Dominios en Windows: Directorio Activo (AD)

Sumario

Introdución

O Directorio Activo (*Active Directory* ou AD) é a peza crave dos sistema operativos de rede de Microsoft Windows e permite, como se verá, moitas funcionalidades como: a centralización de usuarios, as directivas de grupo, as xerarquías de dominio, etc.

Igual co OpenLDAP que vimos en Linux, o Active Directory tamén é un servizo de directorio que permite centralizar a autenticación de usarios e establecer un repositorio central de información para toda a súa infraestrutura de rede, facilitando a administración. O AD Mellora as características dos anteriores servizos de directorio baseados en Windows (principalmente o concepto de controlador de dominio introducido con Windows NT) e agrega características completamente novas.

Está deseñado para funcionar nunha instalación de calquera tamaño, desde só un servidor con algúns centos de obxectos, até múltiples servidores e millóns de obxectos. As contas de usuarios que xestiona Active Directory almacénanse na **base de datos SAM** (*Security Accounts Manager*).

Definicións

Hai unha serie de termos que é necesario coñecer en relación co AD:

- **Nome de dominio**. É un concepto que xa coñecemos do DNS e son as equivalencias entre os nomes de equipos e a súa dirección IP.
- **Controlador de Dominio**. Servidor Windows con AD instalado que almacena, mantén e xestiona a base de datos de usuarios e recursos da rede.
- **Árbore de dominio**. Tamén é un concepto importado do servizo DNS e é o conxunto de dominios formado polo nome de dominio raíz (MEUDOMINIO.GAL) e o resto de dominios relacionados co nome raíz, é dicir, os subdominios. Por exemplo, se tivésemos un subdominio VENTAS, nomearíase como "VENTAS.MEUDOMINIO.GAL", e formaría unha árbore de dominios co dominio raíz.
- **Bosque de árbores de dominios**. É o conxunto de árbores de dominio que non constitúen un espazo de nomes contiguo. Por exemplo, se o noso servidor administrase outro dominio raíz chamado ASIM.ORG, este novo dominio, xunto co anterior MEUDOMINIO.GAL formarían o bosque de árbores de dominios.

O concepto de dominio é máis amplo que no DNS, de feito un dominio en Windows pode estar formado por un único nome de dominio, ou por unha árbore ou incluso un bosque. Isto dependerá do tamaño da institución.

Instalación e configuración

Antes de comezar coa instalación do AD hai que configurar a rede do servidor para que teña unha IP estática. Para instalar e configurar o dominio faremos tres accións:

1. Instalar o AD.
2. Configurar os equipos cliente, é dicir, dar de alta un equipo no dominio.
3. Crear un usuario no AD e comprobar que podemos autenticarnos dende un cliente.

Instalación do AD

Para instalar o AD nun servidor Windows 2003 Server hai que convertelo nun **controlador de dominio primario** ou principal (PDC). Para iso executaremos no servidor, dende Executar do Menú Inicio, o seguinte comando:

```
dcpromo
```

Archivo:Ejemplo.jpg

Lanzarase un asistente que nos informa de que imos proceder a instalar Active Directory. Durante a instalación preguntarásenos sobre diferentes aspectos como:

- Problemas de compatibilidade que poden existir con versións anteriores de Windows.

Archivo:Ejemplo.jpg

- Se se quere crear un controlador de dominio novo ou un **controlador de dominio adicional** (BDC) para un xa existente. Esta última opción escolleríase no caso de ter un equipo de backup para o controlador de dominio existente.

Archivo:Ejemplo.jpg

- Se desexamos crear un dominio nun novo bosque, un dominio secundario nunha árbore de dominios existente ou unha nova árbore de dominios nun bosque existente. No caso máis simplre seleccionaremos a opción por defecto Crear novo dominio nun novo bosque.
- O nome que desexemos para o noso dominio. Se dispomos dun dominio rexistrado en Internet podemos facer uso del, se non, indicaremos un nome de dominio interno.

Archivo:Ejemplo.jpg

- O nome NetBIOS para o noso dominio, co fin de que versións anteriores de Windows (por exemplo "Windows 98") poidan facer uso del.
- O lugar onde se almacenarán diferentes ficheiros necesarios para o AD (deixaremos as rutas por defecto):
    - **A base de datos**. Almacénase no ficheiro NTDS.dit que é o que contén toda a información do AD, usuarios, grupos, impresoras, información sobre o bosque, árbores, dominios, etc., é dicir, é unha base de datos de obxectos.
    - **Os ficheiros de log**.
    - **O volume do sistema compartido**. Contén información do dominio que se replica ao resto de controladores de dominio da rede.

Para que o AD funcione debemos habilitar o servidor DNS. Afortunadamente, o propio asistente da instalación instálao se escollemos esta opción, ademais, xa creará a zona para o dominio. Archivo:Ejemplo.jpg

Tamén debemos especificar se permitiremos permisos compatibles con servidores anteriores a Windows 2000 Serve (fundamentalmente "Windows NT"). Se no dominio vai haber servidores NT mesturados con 2003 débese seleccionar a primeira opción pero por motivos de seguridade é mellor seleccionar a opción "Permisos compatibles só con sistemas operativos de servidor Windows 2000 ou Windows Server 2003". Archivo:Ejemplo.jpg

Hai que especificar tamén un contrasinal para poder acceder ao equipo en modo "Restauración de servizos de Active Directory": Archivo:Ejemplo.jpg

Como resumo final das opcións indicadas, móstrase unha ventá informativa con todos os parámetros seleccionados a través do asistente de instalación de Active Directory. Se aceptamos empezará a instalación do AD: Archivo:Ejemplo.jpg

Configuración dos equipos clientes

Este proceso consiste en incluír os equipos clientes no dominio. O equipo que se vaia introducir no dominio pode ter un S.O. Windows 2000 (Profesional ou Server), XP ou Windows 2003. No caso dos server (2000 server e 2003) non deben ter instalado o AD.

O primeiro que hai que facer é configurar o cliente DNS do equipo cliente para que apunte á IP do servidor DNS que ten a información sobre o dominio do que vai formar parte. Ten que ter o resto de parámetros de rede configurados axeitadamente.

No equipo cliente hai que premer co botón dereito do rato na icona Mi PC-->Propiedades-->Nome de equipo-->Cambiar e escoller un nome para o equipo e o dominio.

Alta de usuario

Para crear un usuario do dominio, accederemos a Usuarios e equipos de Active Directory nas Ferramentas administrativas do Panel de Control. Unha vez alí, prememos co botón dereito do rato sobre o cartafol Users e seleccionaremos a opción Novo e dentro dela Usuario.

Xestión de usuarios e grupos

Podemos definir o **perfil dun usuario** como o contorno cargado polo sistema cando este inicia sesión. Inclúe a configuración do usuario como: elementos de programa, conexións de rede, conexións de impresoras, escritorio, documentos, etc. Devanditos perfís de usuario créanse automaticamente a primeira vez que un usuario inicia unha sesión.

Se nas propiedades do usuario se lle asocia un directorio do servidor como ruta de acceso ao seu perfil, estamos a definir un perfil denominado **perfil móbil**, e que se caracteriza porque se descarga no equipo local cando un usuario inicia sesión, e actualízase tanto localmente como no servidor cando o usuario pecha a sesión. Os perfís de usuarios móbiles están dispoñibles no servidor cando se inicie unha sesión en calquera equipo do dominio, exactamente igual que acontecía co OpenLDPA e NFS en Linux.

É posible dispor dun perfil móbil pero que non se actualiza cando o usuario pecha a sesión. A este perfil chámaselle **perfil obrigatorio**, e tamén se descarga cada vez que o usuario inicia sesión. Os perfís obrigatorios créaos o administrador e asígnaos a un ou varios usuarios a fin de crear perfís de usuario invariables.

Directivas ou políticas

As directivas ou políticas permiten establecer distintas configuracións para os usuarios ou equipos, entre as que poden especificarse, por exemplo, aqueles programas que desexemos que se atopen dispoñibles, os que aparecerán no seu Escritorio, as opcións do menú Inicio, do navegador, etc.

As directivas aplícanse sempre sobre unha OU (Unidade Organizativa) ou sobre o dominio e divídense en:

- **Directivas de configuración de equipo**, para aplicar aos equipos que estean na Unidade Organizativa ou dominio e nas súas ramas.
- **Directivas de configuración de usuario**, para aplicar aos usuarios que estean na Unidade Organizativa ou dominio e nas súas ramas.

Aínda que algunhas directivas de usuarios poden ser modificadas por estes na sesión de traballo, os cambios realizados non se gardarán de forma que a próxima vez que inicie sesión en calquera máquina do dominio, volveránselle a aplicar as directivas definidas polo administrador.

Para configurar unha directiva hai que premer co botón dereito do rato sobre o nome do dominio ou OU, dentro da ferramenta de xestión de usuarios e equipos do AD, e seleccionar Propiedades-->Directiva de grupo-->Modificar.

Ademais de modificar directivas como no caso anterior tamén podemos crear o noso conxunto de directivas propio. Para iso, hai que premer en Propiedades-->Directiva de grupo-->Nueva. Así crearemos un novo **contedor de directivas**. As políticas almacénanse en sysvol para que os clientes poidan acceder a elas.

Existen moitas directivas polo que o administrador do dominio deberá analizar unha por unha cales son do seu interese, por exemplo:

- **Bloqueo de conta**. Permite establecer un número máximo de intentos para o acceso ao sistema, a partir do cal se bloquee a conta de usuario.
- **Política de claves**. Obriga a que os contrasinais dos usuarios teñan unha lonxitude mínima e unha caducidade.
- **Direccións URL**. Permite, entre outras cousas, que todo usuario do dominio teña por páxina de inicio a que se especifique e que non poida modificala.

Cando se modifican directivas estas poden tardar certo tempo en aplicarse. Para forzar a súa aplicación hai que executar GPUPDATE (Group Policy Update) en liña de comandos:

```
gpupdate
```

Para restaurar as directivas orixinais temos outro comando:

```
dcgpofix
```

Prioridade entre directivas

As directivas poden aplicarse a equipos locais, sitios, dominios e unidades organizativas. Por exemplo, un usuario estará nun equipo local que á súa vez se situará nun sitio, pertencerá a un dominio e será membro dunha OU. Pode darse o caso de que no equipo local se aplique unha directiva, outra para o sitio, outra para o dominio e outra para a OU. Polo tanto, pode haber políticas que se contradigan entre si. O sistema ten prioridades entre as directivas segundo onde estean asignadas. A orde de aplicación é a seguinte:

As directivas dunha **OU** prevalecen sobre as do **dominio**, que á súa vez prevalecen sobre as de **sitio**, as cales á súa vez prevalecen sobre as do **equipo local**. As políticas súmanse, só se anulan en caso de ser contraditorias entre elas. Por exemplo, se no dominio habilitamos a política de deshabilitación do panel de control e na OU deshabilitamos esta política, e supomos que ningunha outra das políticas do dominio entra en contradición con ningunha outra das da OU, o resultado que se aplicará a un obxecto contido dentro da OU será a suma de ambas, polo que a política que se aplica será a da OU, non a do dominio, e polo tanto o panel de control será visible.

 **RECORDA**

Prioridade. Aplicaranse as directivas máis xerais sempre e cando non existan contradicións coas directivas máis específicas.

Cando unha directiva **non está configurada** aplícase o que indique a mesma directiva definida nun obxecto superior. Por exemplo, se na unidade organizativa Controladores do dominio non hai definida unha política de lonxitude de claves aplicarase a política do dominio, que está por enriba.

--Arribi 12:15 6 oct 2009 (BST)