Active Directory

Active Directory

- Descripción General del servicio de directorio AD
- Introducción a AD DS
- DNS
- Usuarios, equipos, grupos y unidades organizativas
- Administrar el acceso a recursos
- Políticas de grupo

Descripción General del servicio de directorio AD

- ¿Qué es un servicio de directorio?
- ¿Qué es AD DS?
- ¿Cómo funciona?
- Otras funciones de servidor relacionadas con AD

¿Qué es un servicio de directorio?

- RAE
  - Directorio: 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.
- Espasa
  - Directorio: lista o guía de direcciones y nombres

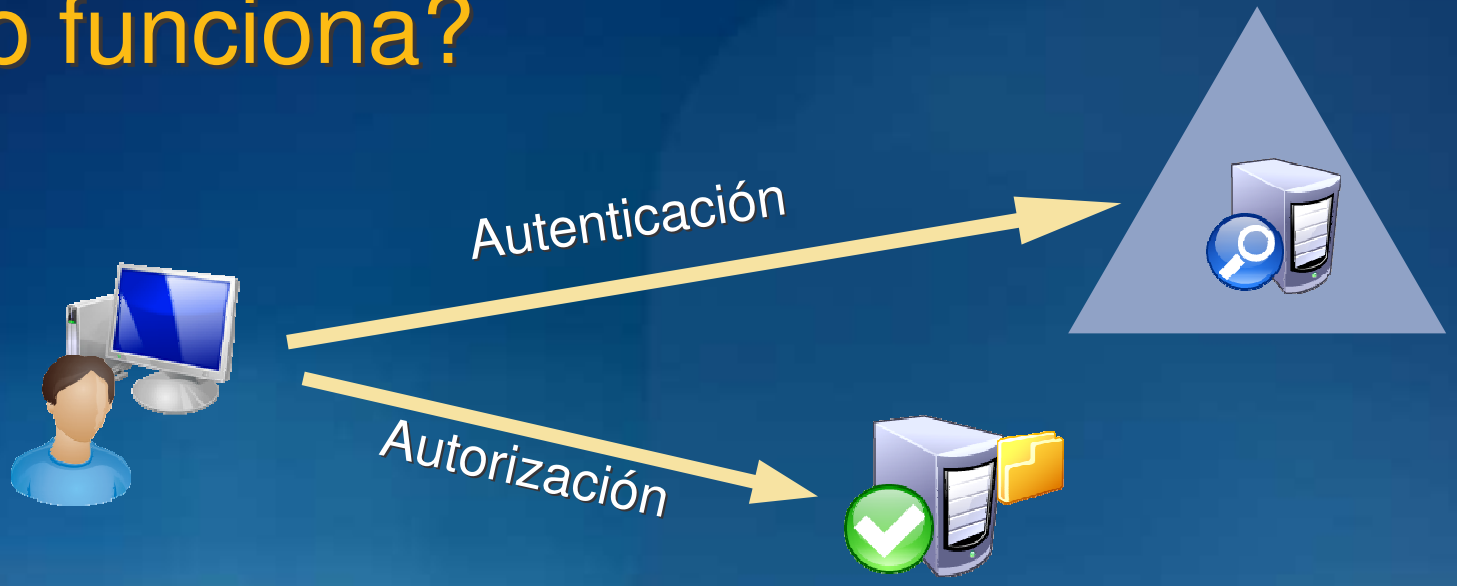
¿Qué es un servicio de directorio? (2)

- Colección de información relativa a objetos de la red
  - Usuarios
  - Equipos
  - Impresoras
  - Carpetas
- Servicios para localizar, usar y administrar tal información
- Punto central para administración y seguridad

¿Qué es AD DS?

- Active Directory Domain Services (AD DS) es un servicio de directorio para una red con W2K8
- Servicios:
  - Administración de cuentas de usuario
  - Autenticación
  - Administración de cuentas de equipo
  - Control de acceso a recursos

¿Cómo funciona?



- Creamos usuarios y equipos en el directorio (BD del directorio)
- Estos objetos podemos agruparlos
- Un usuario utilizará su cuenta de usuario para autenticarse ante un DC
- El usuario accede a los recursos de red
- Los recursos validarán de nuevo al usuario contra el AD DS

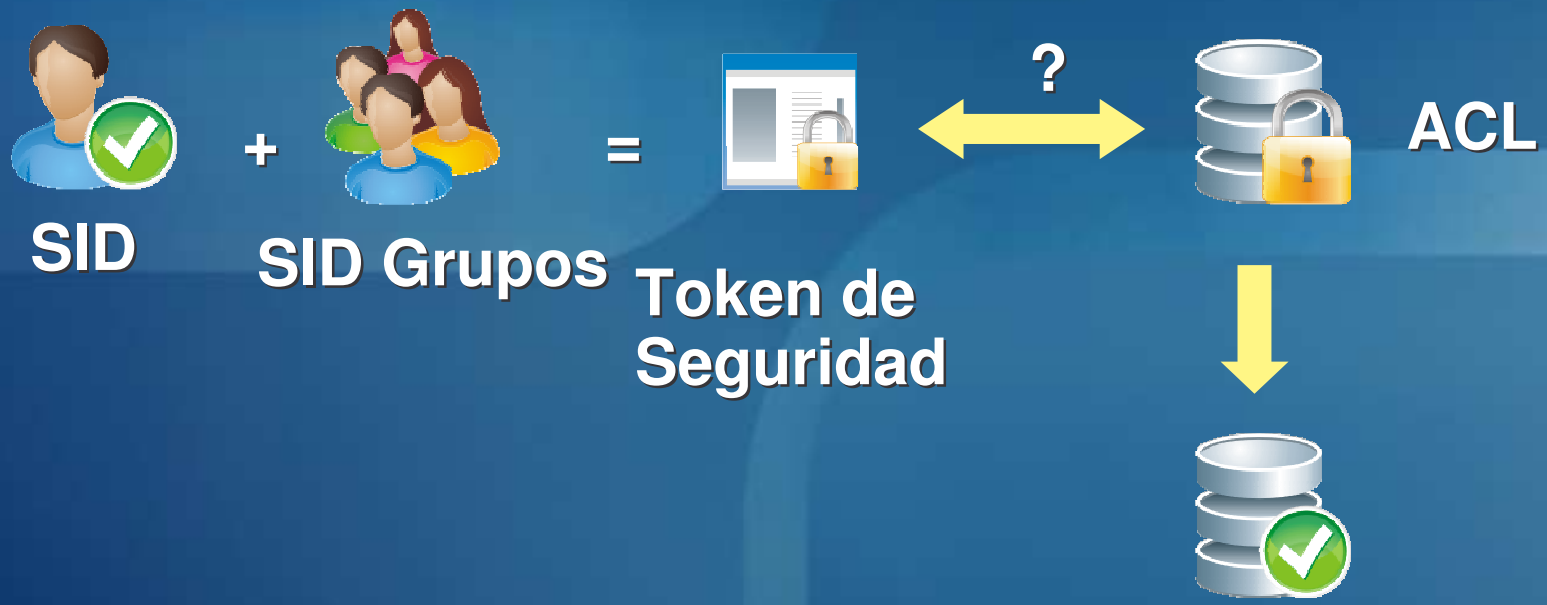
¿Cómo funciona? (2)

Autenticación: proceso mediante el cual verificamos que un usuario es realmente quien que es

- Fases :
  - Interactive Logon
    - Acceso al equipo local
  - Network Authentication
    - Acceso a los recursos de red

¿Cómo funciona?(3)

Autorización: proceso mediante el cual verificamos que un usuario autenticado tiene permiso para realizar una acción



Integración de AD DS con otras funciones de AD

- AD Lightweight Directory Services
- AD Federations Services
- AD Certificate Services
- AD Rights Management Services

Introducción a AD DS

- Descripción general de AD DS
- Componentes lógicos
- Componentes físicos

Descripción general de AD DS

AD DS almacena información acerca de los usuarios, equipos y recursos de red y permite el acceso a los recursos por parte de usuarios y aplicaciones

- Características
  - Centraliza en control de los recursos de red
  - Centraliza o descentraliza la administración
  - Seguridad integrada
  - Escalable

Descripción general de AD DS (2)

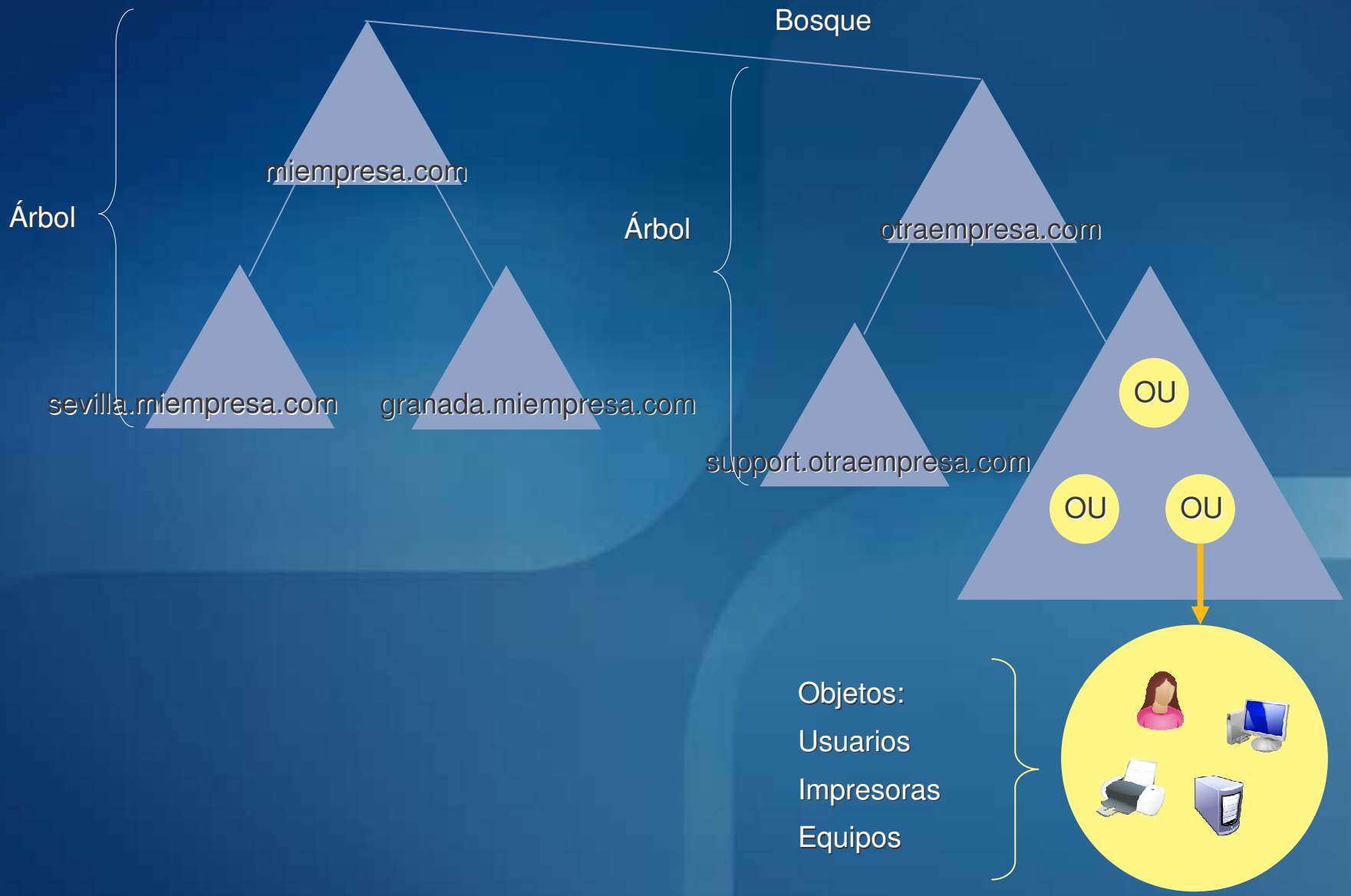
AD DS consta de componentes lógicos y físicos

- Lógicos
  - Dominios
  - Árboles
  - Bosques
  - Objetos de dominio
- Físicos
  - Controladores de Dominio (DC)
    - Servidores de catálogo global
    - RODC
  - Sitios

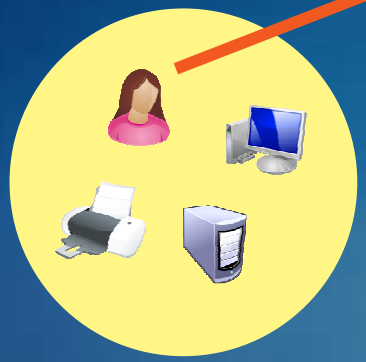
Componentes lógicos (1)

- Dominio
  - Unidad lógica básica que agrupa objetos a los que se les dará acceso a recursos
- Árbol
  - Agrupación de dominios relacionados lógicamente pero separados por razones de seguridad o administrativas.
  - Los dominios mantienen relaciones de seguridad implícitas
- Bosque
  - Agrupación de árboles.
  - Relaciones de seguridad explícitas

Componentes lógicos (2)



Componentes lógicos (3)



Usuario
31/12/2009
Ana
Martínez

Atributos
accountExpires
firstName
lastName
dNSHostName
operatingSystem

Atributos de la Clase de Objeto Usuario
accountExpires
firstName
lastName

Esquema: conjunto de atributos y clases de objetos

Práctica:

- Instalar DC
- Ver herramientas administrativas

Componentes físicos (1)

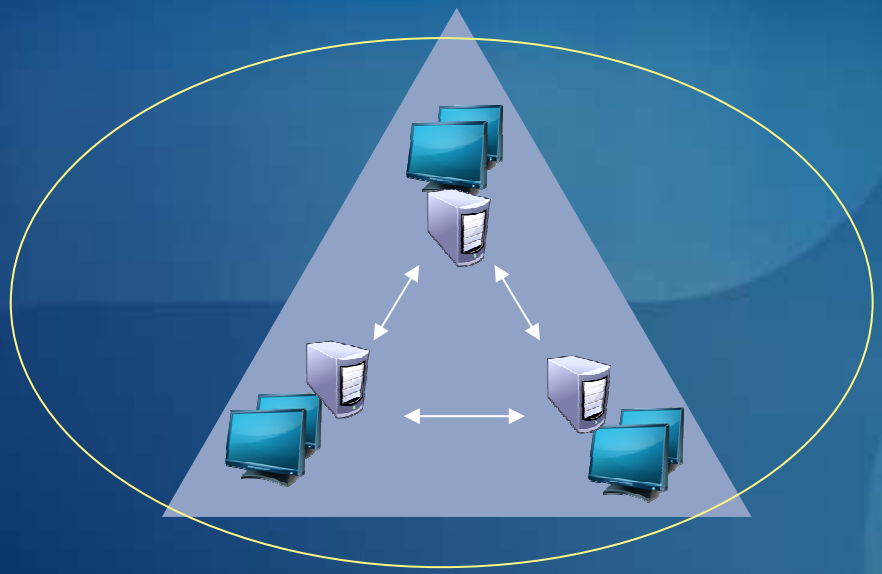
Controlador de dominio: equipo ejecutando W2K8 AD DS

- Funciones
  - Almacenamiento
    - Mantienen la Base de Datos del Directorio Activo
  - Replicación
    - Todos los DC del dominio tienen la misma copia de la base de datos
- Por seguridad debe existir más de uno por dominio
- Catálogo global
  - DC que tienen copia parcial de los objetos de todos los dominios
- RODC

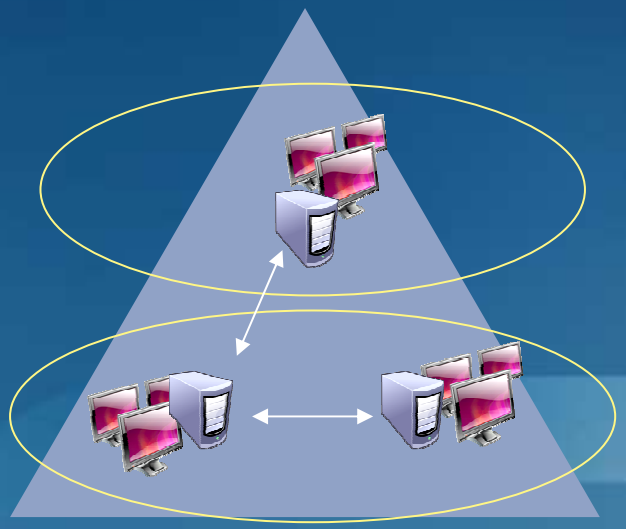
Componentes físicos (2)

Sitio: grupo de equipos conectados físicamente por una conexión rápida. Normalmente una LAN

Dominio con un solo sitio



Sitio 1



Sitio 2

Sitio 1

Dominio con dos sitios

Componentes físicos (3)

Replicación: copia de las modificaciones en la base de datos del Directorio Activo entre Controladores de Dominio

- Intra-Site
  - Los DC se encuentran en el mismo sitio
  - Un cambio se replica automática e inmediatamente al resto de DC del sitio
- Inter-Site
  - Los DC se encuentran en distintos sitios
  - Entre los servidores designados de cada sitio
    - KCC
    - Manualmente
  - Hemos de configurar conectores
    - Costes, ventana de tiempo, intervalo de replicación

Práctica

- Crear Sitios y Subredes
- Asignar subredes a sitios

Práctica

- Enlaces entre sitios

DNS

- Base del Directorio Activo
- Requisitos servidor DNS
  - Registros SRV (obligatorio)
  - Actualizaciones dinámicas
  - Transferencias de zonas incrementales
- Utilizando zonas integradas podemos utilizar la replicación para propagar cambios

Práctica

- Localizar utilizando DNS:
  - DC
  - GC

Usuarios, equipos, grupos y unidades organizativas

- Cuentas de usuario
- Cuentas de Equipo
- Grupos
- OU

Cuenta de Usuario

Objeto que hace posible la autenticación y el acceso a recurso locales o de red

- Toda la información relativa a un usuario
- Puede ser
  - Local: sólo para la máquina en que se crea
  - De dominio: para acceder al dominio y a los recursos de red
  - Integradas (built in)
- Cuando se crea W2K8 AD DS le asigna:
  - GUID
  - SID

Práctica

- Cuentas de usuario

Cuentas de Equipo

- Identifican a un equipo del dominio
- Necesaria para autenticar y auditar los equipos que acceden a la red
- Posibilita la administración utilizando Políticas de Grupo

Practica

- Agregar un equipo al dominio

Grupos

Colección de objetos similares: usuarios, equipos u otros grupos. Simplifican la administración

- Tipos
  - De distribución
    - Utilizados por aplicaciones de correo
    - No pueden utilizarse para control de acceso a recursos
  - De seguridad
    - Asignación de derechos y permisos de acceso a recursos.
- Ambos tipos pueden tener ámbito
  - Local de dominio
  - Global
  - Universal

Práctica

- Grupos y Usuarios

Unidades Organizativas (OU)

Contenedores de otros objetos del dominio

- Utilizadas para
  - Agrupar y organizar objetos con propósitos administrativos
  - Delegar la administración
  - Aplicar Políticas de Grupo
- Organización según criterios
  - Geográficos
  - Funcionales
  - Organizacionales

Práctica

- OU

Administrar el acceso a recursos

- Descripción del control de acceso
- Carpetas compartidas
- Permisos NTFS

Descripción del control de acceso

Security principal: entidad de AD DS que puede ser autenticada por Windows: usuarios, grupos, equipos … Al crearlos se les asigna un SID

Token de acceso: objeto que contiene información acerca de la identidad y los privilegios de una cuenta de usuario

Permisos: reglas para permitir o denegar el acceso a un objeto

DACL: Lista de usuarios y grupos con acceso permitido o no permitido

SACL: Lista de eventos que se auditarán

- ACE: Cada entrada en la DACL y la SACL.
- Conjunto de SIDs permitidos, denegados o auditados

Carpetas compartidas

Carpeta que permite el acceso desde la red

- Por defecto tiene permiso de Lectura para todos
- Se identifican
  - Icono
  - Comando net share
  - Administrador de Almacenamiento y Recursos Compartidos
- Se puede compartir una carpeta pero no un archivo

Carpetas Compartidas (2)

Permiso	Acceso
Lectura	Leer Ejecutar programas
Cambio	Leer Crear ficheros y carpetas Modificar ficheros Borrar ficheros y subcarpetas
Control total	Cambio Cambiar permisos NTFS en ficheros y carpetas

Permisos NTFS

Controlan a qué ficheros y carpetas puede acceder el usuario en el equipo local o en la red a través de las carpetas compartidas

Permisos para archivos	Permisos para carpetas
Lectura	Lectura
Escritura	Escritura
Lectura y Ejecución	Ver Contenido
Cambio	Lectura y Ejecución
Control Total	Cambio
	Control Total

Denegar tiene prioridad sobre Permitir

Son acumulativos

Permisos NTFS (2)

Los permisos especiales permiten controlar más finamente el acceso a los recursos.

- Son una lista de permisos más detallada
- Control más granular de los permisos
- El permiso Lectura, por ejemplo, incluye los permisos especiales
  - List Folder / Read Data
  - Leer Atributos
  - Leer Atributos Extendidos
  - Leer Permisos

Permisos NTFS (3)

La herencia permite administrar el acceso a recursos sin asignarles explícitamente permisos

Por defecto el hijo hereda del padre

- La herencia se puede bloquear
  - A nivel de carpeta
  - A nivel de fichero
- El bloqueo permite propagar nuevos permisos a los hijos

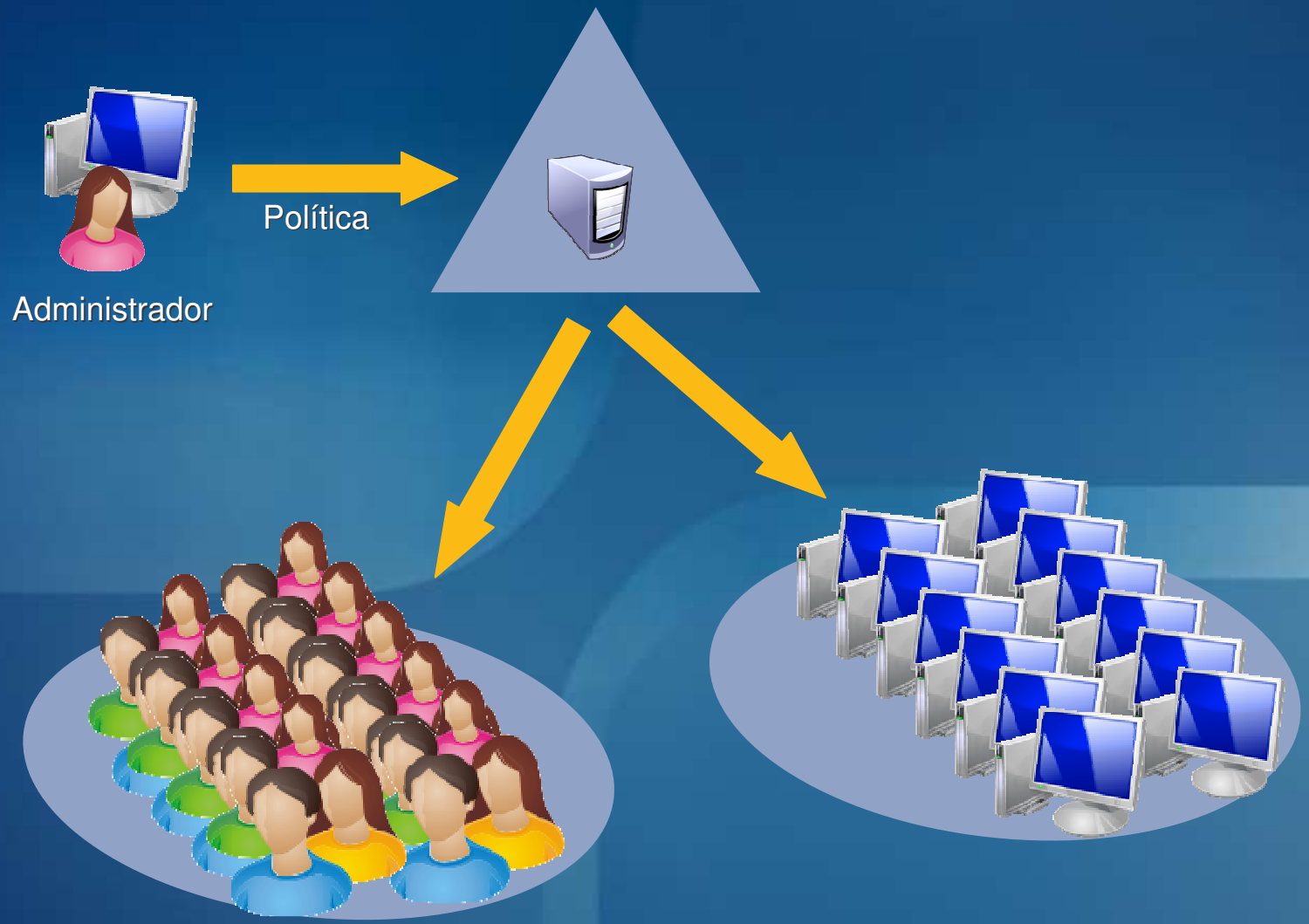
Práctica

- Carpetas compartidas
- Permisos NTFS
- Permisos efectivos

Políticas de grupo

- Descripción general
- Estructura de una GPO
- Aplicación
- Filtros y búsquedas

Más con menos



Estructura de una GPO

- En versiones anteriores de Windows 2008:
  - Son archivos de texto de extensión .adm.
  - Se guardan dentro de %SystemRoot%\Inf
- A partir de Windows 2008:
  - Son archivos XML de extensión .admx y .adml
  - La política en sí (.admx) está separada del idioma de la misma (.adml)
  - Los .admx, se guardan en %SystemRoot%\policyDefinitions
  - Los .adml, en %SystemRoot%\PolicyDefinitions\[Cultura]
    - es-es
    - en-us

Aplicación

- Se aplican sobre
  - Usuarios - HKCU
  - Equipos – HKLM
- Secciones
  - Configuración de Software
  - Configuración de Windows
  - Plantillas administrativas
- Se aplican «linkandolas» sobre
  - Dominio
  - Sitio
  - Unidades Organizativas (OUs).
- No es posible aplicarlas sobre un grupo(*), pero sí usar grupos para definir alcances y filtrados de las mismas.
- Orden de aplicación
  - Locales, Sitio, Dominio y finalmente, OUs

(*) ¿Por qué se llaman entonces Políticas de Grupo?

¿Cuándo se aplican?

- Controladores de dominio
  - Inicio del equipo
  - Cada 5 minutos
- Equipos
  - Inicio del equipo
  - Cada 90 minutos
- Usuarios
  - Inicio de sesión
  - Cada 90 minutos
- Excepciones
  - Enlaces lentos 500 kbps
  - Credenciales en caché
  - Conexiones de acceso remoto
  - Mover objetos

Práctica

- Uso del Editor de Políticas: filtro y búsquedas
- Aplicación de una GPO