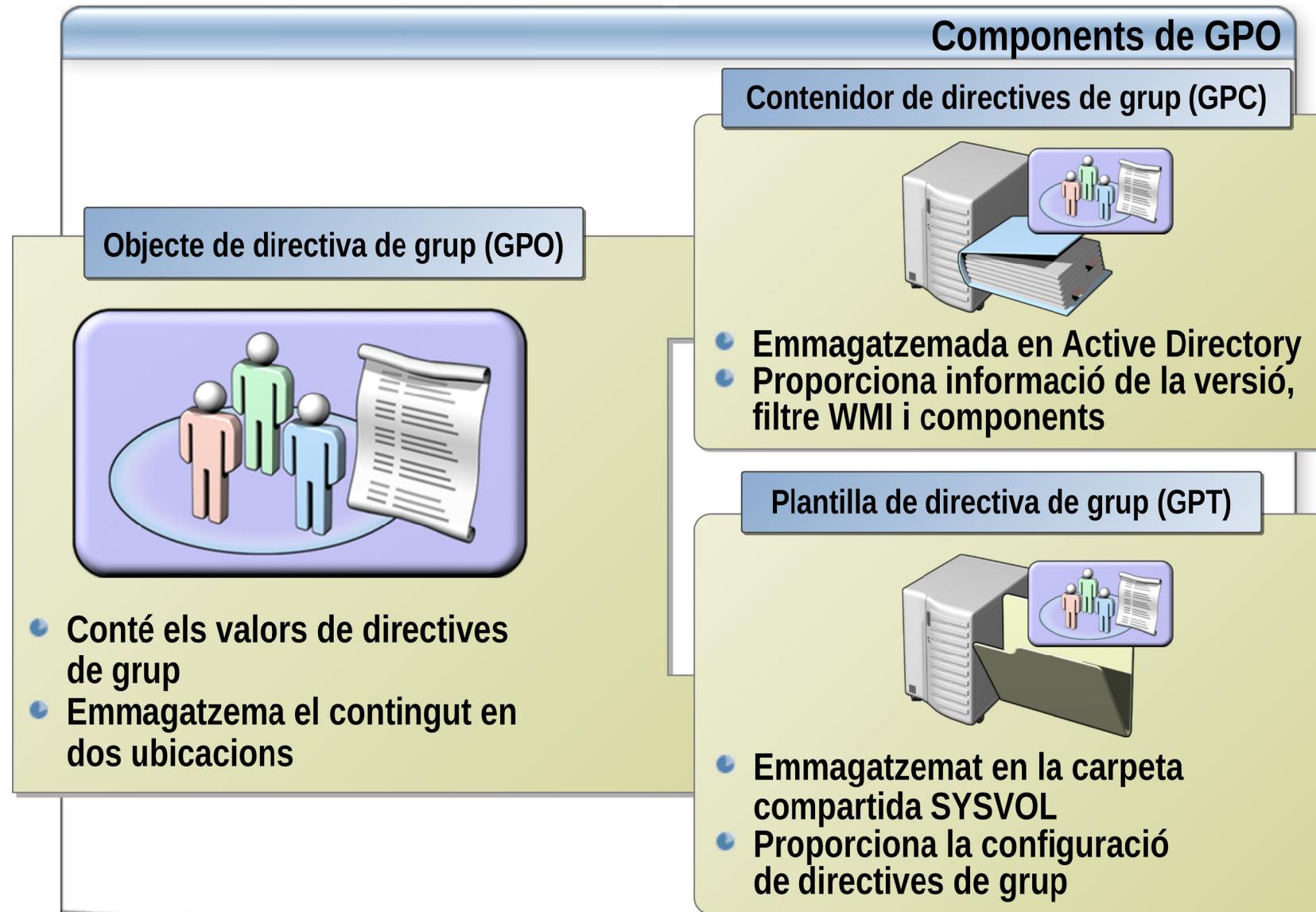


Intervals definits



Forçat ambn GPUpdate.exe

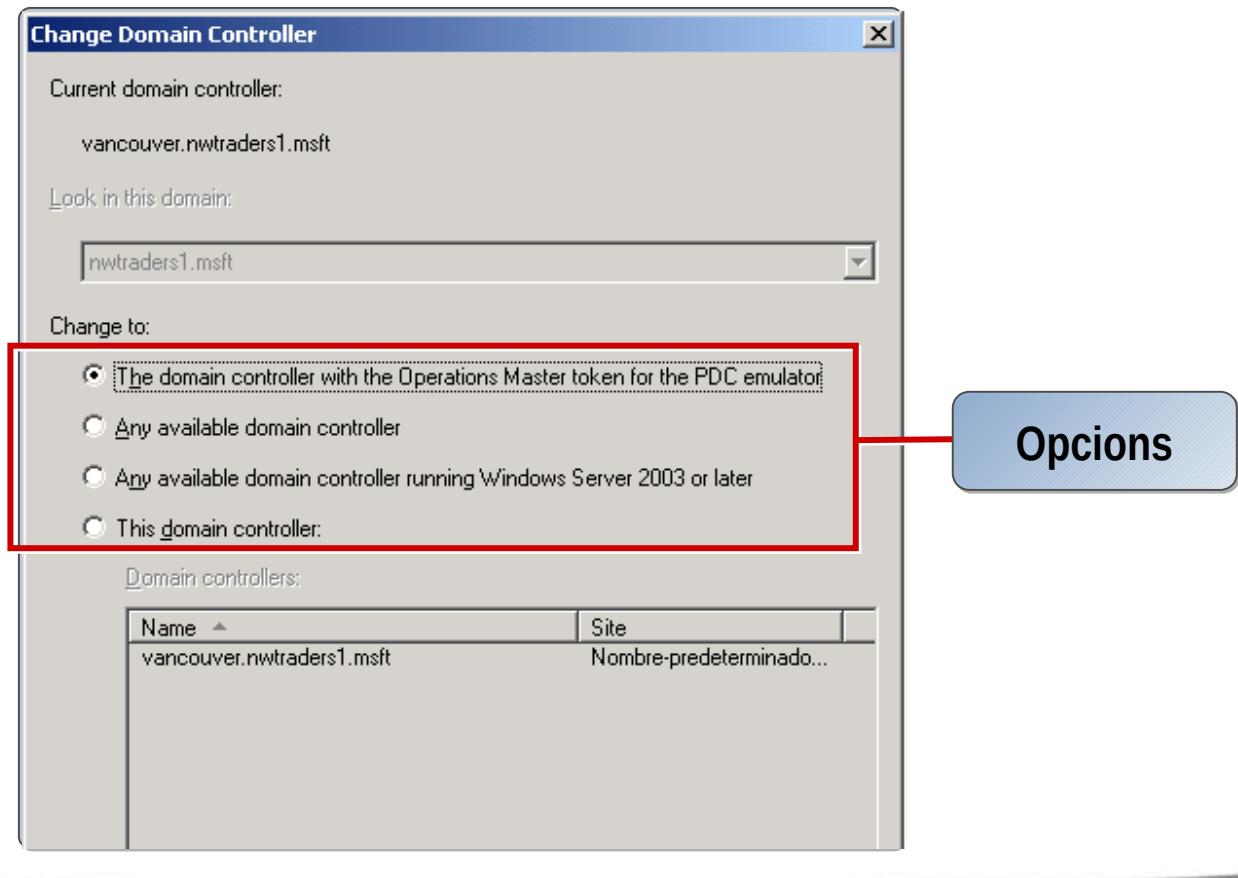
Creació i configuració de GPO



Creació i configuració de GPO

Per què especificar un controlador de domini per l'administració de GPO?

Administració de directives de grup utilitza l'emulador del controlador de domini principal (PDC, *primary domain controller*) en cada domini com el controlador de domini predeterminat per evitar conflictes de replicació.



Creació i configuració de GPO

Cómo especificar un controlador de domini per l'administració de GPO?

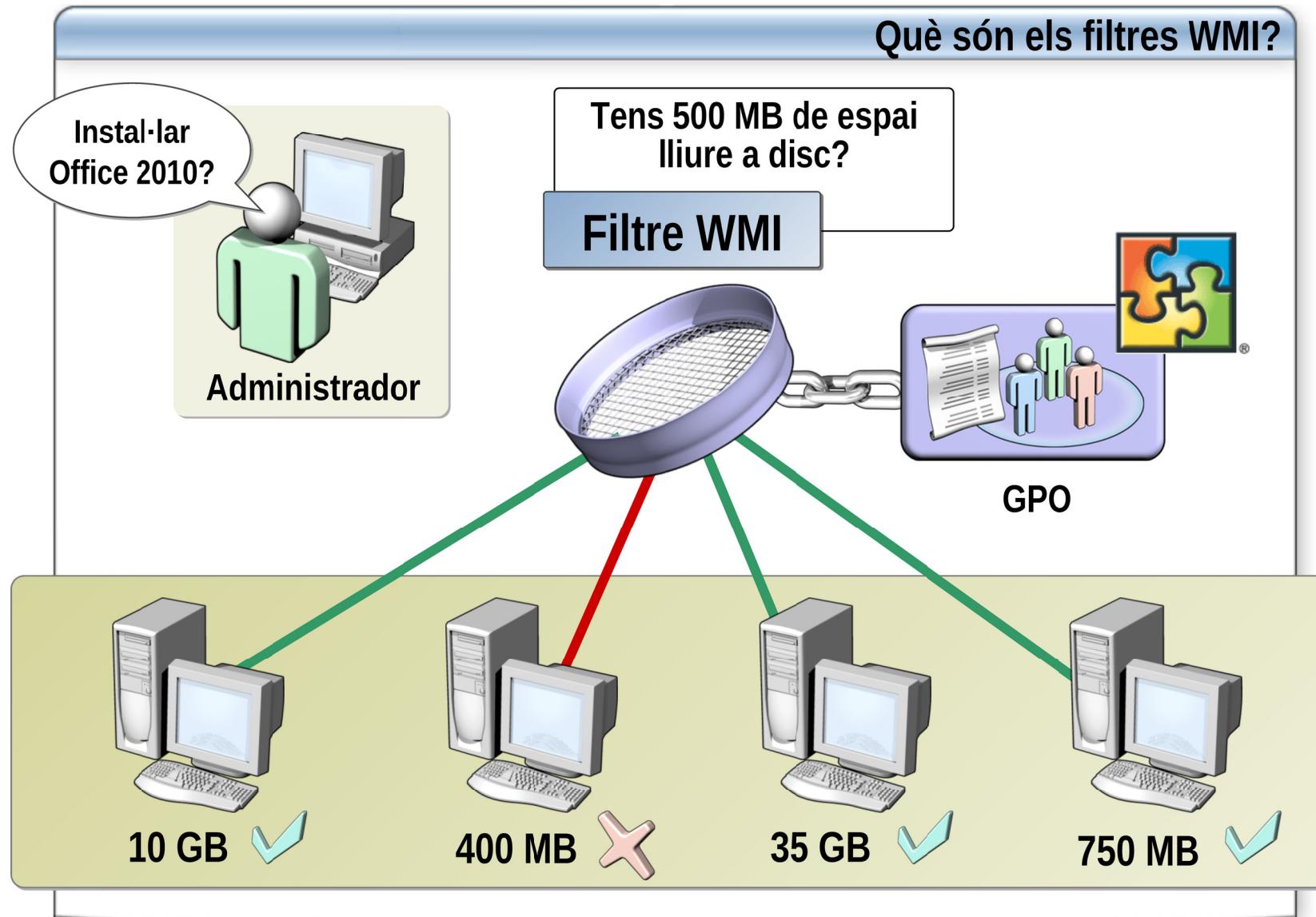
Per especificar un controlador de domini, cal seguir els següents passos:

1.Obrir Administració de directives de grup, expandir el bosc, expandir Dominis i utilitzar un dels següents mètodes:

- Per especificar un controlador de domini per utilitzar-lo en operacions de domini, fes clic amb el botó dret en el domini necessari i, a continuació, fes clic en Canviar el controlador de domini.
- Per especificar un controlador de domini per utilitzar-lo en operacions en llocs, fes clic amb el botó dret en Llocs i, a continuació, fes clic en Canviar el controlador de domini.

2.Al quadre de diàleg Canviar el controlador de domini, en Canviar a, fes clic en Aquest controlador de domini i, a continuació, fes clic en Acceptar.

Creació i configuració de GPO



WMI Filtering

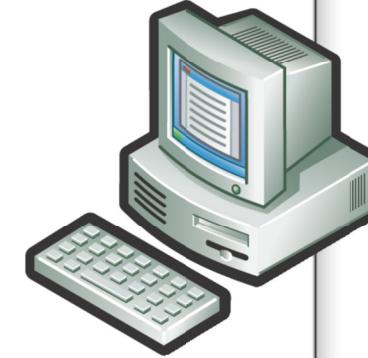


Domain
Controller

XP Professional only



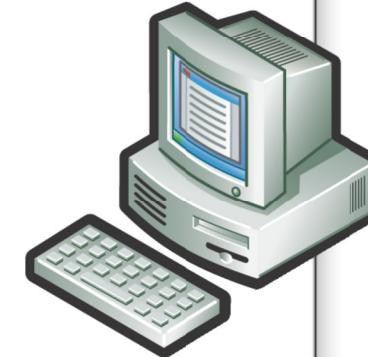
WMI Filter



Windows XP



Windows 2000



Windows XP

Creació i configuració de GPO

Cómo crear un filtro WMI y vincularlo a una GPO?

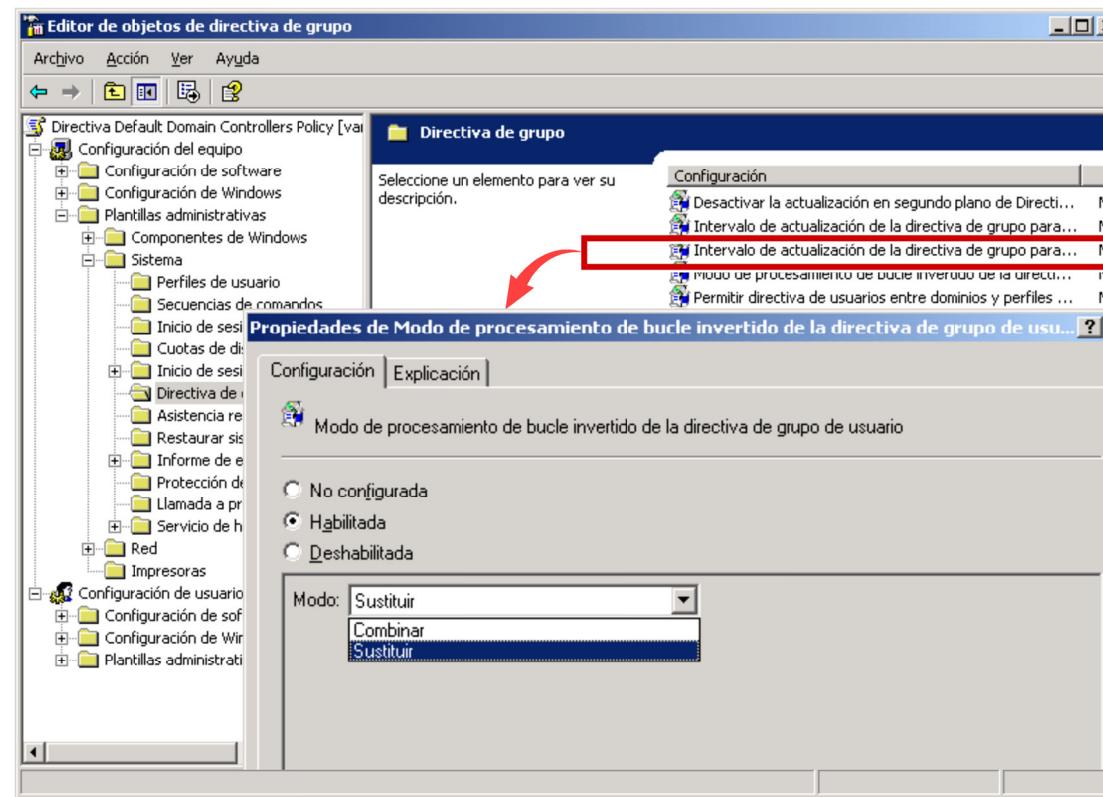
Para crear un filtro WMI y vincularlo a una GPO, realice los siguientes pasos:

1. Abre Administración de directivas de grupo, expande el bosque que contiene la GPO al que deseas agregar un filtro WMI, expande Dominios, expande el dominio que contiene la GPO, expande Filtros WMI, haz clic con el botón derecho en Filtros WMI, y a continuación, haz clic en Nuevo.
2. En la ventana de diálogo Nuevo Filtro WMI, en el cuadro Nombre, escribe un nombre para la consulta.
3. En la ventana de diálogo Descripción, escribe una descripción de la consulta.
4. Haz clic en Agregar.
5. En la ventana de diálogo Consulta WMI, en el cuadro Espacio de nombres, escribe la ruta del espacio de nombres de la consulta o haz clic en Examinar para ver una lista de los espacios de nombres disponibles. Para cada consulta necesitarás especificar el espacio de nombres WMI al que se ejecutará la consulta. El espacio de nombres por defecto debería ser adecuado para la mayoría de las situaciones.
6. En la ventana de diálogo Consulta, escribe una consulta WQL válida y haz clic en Aceptar.
7. En la ventana de diálogo Nuevo Filtro WMI, haz clic en Guardar.
8. Expande Objetos de directiva de grupo y arrastra el filtro WMI hasta la GPO deseada.

Creació i configuració de GPO

Què és el processament en bucle invertit?

Per defecte, les GPO d'un usuari determinen la configuració d'usuari que s'ha d'aplicar quan un usuari inicia sessió en un equip. Però, el processament de bucle invertit aplica la configuració de GPO per l'equip a qualsevol usuari que inicia sessió en aquell equip. S'utilitza en equips d'ús especial, com equips en llocs públics, laboratoris i aules, on s'ha de modificar la configuració d'usuari basant-se en l'equipo utilitzat.



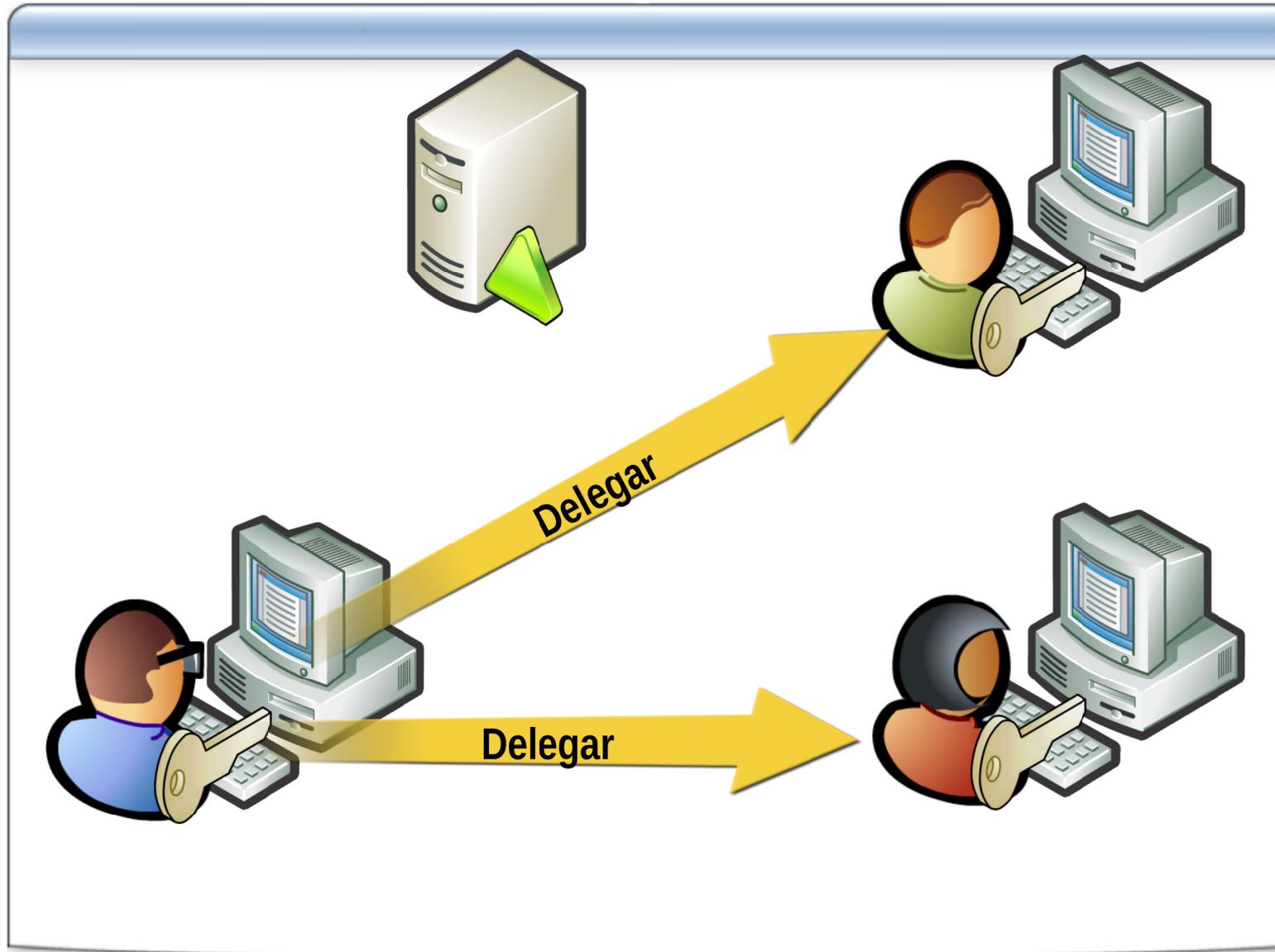
Creació i configuració de GPO

Cómo configurar el modo de processamiento de bucle invertido de la GPO de l'usuari?

Per configurar el Mode de processament de bucle invertit de la GPO d'usuari, realitza els següents passos:

- 1.Obre Administració de directives de grup, expandeix el bosc, expandeix Dominis, expandeix el seu domini i, per últim, fes clic en Objectes de directiva de grup.
- 2.Al panel de detalls, fes clic amb el botó dret en objecte de directiva de grup i, a continuació, fes clic en Editar.
- 3.Al Editor d'objets de directiva de grup, expandeix Configuració de l'equip, expandeix Plantilles administratives, expandeix Sistema i, a continuació, fes clic en Directiva de grup.
- 4.Fes doble clic en Mode de processament de bucle invertit de la directiva de grup d'usuari, si encara no està seleccionat, fes clic en Habilitada.
- 5.A Mode, fes clic en Sustituir o Combinar i, a continuació, fes clic en Acceptar.

Delegar el control de los GPOs



Delegació del control administratiu de GPO

Delegació de GPO

Mètodes d'assignació de permís per crear GPO	Sols permet als usuaris crear GPO en el domini	Permet als usuaris editar o eliminar GPO o vincular GPO
Agregar el grup o usuari al grup Propietaris del creador de directives de grup		
Assignar al grup o usuari permís explícit per crear GPO		

Delegació del control administratiu de GPO

Delegació de directives de grup per un lloc, domini o unitat organitzativa



Permisos:

Vincular GPO

Permisos de lectura i
escriptura pels atributs
gPLinks i gPOptions

Modelar directives de grup

Permís Generar
conjunt resultant de
directives (planeació)

Resultados de directiva de grup

Permís Generar
conjunt resultant
de directives (registre)

Delegació del control administratiu de GPO

Cómo delegar control administrativo para administrar vínculos de directiva de grupo?

Para delegar control administrativo para administrar vínculos de directiva de grupo, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo.
2. Ve a la raíz del bosque y el dominio en el que deseas delegar control administrativo para administrar vínculos de directiva de grupo y, a continuación, haz clic en el vínculo.
3. En el panel de detalles, en la pestaña Delegación, haz clic en Agregar.
4. En el cuadro de diálogo Seleccionar Usuarios, Equipos o Grupos, en el cuadro de texto introduce el nombre del objeto que deseas seleccionar, introduce el principal de seguridad, haz clic en Comprobar nombres y, a continuación, haz clic en Aceptar.
5. En el cuadro de diálogo Agregar usuario o grupo, en el cuadro Permisos, selecciona el permiso adecuado y haz clic en Aceptar.

Delegació del control administratiu de GPO

Cóm delegar control administratiu per crear i editar GPO?

Per delegar control administratiu per crear GPO, realitza els següents passos:

- 1.Obre Administració de directives de grup.
- 2.Ves fins el bosc i el domini en el que vols delegar control administratiu per crear GPO i, a continuació, fes clic en Objectes de directiva de grup.
- 3.Al panel de detalls, a la fitxa Delegació, fes clic en Agregar.
- 4.Al quadre de diàleg Seleccionar Usuaris, Equips o Grups, al quadre Escriu el nom d'objecte que vols seleccionar, introduceix el principal de seguretat, fes clic en Comprovar noms i, a continuació, fes clic en Acceptar.

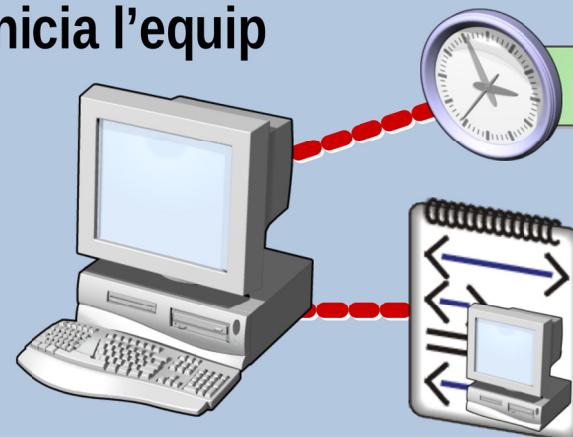
Per delegar control administratiu per editar GPO, realitza els passos anteriors i:

- 5.Al quadre de diàleg Agregar usuari o grup, al quadre Permisos, selecciona el permís adequat i fes clic en Acceptar.

Configuració de la freqüència d'actualització i valors de GPO

Quan s'aplica la GPO?

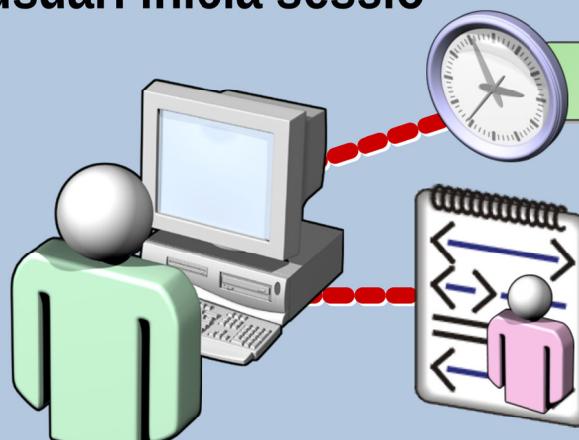
S'inicia l'equip



Interval d'actualització

- Configuració de l'equip aplicada
- S'executen les seqüències de comandes d'inici

L'usuari inicia sessió



Interval d'actualització

- Configuració d'usuari aplicada
- S'executen les seqüències de comandes d'inici de sessió

Configuració de la freqüència d'actualització i valors de GPO

Cómo assignar configuración de secuencia de comandos de GPO?

Para copiar una secuencia de comandos a la GPO adecuada:

1. Localiza la secuencia de comandos en el disco duro con el Explorador de Windows.
2. Edita la GPO adecuada en Administración de directivas de grupo, expande Configuración del equipo (para secuencias de comandos de inicio y apagado) o Configuración del usuario (para secuencias de comandos de inicio o cierre de sesión), expande Configuración de Windows y, finalmente, haz clic en Secuencias de comandos.
3. Haz doble clic en el tipo de secuencia de comandos adecuado (Inicio, Apagar, Iniciar sesión, Cerrar sesión), y haz clic en Mostrar archivos.
4. Copia el archivo de secuencia de comandos desde el Explorador de Windows a la ventana que aparece y, finalmente, cierra la ventana.

Para agregar una secuencia de comandos a una GPO:

1. En el cuadro de diálogo Propiedades para el tipo de secuencia de comandos, haz clic en Agregar.
2. Haz clic en Examinar, selecciona una secuencia de comandos y, finalmente, haz clic en Abrir.
3. Agrega los parámetros de secuencia de comandos necesarios y, finalmente, haz clic en Aceptar.

Configuració de la freqüència d'actualització i valors de GPO

Cómo configurar la freqüència d'actualització dels components de GPO?

Per configurar els components de directiva de grup que s'actualitzen i es poden modificar, realitza els següents passos:

- 1.Obre la GPO adequada en la directiva de grup, expandeix Configuració de l'equip, expandeix Plantilles administratives, expandeix Sistema, fes clic en Directiva de grup i, a continuació, fes doble clic a cada element de la taula anterior.
- 2.Fes clic en Habilitada.
- 3.Fes clic en No aplicar durant el processament periòdic en segon pla.
- 4.Si està disponible, fes clic en Permetre el processament a través d'una connexió de xarxa de baixa velocitat i fes clic en Acceptar.

Configuració de la freqüència d'actualització i valors de GPO

Cómo configurar la freqüència d'actualització de controladors de domini i equips?

Per configurar la freqüència d'actualització, realitza els següents passos:

1.Obre la GPO adequada en la directiva de grup, expandeix Configuració d'usuari o Configuració de l'equip (depenent de la GPO que vols editar), expandeix Plantilles administratives, expandeix Sistema, fes clic en Directiva de grup i, a continuació, fes doble clic en una de les següents configuracions:

- Interval d'actualització de la directiva de grup per usuaris
- Interval d'actualització de la directiva de grup per equips
- Interval d'actualització de la directiva de grup per controladors de domini

2.Fes clic en Habilitada.

3.Estableix d'interval d'actualització en minuts.

4.Estableix la compensació de temps aleatòria i fes clic en Acceptar.

Configuració de la freqüència d'actualització i valors de GPO

Cómo actualizar la configuración de GPO a un equipo de usuario utilizando Gpupdate.exe?

Per actualitzar la configuració de directiva de grup al equip d'un usuari amb la comanda gpupdate, realitza els següents passos:

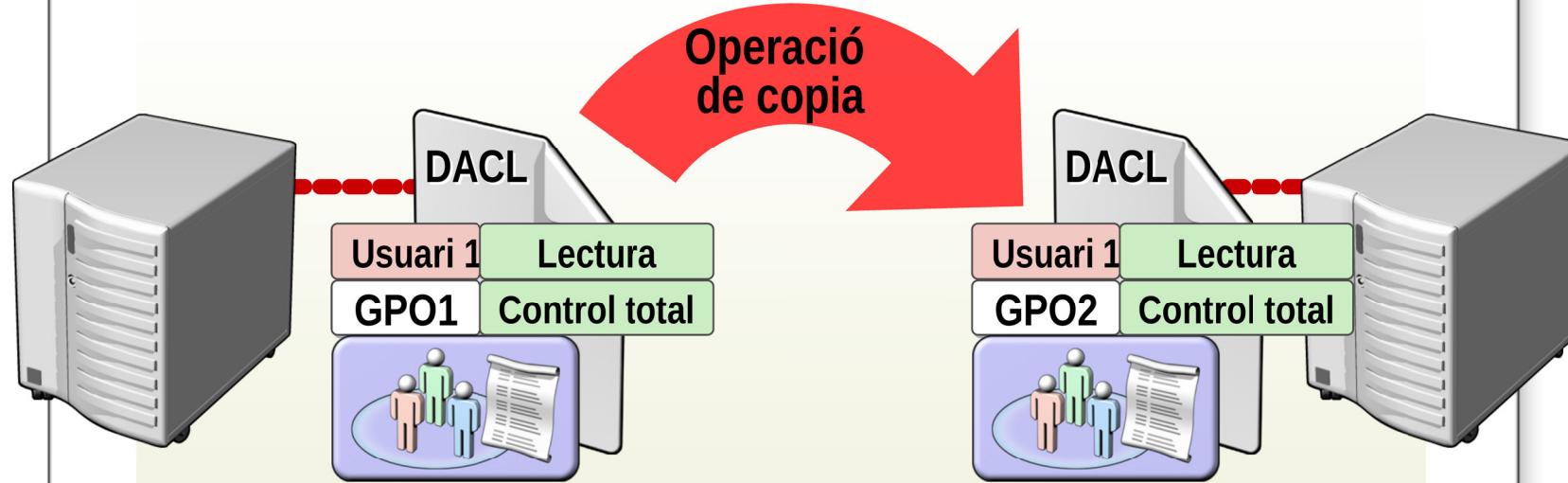
1. Al quadre de diàleg Executar, escriu cmd i fes clic en ENTRAR.
2. La comanda tipus serà:

gpupdate [/target:{equipo|usuario}] [/force] [/wait:valor] [/logoff] [/boot]

Consulta el man de gpupdate per conèixer el significat de cadascun dels paràmetres de la comanda anterior.

Administració de GPO

Què és una operació de copia?



- Una copia d'una GPO transfereix tant sols la configuració dins d'una GPO (té un nou GUID i llista d'accés)
- El nou GPO es crea desvinculat

Administració de GPO

Cómo copiar un GPO? (I)

Para crear una GPO, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo, expande los Objetos de directiva de grupo en el bosque y dominio que contiene la GPO que deseas copiar, haz clic con el botón derecho en la GPO y, a continuación, haz clic en Copiar.
2. Realiza uno de los siguientes pasos:
 - Para colocar la copia de la GPO en el mismo dominio que la GPO original, haz clic con el botón derecho en Objetos de directiva de grupo y haz clic en Pegar.
 - i. En la página Copiar GPO, selecciona Utilizar los permisos predeterminados para las nuevas GPO o Conservar los permisos existentes y haz clic en Aceptar.
 - ii. Una vez completada la copia, haz clic en Aceptar.
 - Para colocar la copia de la GPO en un dominio diferente, sigue al mismo bosque o a otro bosque, expande el dominio de destino, haz clic con el botón derecho en Objetos de directiva de grupo y, a continuación, haz clic en Pegar.
 - i. En la página Asistente para la copia entre dominios, haz clic en Siguiente.

Administració de GPO

Cómo copiar un GPO? (II)

- ii. A la página Especificar permisos escoge Utilizar los permisos predeterminados para las nuevas GPO o Conservar o migrar los permisos de las GPO originales y haz clic en Siguiente.
- iii. A la página Buscar la GPO original haz clic en Siguiente. Si la GPO de origen contiene referencias a principales de seguridad y rutas UNC, verás la ventana del punto iv, de lo contrario continuarás al punto v.
- iv. A la página Referencias de migración, selecciona Copiar-los de forma idéntica desde el origen o Utilizar esta tabla de migración para asignar-los a nuevos valores a las nuevas GPO, selecciona la tabla de migración de la lista y haz clic en Siguiente.
- v. A la página Finalización del asistente para la copia entre dominios, haz clic en Finalizar.
- vi. Una vez completada la operación de copia, haz clic en Aceptar.

Administració de GPO

Què és una operació de copia de seguretat?)



En una operació de copia de seguretat, Administració de directives de grup, exporta totes les dades d'una GPO a l'arxiu seleccionat i desa els arxius de GPT

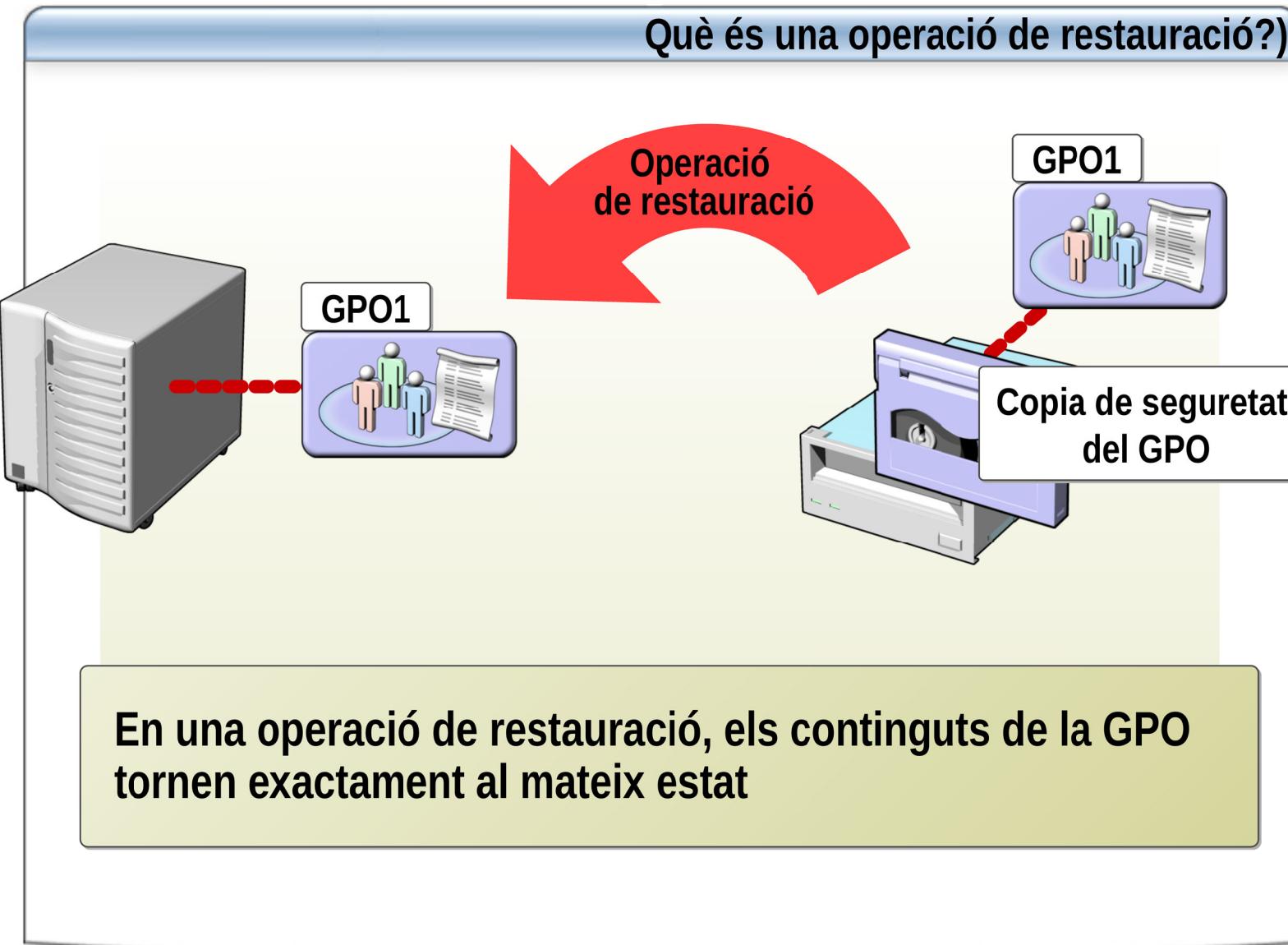
Administració de GPO

Cómo realizar una copia de seguridad de una GPO?

Para realizar la copia de seguridad de una GPO, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo, expande el bosque que contiene la GPO de la que deseas realizar la copia de seguridad, expande Dominios, expande el dominio que contiene la GPO, expande Objetos de directiva de grupo y, a continuación, realiza los siguientes pasos:
 - Para realizar la copia de seguridad de una sola GPO, haz clic con el botón derecho en la GPO y haz clic en Copia de seguridad.
 - Para realizar una copia de seguridad de todas las GPO, haz clic con el botón derecho en Objetos de directiva de grupo y, a continuación, haz clic en Copia de seguridad de todo.
2. En el cuadro de diálogo Copia de seguridad de objetos de directiva de grupo, introduce la ruta a la ubicación donde deseas almacenar la copia de seguridad de la GPO.
3. Escribe una descripción para la GPO de la que deseas realizar la copia de seguridad y haz clic en Copia de seguridad.
4. Una vez completada la operación de copia de seguridad, haz clic en Aceptar.

Administració de GPO



Administració de GPO

Cóm restaurar una GPO? (I)

Per restaurar una versió anterior d'una GPO existent, realitza els següents passos:

- 1.Obre Administració de directives de grup, expandeix el bosc que conté la GPO que vols restaurar, expandeix Dominis, expandeix el domini que conté la GPO, fes clic amb el botó dret en Objectes de directiva de grup i, a continuació, fes clic en Administrar copies de seguretat.
- 2.Al quadre de diàleg Administrar copies de seguretat, selecciona la copia de seguretat de la GPO que vols restaurar i fes clic en Restauració.
- 3.Quan es demani si vols restaurar la copia de seguretat seleccionada, fes clic en Acceptar.
- 4.Al quadre de diàleg Progrés de la restauració, fes clic en Acceptar una cop finalitzada la restauració.
- 5.Al quadre de diàleg Administrar copies de seguretat selecciona una altra GPO que vulguis restaurar o fes clic en Tancar per finalitzar la operació de restauració.

Administració de GPO

Cómo restaurar una GPO? (II)

Per restaurar una GPO eliminada que apareix a la llista de Objectes de directiva de grup, realitza els següents passos:

- 1.Obre Administració de directives de grup, expandeix el bosc que conté la GPO que vols restaurar, expandeix Dominis i, a continuació, expandeix el domini que contingui la GPO.
- 2.Fes clic amb el botó dret en Objectes de directiva de grup i, a continuació, fes clic en Administrar copies de seguretat.
- 3.Al quadre de diàleg Administrar copies de seguretat, fes clic en Examinar, localitza el sistema d'arxius que conté la GPO eliminada, selecciona la GPO, fes clic en Restauració i, a continuació, fes clic en Acceptar per confirmar la operació de restauració.

Administració de GPO

Què és una operació d'importació?



En una operació d'importació, es copien totes les configuracions de GPO des de la GPO d'origen a la GPO de destí

Administració de GPO

Cómo importar configuraciones en una GPO?

Para importar configuraciones en una GPO, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo, expande el bosque que contiene la GPO en la que deseas importar la configuración, expande Dominios, expande el dominio que contiene la GPO, expande Objetos de directiva de grupo, haz clic con el botón derecho en la GPO y, finalmente, haz clic en Importar configuración.
2. En la página Asistente para Importar configuraciones, haz clic en Siguiente.
3. En la página Copia de seguridad de GPO, haz clic en Copia de seguridad.
4. En el cuadro de diálogo Copia de seguridad de objetos de directiva de grupo, escribe la ubicación y la descripción para la copia de seguridad de la GPO y haz clic en Copia de seguridad.
5. Una vez finalizada la operación de copia de seguridad, haz clic en Aceptar y, posteriormente, haz clic en Siguiente.
6. En la página Ubicación de la copia de seguridad, haz clic en Examinar para localizar la carpeta de copia de seguridad de la que deseas importar la configuración y haz clic en Siguiente.
7. En la página GPO de origen, selecciona la GPO de la que deseas importar la configuración y haz clic en Siguiente. Si la GPO de origen contiene referencias a principales de seguridad y rutas UNC, aparecerá el cuadro de diálogo Referencias de migración. Selecciona el modo de migrar los principales de seguridad y las rutas UNC seleccionando Copiar-los de forma idéntica desde el origen o Utilizar esta tabla de migración para asignarlos a la GPO de destino y, finalmente, selecciona una tabla de migración.
8. Haz clic en Siguiente y en la página Finalización del Asistente para importar configuraciones, haz clic en Finalizar, y una vez completada la operación de importación, haz clic en Aceptar.

Comprovació i solució de problemes de GPO

Problemes habituals al implementar directives de GPO

Problema	Causa
No es pot obrir una GPO	No s'han assignat els permisos de lectura i escriptura per la GPO
No es pot editar una GPO	Un problema de xarxa
No es pot aplicar la directiva de grup a un grup de seguretat	Les GPO no s'han aplicat a grups de seguretat
La directiva de grup no afecta a un lloc, domini o unitat organitzativa	Els valors de directiva de grup no estan configurats correctament
La directiva de grup no afecta a un contenidor d'Active Directory	Les GPO no es poden vincular a contenidors d'Active Directory
La directiva de grup no afecta a un equip client	Un GPO no local pot substituir directives locals

Comprovació i solució de problemes de GPO

Cómo comprobar la configuración de directiva de grupo? (I)

UTILIZANDO EL ASISTENTE PARA MODERAR DIRECTIVAS DE GRUPO

Para crear una nueva consulta para modelar directivas de grupo, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo, examina el bosque en el que deseas crear una consulta para modelar directivas de grupo, haz clic con el botón derecho en Modelar directivas de grupo y, a continuación, haz clic en el Asistente para modelar directivas de grupo.
2. En la página Asistente para modelar directivas de grupo, haz clic en Siguiente, escribe la información adecuada en las páginas del asistente y haz clic en Finalizar.

Para ver la consulta para modelar directivas de grupo, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo.
2. Ve a través del bosque que contiene la consulta para modelar directivas de grupo que deseas ver, expande Modelar directivas de grupo, haz clic con el botón derecho en la consulta y, a continuación, haz clic en Vista avanzada.

Comprovació i solució de problemes de GPO

Cómo comprobar la configuración de directiva de grupo? (II)

UTILIZANDO RESULTADOS DE DIRECTIVA DE GRUPO

Para crear una consulta de resultados de directiva de grupo, realiza los siguientes pasos:

1. En Administración de directivas de grupo, ve hasta Resultados de directiva de grupo, haz clic con el botón derecho en Resultados de directiva de grupo y, a continuación, haz clic en Asistente de resultados de directiva de grupo.
2. En la página Asistente de resultados de directiva de grupo, haz clic en Siguiente.
3. En la página Selección de equipo, selecciona el equipo actual o haz clic en Examinar para seleccionar otro equipo y, a continuación, haz clic en Siguiente.
4. En la página Selección de usuario, selecciona el usuario actual o especifica un usuario y, a continuación, haz clic en Siguiente.
5. En la página Resumen de las selecciones, comprueba tus selecciones y, a continuación, haz clic en Siguiente.
6. En Finalización del Asistente de resultados de directiva de grupo, haz clic en Finalizar.

Para ver la consulta de resultados de directiva de grupo, realiza los siguientes pasos:

1. Abre Administración de directivas de grupo.
2. Ve hasta el bosque que contiene la consulta para modelar directivas de grupo que deseas ver, expande Resultados de directiva de grupo, haz clic con el botón derecho en la consulta y, a continuación, haz clic en Vista avanzada.

Webgrafia i/o material

- <http://www.microsoft.com/spain/windowsserver2003/technologies/management/grouppolicy/default.aspx>
- **Llibre recomenat**
 - Windows server 2008 R2