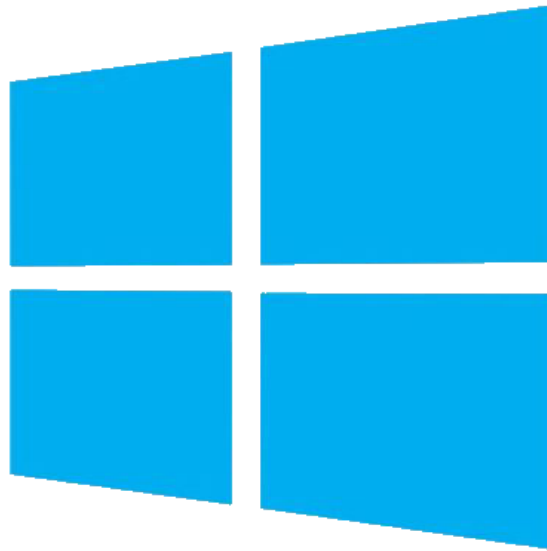


ADMINISTRACIÓN DE SISTEMAS | PRÁCTICA 3

Gestión de usuarios y recursos en Windows 2012 - Dominio Raíz



Active Directory

Por: Éric Dürr Sierra ([alu0101027005](#))

El siguiente documento pretende **recopilar todo el proceso** llevado a cabo para el desarrollo de la práctica del bloque de administración de sistemas en **Windows**. Concretamente se expone el desarrollo del servidor raíz (**CD1ASXT09** | **astxt09.local**).

Se detallarán más en profundidad aquellos aspectos que sean pertinentes al volumen teórico de la asignatura al igual que se resumirán aquellos aspectos más secundarios o que puedan resultar obvios.

Índice

1. [Introducción](#)
 2. [Situación de la organización](#)
 3. [Diseño de la estructura de la organización](#)
 4. [Desarrollo de los requisitos de la organización](#)
 - [Administración de las directivas](#)
 - [Administración de los empleados](#)
 - [Administración de los grupos](#)
 - [Administración de los prtoyectos](#)
 - [Administración de los recursos compartidos](#)
 5. [Script de automatización de nuevos usuarios \(parte opcional\)](#)
 6. [Problemas encontrados](#)
 7. [Conclusión](#)
 8. [Bibliografía y referencias](#)
-

1. Introducción

Principalmente se abordará la creación de un entorno basado en Windows 2012 que deberá soportar un número determinado de usuarios, grupos globales, grupos locales y directorios a fin de organizar cuatro proyectos. dos de ellos hospedados en el dominio raíz y los otros dos sencillamente considerados a través de los grupos globales, ya que se encuentran en otro dominio.

Los proyectos que residen en este dominio (el raíz) son el de Auditorio y el de Aeropuerto, además de los cinco de diez empleados (1, 2, 3, 7, 8) que participarán y dirigirán los mismos.

Algunas palabras claves con las que vincular este proyecto son:

- Directorio Activo

Son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

- Windows Server

Es el nombre corporativo de una serie de sistemas operativos de servidor producidos por Microsoft

- Administrador del servidor

Es una consola de administración en Windows Server que permite provisionar y manipular remota y localmente las funcionalidades y recursos del Directorio Activo

- DNS (Domain Name System)

es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

- DHCP (Dynamic Host Configuration Protocol)

Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración en forma dinámica. Sólo habrá que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente.

- Directivas

Con ellas podemos administrar virtualmente todo en los sistemas de nuestro entorno, desde el fondo del escritorio hasta qué aplicaciones pueden ejecutarse. Incluyendo no sólo los escritorios cliente sino también los servidores.

- Dominio

Un dominio de Active Directory es un contenedor lógico utilizado para administrar usuarios, grupos y computadoras entre otros objetos.

- Bosque

En Active Directory el bosque (forest) es una colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración.

- Árbol

Un árbol de dominios (tree) es una colección de uno o más dominios que comparten un espacio de nombre contiguo. Por ejemplo si el primer dominio se llama contoso.com y tiene un subdominio, este sería subdominio.contoso.com.

- Grupo global

Se usan los grupos con ámbito Global para administrar objetos de directorio que requieran un mantenimiento diario, como las cuentas de usuario y de equipo. Dado que los grupos con ámbito Global no se replican fuera de su propio dominio, las cuentas de un grupo con ámbito Global se pueden cambiar frecuentemente sin generar tráfico de replicación en el catálogo global.

- Grupo local

Los grupos con ámbito Local de dominio ayudan a definir y administrar el acceso a los recursos dentro de un dominio único.

Su visibilidad se restringe al dominio donde han sido definidos.

2. Situación de la organización

Nuestra organización va a disponer de diez empleados para llevar a cabo cuatro proyectos. Estos proyectos se encuentran divididos entre dos dominios. Cada dominio se encargará de administrar dos proyectos y cinco de los usuarios. Sin embargo los empleados y directores participan en múltiples proyectos ubicados en ambos dominios.

Empleados: Emple1, Emple2, Emple3, Emple4, Emple5, Emple6, Emple7, Emple8, Emple9 y Emple10.

Proyectos: Auditorio, Aeropuerto, Centro comercial y Parque.

Estos empleados también estarán sujetos a unos horarios y obligaciones que deberán administrarse correctamente para llevar a cabo los requisitos de la organización.

Sus roles se ven representados en la siguiente tabla:

Empleado/ Dominio	auditorio (R)		aeropuerto (R)		parque (I)		centro comercial (I)	
	Direc.	Particip.	Direc.	Particip.	Direc.	Particip.	Direc.	Particip.
emple1/R		x		x			x	
emple2/R	x				x			x
emple3/R		x				x	x	
emple4/I	x		x					x
emple5/I		x	x			x	x	
emple6/I		x		x		x		x
emple7/R	x			x			x	
emple8/R	x				x			x
emple9/I			x		x			x
emple10/I	x			x		x	x	

En la tabla se muestra la división de responsabilidades de los empleados en ambos dominios. Cada elemento se establece como:

- R: Dominio Raíz.
- I: Dominio de instalaciones.
- Direc: Director del proyecto.
- Particip: Participante del proyecto.

Cuando se establezcan los permisos estos roles supondrán la forma de establecer los permisos en base a la jurisdicción de cada tipo de empleado.

También nuestra organización está **sujeta a** una serie de **requisitos** divididos en los distintos ámbitos (**contraseñas, directorio privado, proyectos, directores e información compartida**) que se nos establecen en el enunciado.

3. Diseño de la estructura de la organización

Esta práctica se ha desarrollado de forma paralela en dos dominios alojados en diferentes máquinas virtuales, de modo que cada alumno (que ejerce el rol de administrador) deba encargarse individualmente de configurar y gestionar sus recursos para que los empleados puedan operar sin impedimentos en cada uno de los proyectos.

Uno de los dos dominios debe ser la raíz, donde se aloja la base de la organización (que es en el que se centra este informe), el cual denominamos bajo el DN "*dc=asxt09,dc=local*" (*asxt09.local*).

La elaboración del nombre del dominio se compone por:

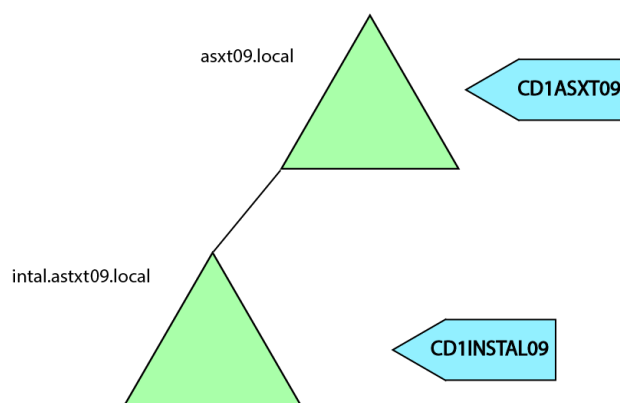
as (Administración de Sistemas)

XX (Día y turno, en este caso miércoles tarde)

YY (Número del grupo, en este caso el 9)

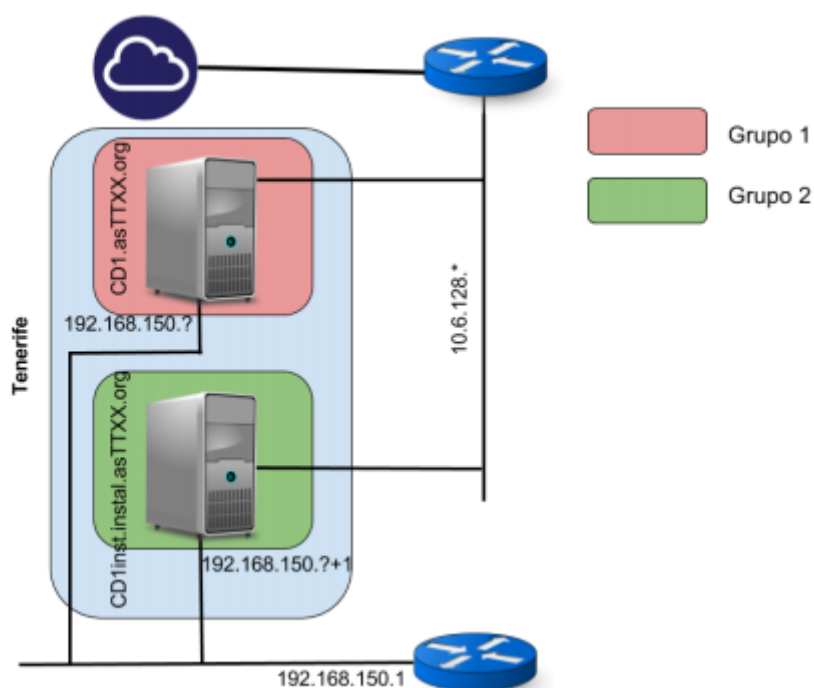
.local (La segunda componente del DN)

El otro dominio, es el de instalaciones, cuyo DN es similar pero con la extensión de subdominio *instal* (*instal.asxt09.local*). Este será hijo del dominio raíz. La siguiente imagen ilustra este bosque.



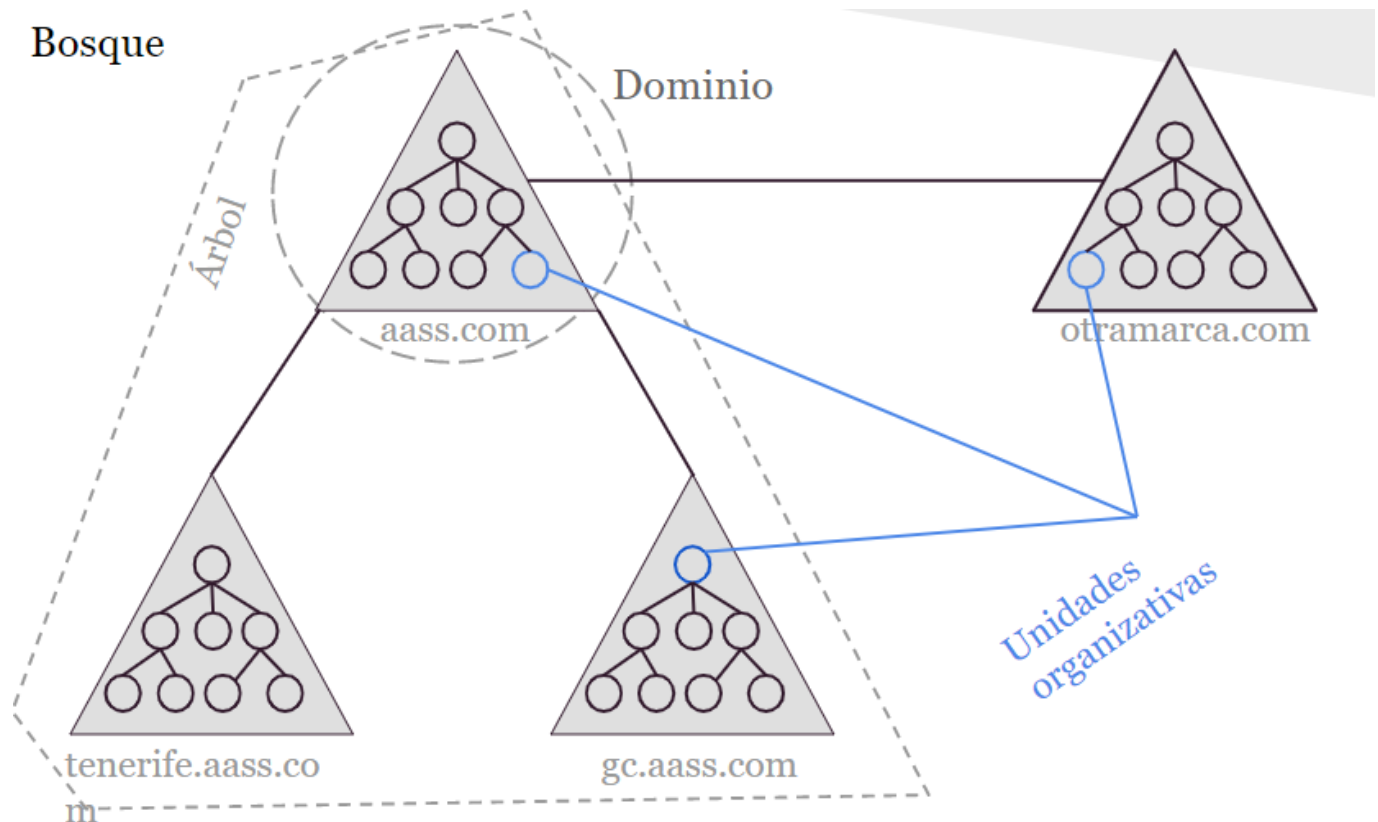
Que el dominio de instalaciones sea hijo del Raíz no implica que el padre administre ambos. Cada dominio deberá administrarse de manera independiente siendo las jurisdicciones de responsabilidad de los recursos locales a cada uno de ellos.

También se debe distinguir la estructura por sedes, cada una con su raíz, con sus máquinas y sus Administradores. En este caso la de Tenerife, en el dominio raíz hablamos del controlador de dominio *CD1ASXT09*.



Como se aprecia en la imagen cada controlador del dominio dispondrá de dos interfaces de red para conectarse; una de ellas interna 192.168.150.--- y otra externa 10.6.128.---. La interna se empleará para comunicar los controladores dentro del bosque, mientras que la externa será empleada para conectarse a la red.

Cabe destacar que no se debe confundir el bosque con sus unidades organizativas, las cuales son internas a cada dominio. La siguiente imagen ilustra este concepto:



Resumen:

Nuestro dominio será **asxt09.local**, bajo el controlador **CD1ASXT09**, dentro del bosque de la sede de Tenerife. A su vez nuestro dominio contiene la Unidad Organizativa (OU) *Practica_3* donde distinguiremos otras dos OUs, *grupos* y *empleados* que contendrán cada una de las entradas de usuarios y grupos respectivamente que iremos creando.

4. Desarrollo de los requisitos de la organización

En este apartado se expondrán los distintos aspectos de la administración del sistema de la organización en base a los requisitos exigidos por la misma. Se parte desde el punto en que la instalación y configuración del dominio ha sido realizada según los documentos proporcionados y el Directorio Activo es completamente funcional.

Además de que se ha preparado la máquina para estar conectada por medio de las dos interfaces de red, interna y externa, a la máquina del dominio de instalaciones y a internet respectivamente.

4.1. Administración de las directivas

Las directivas en Active Directory nos permiten establecer unas normas para configurar múltiples aspectos sobre el dominio. En este caso se manipularán directivas especialmente relacionadas con la configuración de seguridad y accesibilidad del dominio por parte de los usuarios del mismo. Cabe destacar que hay numerosas directivas para propósitos muy variados, pero se hablarán de las empleadas.

En primera instancia se van a preparar las directivas pertinentes a las contraseñas de los usuarios que creemos en el dominio con el fin de cumplir algunos de los requisitos impuestos por la organización. Ocuparemos en este apartado los siguientes:

1. Los usuarios deben cambiar de contraseña cada 3 meses.
2. Los usuarios no pueden cambiar las contraseñas hasta 2 semanas después de haberla cambiado.
3. No se permiten contraseñas en blanco. Deben tener una longitud mínima de 4 caracteres.
4. La nueva contraseña no puede coincidir con las dos últimas introducidas por el usuario
5. Si se producen 4 intentos fallidos de autenticación en el mismo intervalo de 10 minutos se debe bloquear permanentemente la cuenta.

Para manipular estas directivas debemos abrir la herramienta de *Administración de directivas de grupo* presente en el panel del *Administrador del servidor*. El siguiente paso es acceder a las directivas que necesitamos, para ello debemos localizarnos en:

Dominios → asxt09.local → Default Domain Policy

Una vez localizado este archivo debemos editarlo dando *click derecho* y pulsando *editar*. En la ventana emergente el siguiente paso es situarnos en:

Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directivas de contraseña

 imagen de localización de directivas de contraseña

Una vez en esta localización el siguiente paso es configurar los atributos de la directiva en base a los requisitos. Empleando la ventana de propiedades de cada uno podremos establecer :

- El historial de contraseñas con el valor 2 para recordarlas y satisfacer así el requisito 4.

 imagen de las propiedades del requisito 4

- Longitud mínima de la contraseña con valor de 4 caracteres para satisfacer el tercer requisito.

 imagen de las propiedades del requisito 3

- Vigencia máxima de la contraseña con valor 90 días para satisfacer el primer requisito


 imagen de las propiedades del requisito 1

- Vigencia mínima de la contraseña con valor de 14 días para cumplir el requisito 2

 imagen de las propiedades del requisito 2

Para cumplir un último requisito a los usuarios se les asignará como contraseña su propio nombre de usuario.

Con todo cumplimentado la directiva debería de lucir de forma similar a la siguiente imagen:

 imagen de requisitos de contraseña

Otras directivas que debemos manipular con las de asignación de derechos de usuario para que estos se puedan conectar desde el escritorio remoto y para permitir el acceso local. Esto también se encuentra detallado en el documento que antecede a la práctica, pero en un resumen global se deben manipular los atributos antes mencionados en la directiva de *Asignación de derechos de usuario* añadiendo a los grupos que queremos que accedan, en nuestro caso un grupo que contenga a los empleados del dominio. Se accede a esta directiva a través de:

Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario

4.2. Administración de los empleados

Se van a crear 5 empleados, cada uno de ellos dispondrá de un directorio privado. Se explicará como se lleva a cabo este proceso de manera manual, pero en el [apartado 5](#) de este informe se expone el script que permite automatizar el proceso.

Para llevar a cabo la creación de los usuarios debemos emplear la herramienta de Usuarios y equipos de Active Directory, la cual se encuentra también en el Administrador del servidor.

En la ventana de dicha herramienta se nos presentan las distintas entradas de nuestro dominio. Desde aquí podremos crear grupos y usuarios además de unidades organizativas y otras opciones que no conciernen a este apartado.

El primer paso es crear una unidad organizativa con:


Click derecho sobre el dominio → Nuevo → Unidad Organizativa

Aquí crearemos otras dos con el mismo procedimiento para albergar en una los usuarios y en otra los grupos (esto mantendrá las cosas más ordenadas). Es dentro de la unidad organizativa de empleados donde debemos crear los usuarios seleccionando su opción en la barra de opciones superior o con:

Click derecho sobre el Empleados → Nuevo → Usuario

Una vez ejecutemos esa opción debemos introducir los parámetros en la ventana emergente para crear el usuario. Se introducirá un nombre de pila y un nombre de inicio de sesión y en el siguiente apartado una contraseña desmarcando la opción de cambiarla en el siguiente inicio de sesión.

Este proceso se debe repetir para los 5 empleados del dominio bajo la unidad organizativa Empleados y debería quedar algo similar a esto:

 imagen de los usuarios en la unidad organizativa


En cuanto a las propiedades de cada usuario debemos atender a 3 de sus campos especialmente:

- Cuenta: para administrar sus horarios y la fecha de expiración.
- Perfil: para indicar el script de inicio de sesión y su carpeta particular.
- Miembro de: para administrar los grupos a los que pertenece el usuario.


El primer campo que vamos a revisar va a ser el de *Cuenta* para hacer cumplir los siguientes requisitos impuestos por la organización:

- Los empleados del turno de mañana (1,2 y 3 en este dominio) acceden de 08:00 a 15:00
- Los empleados del turno de tarde (7 y 8 en este dominio) acceden de 14:00 a 21:00
- Los empleados 1 y 3 del dominio se contratan temporalmente por 6 meses

Así pues, en esta pestaña se debe acceder al apartado de *Horas de inicio de sesión* e introducir las franjas correspondientes mediante la herramienta interactiva quedando de la siguiente manera para los empleados 1, 2 y 3:

 imagen de horas de inicio para mañana


y así para los empleados 7 y 8:

 imagen de horas de inicio para tarde

Por último se debe modificar para 1 y 3 la expiración de la cuenta marcando *Fin de:* e introduciendo la fecha de expiración (6 meses desde la creación en nuestro caso).

Por otro lado en la pestaña perfil podremos modificar algunos campos que nos servirán en un futuro para compartir recursos al usuario. Aquí indicaremos el nombre del inicio de sesión y su carpeta particular marcando **Conectar:** e indicando el nombre del recurso compartido así como la unidad donde se va a montar.

Debería quedar como en la imagen siguiente:

 imagen de pestaña perfil


Por otro lado para la creación de los directorios de cada usuario vamos a crear carpetas en *C:/home* siendo *home* una carpeta creada por nosotros. Se debe crear una por empleado y acto seguido modificar sus propiedades para que solo su propietario y el administrador tengan acceso a ella. De esta manera, por cada directorio personal vamos a modificar los permisos dentro de la ventana de propiedades.

Para modificar los permisos debemos acceder a la pestaña de *Seguridad* donde podremos modificar quien tiene acceso al recurso. Debemos *editar* los permisos y en la ventana emergente agregar al usuario pertinente y eliminar los grupos o usuarios que no nos sean de interés (todos menos el Administrador, los Administradores y el usuario en cuestión). La siguiente imagen ilustra como debería quedar:

 imagen de grupos o usuarios home

Una vez hecho esto queda modificar los permisos para que este usuario tenga control total dentro de su directorio excluyendo la eliminación del mismo o la modificación de sus permisos. A esto accedemos

mediante el botón de *Opciones avanzadas* de la pestaña *Seguridad*. En la ventana emergente debemos seleccionar al empleado y *Editar* sus permisos avanzados. Deben quedar seleccionados, solo para este directorio, tal y como muestra la imagen:

 imagen de permisos home

Tras esto solo quedaría compartir el recurso, pero eso se detalla en una sección futura.

4.3. Administración de los grupos

De cara a poder asignar permisos a los usuarios en calidad de ejercer distintos roles (*participante o director*) en cada uno de los proyectos se deben crear grupos globales que encapsulen bajo dichos roles a los empleados de cada proyecto de cara a que estos puedan ser accesibles por el dominio de instalaciones. Además se deben crear grupos de carácter local que tendrán la funcionalidad de recopilar los grupos globales de cada uno de los proyectos y proporcionar permisos a los empleados de una manera más controlada.

El siguiente esquema ilustra esta estructura:

 imagen de estructura de grupos

Los grupos se van a crear siguiendo el mismo proceso empleado en el [apartado anterior](#)

4.4. Administración de los proyectos

4.5. Administración de los recursos compartidos

5. Script de automatización de nuevos usuarios (parte opcional)

6. Problemas encontrados

7. Conclusión

8. Bibliografía y referencias

- [Documentio de instalación AD-IAAS](#)
- [Documento de instalación de Máquina windows en el IAAS](#)
- [Manual de Active Directory](#)
- [Documentación de Windows 10 y Windows Server 2016 para PowerShell](#)
- [Grupos de Active Directory | Windows Server 2012](#)
- [Conceptos de Active Directory | Exchange](#)
- [Tutorial de creación de usuarios en AD mediante PowerShell](#)
- [Uso de CVS en PowerShell | Documentación de Microsoft](#)