Recursosinformáticos

Windows Server 2016

Arquitectura y Administración de los servicios de dominio Active Directory (AD DS)

Jean-François APREA

eni

Introducción a los servicios AD DS

DNS: conceptos, arquitectura y administración

Integración de las zonas DNS en Active Directory

Servicios de ubicación AD DS y servicios DNS

Componentes de la estructura lógica

Grupos, unidades organizativas y delegación

Fundamentos de las directivas de grupo

Gestión de software con directivas de grupo

Configuración de los roles Active Directory

Introducción a Azure Active Directory

Windows Server 2016

Servicios de dominio Active Directory

Este libro sobre Active Directory se dirige a los **arquitectos y administradores de red** que deseen diseñar y gestionar una infraestructura de servicios de dominio Active Directory con Windows Server 2016. El enfoque de "**arquitectura**" del libro permite al lector comprender los conceptos esenciales y tomar conciencia de las mejores prácticas.

Los primeros capítulos describen la implementación y administración de los**servicios DNS** con los **servicios Active Directory**. Los capítulos siguientes insisten en los elementos de estructura como los **dominios**, las **UO**, los**árboles**, los **bosques** al igual que la creación y la configuración de los objetos de directivas de grupo (uso de la consola **GPMC**, análisis y modelización **RSoP**, **delegación**, etc). Las nuevas posibilidades de las**Preferencias de las directivas de grupo** se presentan y luego el **ciclo de vida del software** se trata empleando la administración de software dentro de las infraestructuras Active Directory.

El siguiente capítulo aborda la configuración de los **roles de servidor** con los servicios Active Directory de Windows Server 2016.

Los principios fundamentales y la configuración de los servicios de**certificados AD CS**, las novedades y la instalación de los servicios de federación **AD FS**, los servicios **LDAP AD LDS** y la gestión de los servicios de derechos digitales **AD RMS** nos permitirán visualizar la importancia de las novedades aportadas por Windows Server 2016. El último capítulo nos permitirá descubrir los **servicios Azure AD** y comprender el valor aportado por las soluciones Cloud Microsoft Azure en modo híbrido.

Los capítulos del libro:
Prólogo – Introducción a los servicios AD DS – DNS: conceptos, arquitectura y administración – Integración de las zonas DNS en Active Directory – Servicios de ubicación AD DS y servicios DNS – Componentes de la estructura lógica – Grupos, unidades organizativas y delegación – Fundamentos de las directivas de grupo – Gestión de software con directivas de grupo – Configuración de los roles Active Directory – Introducción a Azure Active Directory

---

Jean-François APRÉA

Consultor Senior, Arquitecto de infraestructuras Microsoft en RDI (filial del Grupo SPIE ICS), **Jean-François APRÉA** cuenta con el reconocimiento MVP (Microsoft Most Valuable Professional) Cloud & Datacenter Management desde hace más de 10 años. Cuenta con la certificación MCSE Private Cloud & Server Infrastructure al igual que Microsoft Azure Specialist (Implementing and Architecting Azure Solutions). Aparte de su participación en los programas beta y seminarios técnicos de Microsoft, ha participado en múltiples proyectos de infraestructuras para grandes empresas y conoce a la perfección las expectativas de los arquitectos y administradores Windows Server y System Center.

Introducción

Con Windows Server 2016, y como ocurre en cada entrega de una versión principal, Microsoft introduce un importante número de nuevas funcionalidades.

Más allá de las mejoras habituales que hemos podido conocer con Windows Server 2012 R2 y versiones anteriores, Windows Server 2016 sigue dentro de la estrategia Cloud OS de Microsoft con avances importantes para atender los desafíos del cloud. Así, con la nueva versión de Hyper-V, el soporte de los contenedores de Windows y la introducción de Nano Server, esta última versión de Windows Server se adhiere a los principios de desarrollo de aplicaciones modernas conservando las prácticas conocidas por los equipos de TI.

Windows Server 2016, ¡una gran versión!

Para convencer, basta con listar los ejes de evolución aportados. En efecto, Windows Server 2016 incorpora las nuevas tecnologías y funcionalidades listadas a continuación:

- Storage Spaces Direct: esta nueva tecnología permite la aplicación de nuevos sistemas de almacenamiento altamente disponibles usando almacenamiento de tipo local. Se trata de un avance muy importante en el marco de la estrategia "All Software Defined" de Microsoft y el soporte de un modelo de hyper-convergencia. Con este importante bloque orientado al SDS - Software Defined Storage (SDS), el objetivo es simplificar la puesta en marcha y la administración del almacenamiento, permitiendo un uso más fácil y generalizado de los nuevos discos de tipo SATA y NVMe. Cabe recordar que estos tipos de discos no podían ser utilizados con los clústers Windows Server 2012 R2, los entornos Storage Spaces y discos compartidos.

- Storage Replica: esta nueva tecnología permite la aplicación de la replicación de almacenamiento a nivel de bloques en modo sincróno, y esto, de manera totalmente transparente para el equipo. Storage Replica es un avance significativo que puede ser utilizado entre los clústers, y también entre simples servidores para construir -soluciones de plan de recuperación de la actividad (PRA) a bajo costo. La solución también podrá ser utilizada en el marco de soluciones de alta disponibilidad (HA), con los clústers repartidos en varios lugares geográficos. La utilización de la replicación síncrona permite la puesta en espejo de los datos en diferentes lugares de tal manera que los volúmenes controlados por Storage Replica dispondrán entonces de una tolerancia a las interrupciones del servicio. Además de la replicación síncrona, Storage Replica soporta un modelo de replicación asíncrona que puede ser empleado cuando las conexiones de red son menos eficaces. En este último caso, la integridad de datos estará garantizada, pero una pérdida de datos "transitoria" deberá ser prevista y soportada.

- Mejor tolerancia de los clústers: los servicios de Transición de Windows Server 2016 se han mejorado para ofrecer una mayor resiliencia de las máquinas virtuales en entornos cloud que conocemos hoy. De esta forma, podemos contemplar el uso de hardware menos sofisticado a través de una mejor gestión de los fallos transitorios. Este punto es todavía más cierto porque estos fallos son mucho más numerosos hoy en día que los fallos de servicio de almacenamiento, considerados tan críticos desde el punto de vista de los datos. Para conseguirlo, Windows Server 2016 minimiza aún más los tiempos de parada o indisponibilidad de las máquinas virtuales minimizando los fallos de comunicación intra-cluster y aumentando así la persistencia operacional de cada uno de los nodos.

- Mejor gestión de los clústers multi-sitio: los clústers de conmutación cuyos nodos están distribuidos en varios sitios pueden agruparse en función de su ubicación. Esta mejora es importante porque las operaciones internas relacionadas con el funcionamiento del clúster se simplificarán (comportamiento de conmutación, políticas de inversión, gestión de *heartbeat*, gestión del quorum).

- Nuevos clústers de conmutación por error autónomos: los clústers de conmutación ya no dependen de Active Directory. Desde hace más de 20 años, los nodos miembros de un clúster debían ser miembros de un dominio NT o Active Directory. Ahora, Windows Server 2016 es mucho más flexible mediante la creación de clústers de conmutación independientes (llamados en inglés Workgroup Clusters). Por supuesto, la integración de los nodos dentro de un dominio Active Directory es siempre posible, los miembros de un mismo clúster pueden formar parte de un único dominio de Active Directory. Cabe señalar también que Windows Server 2016 soporta un nuevo escenario donde los miembros de un mismo clúster de conmutación pueden pertenecer a varios dominios Active Directory.

- Actualización de los clústers de conmutación: los clústers de conmutación de Windows Server 2012 R2 pueden ser actualizados a nodos Windows Server 2016 sin ninguna incidencia sobre el funcionamiento de las máquinas virtuales Hyper-V o de los servicios de almacenamiento SOFS (*Scale-Out File Server*) utilizados por el clúster. Esta nueva funcionalidad - llamada en inglés Cluster Operating System Rolling Upgrade, permite al equipo de TI actualizar progresivamente a Windows Server 2016 cada nodo que funcione inicialmente en Windows Server 2012 R2. Una vez actualizado el conjunto de nodos, el clúster puede alcanzar el nivel "Windows Server 2016", para que las nuevas funcionalidades ofrecidas por éste estén disponibles.

- Testigo en Azure para los clústers de conmutación: llamado en inglés Cloud Witness, testigo en la nube; esta nueva posibilidad de configurar un testigo para compartir archivos permite posicionar quorum sobre Azure dentro del Servicio de Almacenamiento Microsoft Blob Storage. De esta forma, no es necesario disponer de un centro de datos adicional para mantener quorum en el caso de un clúster cuyos nodos estén ubicados en varias ubicaciones. Cabe destacar el escaso impacto económico de esta solución de arquitectura en Azure directamente relacionado con el escaso número de operaciones de lectura y escritura que se llevarán a cabo.

- PowerShell: con una primera introducción en Windows 10, PowerShell 5.0 en -Windows Server 2016 mejora la seguridad empleando evoluciones en la protección del entorno de ejecución.

- PowerShell Direct: esta novedad permite la administración con Windows Power-Shell dentro de una máquina virtual Hyper-V sin que sea necesario disponer de conectividad de red. Esta nueva capacidad hace más fáciles las tareas de administración de las máquinas virtuales con independencia de las limitaciones introducidas por la configuración de red.

- Servicios RDS de Windows Server 2016: los servicios de terminales RDS evolucionan con el soporte de OpenGL para las tarjetas gráficas virtuales RemoteFX. Esta nueva versión de los servicios RDS soporta también las sesiones personales RDS - llamadas en inglés Personal Session Desktops. Esta funcionalidad permite aumentar el nivel de seguridad al separar por completo las sesiones RDP de las máquinas virtuales de aquellas de los servidores Hyper-V disponibles dentro de la plataforma cloud Microsoft Azure o dentro de un entorno local «on-premise».

- Servicios de red SDN - *Software Defined Networks*: Windows Server 2016 introduce una nueva infraestructura de red para el centro de datos. Esta infraestructura está compuesta por el nuevo rol llamado Controladora de red. Éste proporciona un punto de automatización para la implementación de las operaciones de configuración, supervisión y diagnóstico de las redes virtuales, las redes físicas y las direcciones IP. Microsoft proporciona muchos scripts basados en SDN en Windows Server 2016 para configurar estos elementos y también para crear sus propias funciones. Cabe señalar que System Center Virtual Machine Manager 2016 también permite la gestión del nuevo rol de Controlador de red de Windows Server 2016.

- Nano Server: con Windows Server 2016, se ofrece un nuevo enfoque de instalación. Nano Server recoge los principios de las instalaciones en modo Core pero con una huella aún más baja, inferior a 400 MB - aproximadamente 20 veces menos que una versión completa del sistema operativo. Ultra optimizado y solo administrado de forma remota al estar desprovisto de los componentes de apertura de sesión local y RDS, este tipo de instalación se recomienda en particular para los centros de datos con los roles Hyper-V, los servicios de almacenamiento Storage Spaces Direct, los servicios de archivo SOFS, los roles de Servidor DNS e IIS sin olvidar el soporte para los contenedores. Nano Server puede ser instalado en máquinas físicas, máquinas virtuales, soporta los contenedores Hyper-V y Windows Server y puede ser desplegado en a penas 40 segundos - comparado con los 5 minutos necesarios para realizar una instalación en modo Server Core y los 20 minutos de una instalación de Windows Server Standar o Datacenter. Su tamaño permite por supuesto reducir al mínimo las operaciones de mantenimiento empleando un número restringido de correctivos a aplicar.

- Containers Windows Server: se trata de uno de los ejes más importantes del desarrollo para Microsoft. En efecto, Windows Server 2016 incluye el soporte de los contenedores Docker. Esta nueva tecnología proveniente de forma directa de los entornos cloud bajo Linux abre nuevas perspectivas para un futuro, sin duda no tan distante. La idea es crear un nuevo modelo al lado de las máquinas virtuales tradicionales. Gracias a los contenedores, será posible consumir menos recursos, minimizar las dependencias en relación con el sistema operativo y ofrecer un nuevo modelo de despliegue de aplicaciones mucho más ágil - Modelo DevOps. Desde el punto de vista del administrador, los contenedores Windows Server pueden ser desplegados y gestionados empleando el cliente Docker para Windows y también empleando Windows PowerShell. Además de estos avances, la utilización de contenedores Windows Server permite a las aplicaciones estar aisladas dentro del contenedor y no dentro de una máquina virtual mucho más pesada en términos de consumo de recursos de disco, memoria y CPU, sin hablar del tiempo de reinicio inherente al sistema operativo y gestión de las múltiples actualizaciones a menudo inútiles de forma funcional.

  Una extensión de los Containers Windows Server también es presentada con los Containers Hyper-V en especial adaptadas a los entornos aplicativos que requieren un nivel de aislamiento más elevado.

Con respecto a los servicios de Active Directory... ¿Evolución o revolución?

Active Directory, aparecido con Windows 2000 Server tiene ahora más de 15 años, constituye la fundación de las redes de empresas que emplean las tecnologías Microsoft. Las novedades y mejoras de Windows Server 2016 para Active Directory son muchas, pero los fundamentos son siempre los mismos. ¡Por fortuna para todas las infraestructuras ya desplegadas desde hace varios años!

A medida que avancemos en la lectura de este libro, los arquitectos e ingenieros de sistema que ya conocen los servicios de dominio de Active Directory tendrán la oportunidad de consolidar sus conocimientos descubriendo las modificaciones aportadas por Windows Server 2016. Por su parte, quienes se sumerjan por primera vez en los servicios de dominio de Active Directory descubrirán el

conjunto de estas bases, ¡y mucho más si se considera las novedades introducidas por esta nueva versión!

Windows Server 2016 es una versión mayor en más de un sentido. Asimismo, permitirá sin duda aumentar los servicios ofrecidos en el entorno local la empresa con miras a la posibilidad de adherirse a un modelo de cloud híbrido moderno basado en el cloud Microsoft Azure.

En este libro, hemos acordado que la utilización del término "Windows Server 2016" consideraba también las versiones anteriores Windows Server 2012 y Windows Server 2012 R2. Sin embargo, encontraremos una observación cuando sea necesario precisar algunas particularidades de estas versiones y también de las versiones anteriores, Windows Server 2008 R2, e incluso Windows Server 2003.

Buena lectura

Función del servicio de directorio en la empresa

El Servicio de directorio es uno de los componentes más importantes de un sistema de información, sea cual sea su tamaño. Ofrece los servicios centrales capaces de coordinar los múltiples elementos que componen al sistema de información. Por ejemplo; ¡imaginemos que un usuario busca un elemento de la red sin saber el nombre o el lugar! En primer lugar, el problema parece insoluble, aunque es poca cosa. De hecho, el usuario podrá resolver por sí mismo este problema mediante una búsqueda en el sistema de directorio basada en uno o varios atributos que conoce. De esta manera, por ejemplo, nuestro usuario puede localizar una impresora en color que soporte la impresión por ambas caras, el grapado y situada en su misma planta.

Con este primer ejemplo, podemos ahora introducir los fundamentos del directorio Active Directory. Este directorio debe ofrecer los medios de almacenar toda la información que caracteriza a todos los objetos que pueden existir en la red de la empresa, así como disponer de servicios capaces de hacer esta información utilizable de forma global por los usuarios, en función de sus derechos y privilegios.

Por consiguiente, los servicios de dominio de Active Directory de Windows Server ofrecen las funcionalidades que se enumeran a continuación:

- La posibilidad de publicar a escala empresarial los servicios indispensables para el buen funcionamiento de ésta. Los departamentos de carácter general podrán encontrar su lugar dentro de un servicio de directorio que ofrece tales posibilidades de publicación y de selección. Por ejemplo, podría tratarse de una aplicación que se ejecuta en el puesto de trabajo para localizar el servidor de mensajería instantánea, como Microsoft Skype Empresarial, más cercano y con mayor disponibilidad. Retomando el ejemplo anterior, también podría tratarse de un puesto de trabajo que selecciona una entidad certificadora capaz de emitir un certificado basado en una plantilla específica para acceder a un sitio o una aplicación securizada de una forma concreta.
- Podrá ser necesario asumir el rol de columna vertebral para el conjunto de los servicios seguros de la red empresarial. De esta manera, los administradores podrán apoyarse en un modelo de gestión global de la seguridad, que permita garantizar de forma más sencilla un alto nivel de seguridad de acceso y un mayor grado de confidencialidad de los datos sensibles. Por ejemplo, en el caso de la distribución automática de certificados digitales para firmar un mensaje de correo electrónico o también el soporte de la autenticación de usuarios al presentar una tarjeta inteligente. Para la verificación de la huella dactilar o por ejemplo el reconocimiento del iris. También podría tratarse de distribuir las listas de control de acceso a un firewall en función de la autenticación del usuario en una conexión VPN. De esta manera, los servicios de dominio de Active Directory permiten o prohíben a un usuario remoto el acceso a ciertos recursos de red privados controlando de forma dinámica las reglas contenidas en un firewall.
- El directorio se distribuye de forma global. Esta funcionalidad permite a todos los usuarios de la red utilizar todos los servicios de seguridad, los servicios de aplicación y servicios de búsqueda de Active Directory. Por supuesto, ¡los servicios globales deben ser accesibles de forma «global»! No puede ser de otra manera, especialmente si se trata de los controles de acceso y el buen funcionamiento de aplicaciones críticas como la mensajería o los servicios de colaboración. Es evidente que estos requisitos deberán someterse a una adopción generalizada de las tecnologías indispensables para su implementación.
- El directorio debe disponer de funciones naturales que permitan la tolerancia a fallos. La replicación del directorio Active Directory en cada lugar geográfico importante le permitirá jugar su papel central. Por ejemplo, la desaparición de un controlador de dominio de un sitio geográfico determinado debe ser resuelta sin necesidad de intervención humana. Descubriremos más adelante que los servicios de dominio de Active Directory disponen de tales mecanismos a través de la capacidad de gestión de espacios denominados "sitios huérfanos".
- Los servicios de dominio de Active Directory aportan con ellos la tecnología de particiones que permite apoyarse en un espacio de almacenamiento distribuido a nivel empresarial. De esta forma, el directorio Active Directory es capaz de gestionar millones de objetos y permite a los usuarios acceder cualquiera que sea su ubicación. Este papel central dotará a los servicios de directorio de un carácter estratégico y crítico en particular que habrá que considerar siempre a futuro, a medida que evoluciona.

Posicionamiento e innovaciones en Windows Server

1. Versión mayor de Windows Server "Cloud OS"

Introducido con Windows Server 2012 R2, Cloud OS fue presentado por Satya Nadella como la base de una moderna generación de Sistemas Operativos diseñada para satisfacer las necesidades actuales y futuras. Windows Server 2016 ha sido concebido con este espíritu como una versión mayor para proporcionar a las empresas una plataforma cloud adaptada a todas las cargas y todos los escenarios en los ámbitos de la virtualización, soporte de aplicaciones con un nivel de disponibilidad y seguridad muy alto. Los mayores cambios y avances se refieren a los servicios de virtualización con una nueva versión del hipervisor Hyper-V aún mejor y más fácil de gestionar, desde un simple servidor de grupo de trabajo a los mayores centros de datos. A día de hoy, Hyper-V soporta 320 procesadores lógicos, 1024 VM 2048 procesadores virtuales, 4 TB de RAM por máquina host Hyper-V, 64 nodos Hyper-V por clúster, y 8000 VM ejecutadas de forma simultánea en un clúster con una capacidad de almacenamiento y red solo limitado por el hardware empleado.

Del lado de virtualización y cloud, Windows Server 2016 introduce:

- Nano Server, un kernel optimizado para Hyper-V, los servicios de archivos SOFS, servicios Web y Containers Windows.
- Los Containers Windows e Hyper-V, para minimizar el número de VM y minimizar las operaciones de mantenimiento ofreciendo un inicio casi instantáneo.
- El soporte nativo de ReFS que permite a Hyper-V realizar operaciones pesadas sobre archivos de discos virtuales VHDX de forma casi instantánea.
- Soporte para la virtualización dentro de la virtualización - en inglés Nested Virtualization.
- Los nuevos archivos VHDS, soportan a los archivos VHDX compartidos con las funcionalidades de copia de seguridad en caliente, y dimensionamiento dinámico para su adición y eliminación.
- La protección de los recursos Hyper-V, para limitar de forma automática el consumo anormal de recursos con el fin de proteger los recursos globales del equipo host Hyper-V.
- Virtual TPM, para añadir a las máquinas virtuales un chip virtual TPM utilizable por BitLocker con el fin de encriptar los discos de las máquinas virtuales.
- El arranque seguro Linux, para securizar el arranque de las máquinas virtuales -Linux; Windows Server 2016 permite ahora ofrecer esta funcionalidad. Introducido inicialmente para las máquinas virtuales Gen 2 de Windows 2012 y Windows 8 y versiones posteriores de Windows Server 2012 R2 en las máquinas virtuales Linux.
- Las máquinas virtuales blindadas, para proteger la ejecución de máquinas virtuales dentro de fábricas designadas como poseedores de estas máquinas virtuales. Las máquinas virtuales de tipo Shielded (en castellano: blindadas), soportan el uso de un chip TPM y requieren el uso del nuevo rol Host Guardian Service.
- El soporte de los clústers Hyper-V repartidos con Storage Replica para replicar el almacenamiento CSV de las máquinas virtuales dentro de un clúster o incluso entre diferentes clústers. Por supuesto, la funcionalidad Storage Replica de Windows Server 2016 puede también usarse para simples servidores de archivos.
- Almacenamiento resiliente de máquinas virtuales: en Windows Server 2016, una fallo mayor de almacenamiento no significa que las máquinas virtuales presentarán a su vez fallos, ya que éstas se mueven de forma automática en modo hibernado y se restauran cuando los problemas relacionados con el sistema de almacenamiento estén resueltos. Con Windows Server 2012 R2, cuando una máquina virtual pierde su acceso al sistema de almacenamiento durante un período superior a 60 segundos, se considera que la máquina virtual tiene un fallo.

La lista de nuevas funcionalidades incluidas en Windows Server 2016 es larga pero, entre las más interesantes, también podemos observar los nuevos puntos de control de producción (snapshots con soporte VPP dentro de las VM), añadir o suprimir en caliente discos compartidos VHDX para las VM en clúster, adición y eliminación en caliente de la memoria sin que sea necesario utilizar la funcionalidad de gestión de memoria dinámica Hyper-V, la adición y supresión en caliente de tarjetas de red virtuales, la identificación de las tarjetas de red virtuales dentro de las VM y en las VM, la actualización de los servicios de integración de Hyper-V via Windows Update, el soporte de OpenGL 4.4 con RemoteFX, más de 300 nuevos comandos Windows PowerShell para Hyper-V, servicios de clúster, Windows Defender, y mucho más.

2. Evoluciones en materia de seguridad

Windows Server 2008 R2 y Windows Server 2012 R2 han contribuido de manera importante al fortalecimiento de la seguridad mediante la protección de los accesos a redes, con los nuevos controladores de dominio en modo sólo lectura (RODC, *Read Only Domain Controller*) y las nuevas versiones de los servicios de certificados AD CS (*Active Directory Certificate Services*). Los servicios de gestión de derechos digitales AD RMS (*Active Directory Rights Management Services*), también se han mejorado y permiten una gestión de la información crítica y datos confidenciales dentro y fuera de la empresa. La presencia de las funciones de refuerzo de los servicios de Windows, el nuevo Firewall de Windows bidireccional y funciones criptográficas CNG (*Crypto Next Generation*) también son puntos esenciales. Por su parte, Windows Server 2016 proporciona un importante número de innovaciones en términos de seguridad con muchas mejoras y también la presencia de Windows Defender, el Anti-malware que viene con Windows 10.

3. Acceso a aplicaciones y movilidad

Los usuarios móviles no están desocupados, ya que ahora es posible ejecutar programas desde cualquier ubicación remota a través de RemoteApp dentro de un entorno empresarial local y también a través de las RemoteApp ofrecidas dentro del cloud Microsoft Azure. Del lado de movilidad, las tecnologías ya disponibles en Windows Server 2012 R2 como DirectAccess, los documentos de trabajo y la funcionalidad BranchCache se han mejorado. Del lado de Azure, el paquete EMS - de *Enterprise Mobility Suite*, es también muy interesante tanto en términos de servicios ofrecidos (Microsoft Azure AD Premium, Microsoft Intune, Azure Rights Management, Microsoft Advanced Threat Analytics) como de licencias, especialmente en relación a las licencias tradicionales On-Premise.

Para saber más sobre EMS, busque Microsoft Enterprise Mobility en el sitio de Microsoft.

4. Evoluciones aportadas por Windows Server 2008 R2, Windows Server 2012 R2 y Windows Server 2016

Tras el paso de Windows NT a Windows 2000, y luego a Windows Server 2003, Windows Server 2008 R2 es en verdad el punto de partida de una nueva generación de Windows Server. Esta versión de Windows Server 2008 R2 introdujo funcionalidades, las cuales, en su mayoría fueron mejoradas de forma considerable con Windows Server 2012 R2.

La lista de funcionalidades siguiente resume el conjunto de evoluciones aportadas por Windows Server 2008 R2 Windows Server 2012 R2 y también Windows Server 2016:

- Firewall con funcionalidades avanzadas de seguridad
- Administrador de servidor
- Modo de instalación en Server Core
- Servicios de certificados de Active Directory (ADCS)
- AD CS: Enterprise PKI (PKIView)

- AD CS: Servicio de inscripción de dispositivo de red
- AD CS: Servicio web de directiva de inscripción de certificados
- AD CS: Servicio web de inscripción de certificados
- AD CS: Respondedor en línea
- Cryptography Next Generation
- AD DS: Servicios AD DS (Active Directory Domain Services)
- AD DS: Auditoría
- AD DS: Directivas de contraseñas granulares
- AD DS: Controladores de dominio en solo lectura
- AD DS: Reinicio en caliente de los servicios AD DS
- AD FS: Servicios de federación de Active Directory
- AD LDS: Active Directory Lightweight Directory Services
- AD RMS: Active Directory Rights Management Services
- Servidor de aplicaciones
- Servidor DNS
- Servicios de archivos y almacenamiento
- Copia de seguridad de Windows Server
- Servidor de NFS
- Transactional NTFS / Self-Healing NTFS
- Network Policy and Access Services Role: el rol NPS siempre presente en Windows Server 2016 no soporta el protocolo NAP - *Network Access Protection*.
- Windows Server Essentials Media Pack: este componente se puede descargar desde el sitio de Microsoft a través del enlace:https://www.microsoft.com/en-us/download/details.aspx?id=40837
- Servicios de escritorio remoto: Host de sesiones de Escritorio remoto, anfitrión de virtualización de servicios de Escritorio remoto, servicio Broker para las conexiones de Escritorio remoto, Puente de los servicios de escritorio remoto, acceso remoto a la oficina a través de Internet (acceso a los programas RemoteApp)
- Servidor Web (IIS)
- Servicios de despliegue Windows
- Cifrado de discos BitLocker
- Clustering de conmutación por error
- Equilibrio de carga de red
- Componentes de red TCP/IP Next Generation

a. Innovaciones introducidas en Active Directory

Como ocurre desde la primera versión de Active Directory incluida con Windows 2000 Server, los servicios de directorio Active Directory tienen como función principal gestionar los objetos usuarios/grupos de usuarios, recursos de tipo equipos o impresoras, aplicaciones como Microsoft Exchange Server o aplicaciones de terceros, y garantizar el acceso a la totalidad de estos recursos a través de los servicios de autenticación modernos y seguros basados en los protocolos estándar del mercado como LDAP, NTLM y Kerberos v5.

Los servicios de Active Directory de Windows Server 2016 mejoran las funcionalidades de Windows Server 2012 R2, las cuales, en su mayoría fueron introducidas con Windows Server 2008 R2. Cabe señalar que los servicios de directorio Active Directory han pasado a denominarse Servicios de dominio de Active Directory (en inglés AD DS de *Active Directory domain Services*) a partir de Windows Server 2008 R2. Esta introducción a los servicios de dominio de Active Directory presenta las mejoras más notables.

b. AD DS: Auditoría

Los controladores de dominio Windows Server 2008 R2 y posteriores soportan nuevas subcategorías (*Directory Service Changes*) para registrar los antiguos valores y también los nuevos valores de atributos en las operaciones de cambio de atributos sobre los objetos de Active Directory. Un nuevo parámetro, para definir la directiva de los controladores de dominio *Audit Directory Service Access*, permite activar o desactivar esta nueva funcionalidad. Por supuesto, ésta es muy interesante para todos aquellos que deseen vigilar las operaciones realizadas sobre los objetos. Tenga en cuenta que la administración de los atributos a auditar siempre será a nivel de los objetos, permitiendo así una granularidad precisa de configuración. Los nuevos servicios de auditoría permiten registrar los valores de atributos durante los cambios.

Las versiones anteriores de Windows Server tenían la posibilidad de registrar los eventos de modificación de los atributos, pero no permitían registrar ni los valores anteriores ni los nuevos. Observe también que las nuevas funciones de auditoría de los servicios de dominio de Active Directory se aplicarán de la misma manera sobre los servicios AD LDS (*Active Directory Lightweight Directory Services*).

c. AD DS: Gestión granular de directivas de contraseña

Con los dominios Windows 2000 y Windows Server 2003, una única directiva de contraseñas y bloqueo de cuentas podía aplicarse a todos los usuarios de un dominio. Los servicios de dominio de Active Directory de Windows Server 2008 R2 y posteriores, permiten definir diferentes directivas de contraseñas, tanto en términos de complejidad como en términos de bloqueo de cuentas.

Esta nueva funcionalidad será de interés para muchos administradores que deseen imponer políticas de contraseñas más seguras para usuarios o grupos de usuarios especialmente sensibles. Ahora se pueden crear múltiples directivas de contraseña dentro del mismo dominio y aplicarlas en diferentes conjuntos de usuarios. Estas nuevas directivas de cuentas se aplican solo a los objetos usuarios, de la clase`inetOrgPerson` y también a los grupos globales de seguridad.

d. AD DS: Controladores de dominio en solo lectura

Los controladores de dominio se encuentran por definición disponibles en lectura y escritura. Cuando las limitaciones de la arquitectura de la red lo exijan, puede ser necesario colocar en un sitio remoto un controlador de dominio para autenticar usuarios y ofrecer los servicios de infraestructura habituales. El problema es que con mucha frecuencia los sitios remotos no disponen del nivel de seguridad necesario para mantener dentro de un local seguro servidores de infraestructura tales como controladores de dominio disponibles en escritura.

Para paliar esta problemática, Windows Server 2008 R2 introdujo un nuevo tipo de controlador de dominio llamado controlador de dominio en modo sólo lectura o RODC (*Read-Only Domain Controller*). Esta solución permite desplegar controladores de dominio en ubicaciones donde

un nivel de seguridad adecuado no se puede garantizar. Además de forzar la base de datos Active Directory en modo sólo lectura, los RODC introducen también otras mejoras, como la replicación unidireccional, la puesta en cache de datos de identificación, así como la posibilidad de especificar qué contraseñas se replican en la base de datos Active Directory, la separación de funciones, así como la asunción de la problemática de las inscripciones DNS dinámicas en las zonas DNS integradas en las bases de datos Active Directory disponibles en modo sólo lectura.

e. AD DS: Reinicio de los servicios de dominio Active Directory

La posibilidad de reiniciar los servicios de dominio de Active Directory en caliente sin el reinicio del servidor ofrece gran flexibilidad durante las actualizaciones de Windows o por ejemplo durante una operación de desfragmentación de la base de datos Active Directory. Cabe señalar, sin embargo, que debemos tener en cuenta las dependencias relacionadas con las aplicaciones.

f. AD DS: Ayuda a la recuperación de datos

Antes de la utilización de los controladores de dominio Windows Server 2008 R2, cuando los objetos eran borrados de forma accidental, la única manera de determinar qué objetos se habían borrado era restablecer la totalidad de la base de datos Active Directory.

Aunque la funcionalidad de ayuda para la recuperación de datos Active Directory no permita restaurar directamente los datos posiblemente borrados, puede ayudar en el procedimiento de recuperación de datos.

Mediante la herramienta de montaje de base de Active Directory, los datos de Active Directory registrados en las instantáneas son accesibles en modo solo lectura. De esta manera, el administrador podrá comparar los datos en diferentes puntos en el tiempo sin necesitar detener el sistema.

Por último, una nueva opción muy importante permite forzar la supresión de los servicios de Active Directory cuando el controlador de dominio erróneo es arrancado en modo Directory Services Restore Mode.

Todas estas nuevas características se detallan más adelante en el libro.

5. Integración de la innovación dentro de Windows Server

Windows Server integra un número importante de tecnologías, funcionalidades y servicios diseñados para formar una solución duradera y adaptada a las necesidades de las empresas. Uno de los mayores beneficios de esta plataforma se refiere a la integración de todos estos servicios en el centro del sistema, de la plataforma entera, y proviene de la facilidad de implementación de ésta. Windows Server fue diseñado en base a hipótesis que son el reflejo de la experiencia en las empresas. El objetivo de este enfoque es permitir un rápido despliegue de soluciones de partida complejas y al mismo tiempo más cercano a las expectativas y necesidades expresadas por los clientes.

La estrategia consiste en innovar en torno a la plataforma Windows Server. En efecto, esta plataforma tiene en realidad la vocación de explorar y abrir una serie de vías. Este punto se refiere especialmente a los proveedores de aplicaciones, los proveedores de servicios, los integradores de sistemas, y por supuesto, los desarrolladores de sistemas que puedan, sobre la base de las tecnologías presentes en Windows Server, crear soluciones interesantes. Los servicios básicos integrados en el sistema, así como las funcionalidades que Windows Server proporciona permiten a los fabricantes y socios concentrarse en el diseño de soluciones para ampliar los servicios básicos de Windows y aportar un valor añadido sustancial.

Los clientes y analistas externos han comprobado que el enfoque de Microsoft con respecto a la innovación tiene por efecto acentuar el desarrollo de aplicaciones de muy alta calidad, de favorecer la disminución del coste total de la propiedad (TCO) permitiendo una mejor productividad y eficacia en relación con las soluciones competidoras.

Servicios básicos y protocolos estándar

Los servicios de directorio Active Directory permiten la aplicación de un espacio lógico organizado de manera jerárquica, donde resulta fácil para cualquier usuario autorizado de la red localizar y utilizar cualquier tipo de información.

Todo el mundo debe por último encontrar su interés, ya que los usuarios podrán, por ejemplo, utilizar los servicios de búsqueda y localizar los recursos que necesitan, mientras que los administradores podrán, por su parte, mejorar la gestión de las cuentas de usuarios, sus privilegios, así como los recursos y permisos que están asociados.

La centralización de la información dentro de los servicios de directorio permitirá también evitar los incontables pérdidas de tiempo ocasionadas por largos "paseos" por los servidores en búsqueda de la hipotética presencia del elemento deseado.

Cualquiera que sea el sistema de directorio y el uso para el que fue concebido originalmente, es evidente que el fin que este permite es estructurar la información organizando ésta sobre la base de objetos más o menos complejos y de sus atributos respectivos, ellos mismos más o menos numerosos y específicos.

De forma por completo lógica, si el directorio está posicionado en el centro del sistema de información, entonces se convierte en un elemento de elección para servir como componente central al conjunto de los servicios de seguridad y control de acceso a los objetos soportados.

Esta elección se encuentra, por naturaleza, en el corazón de la estrategia de Microsoft. Entre los puntos más importantes, podemos ya señalar que la implementación de Kerberos V5 como método de autenticación principal y la fuerte integración de los servicios de gestión de certificados digitales X509 v3 como elementos que forman hoy parte del éxito de los servicios de Active Directory.

Así, el directorio puede ofrecer de manera genérica y segura todo tipo de datos en cualquier tipo de clientes. Los servicios del sistema operativo, aplicaciones y, en sentido amplio, cualquier entidad de seguridad habilitada que ostente los derechos suficientes podrá acceder.

Otro punto positivo generado por los servicios de seguridad integrados en el sistema de directorio es permitir la implementación de una autenticación única disponible en toda la escala de la empresa. Esta característica no hizo su aparición con los servicios de dominio de Active Directory. Partiendo con Windows NT (e incluso antes en menor medida con LAN Manager), la apertura de sesiones de dominio a través del protocolo NTLM v1 o v2 ha sido utilizada de forma amplia por aplicaciones Windows de terceros. El tiempo ha transucrrido, y Windows Server 2012 R2 y Windows Server 2016 extienden estos conceptos basándose en las tecnologías más exhaustivas y probadas de la industria.

La siguiente tabla resume los puntos clave que caracterizan a Active Directory.

Funcionalidades Active Directory	Beneficios para la empresa
Sistema de almacenamiento distribuido.	Almacenamiento de datos de directorio unificado que requieren pocas tareas administrativas.
Extensibilidad del Directorio.	Integración de aplicaciones de terceros con extensión del esquema de Active Directory.
Administración centralizada y delegación.	Control de los privilegios de administración y los parámetros de seguridad de modo jerárquico a escala empresarial.
Disponibilidad de información del directorio, tolerancia a fallos, alto rendimiento.	El directorio puede actualizarse a partir de cualquier controlador de dominio, cuando un controlador de dominio esté disponible. La disponibilidad y la gestión de los flujos de replicación están controlados mediante el ajuste dinámico de la topología de replicación y empleando el modo de replicación multi-maestro. La estructura de bosque de Active Directory -árboles, dominios y controladores de dominio- soporta estructuras con millares de emplazamientos geográficos y millones de objetos.
Gestión de configuraciones y cambios en la configuración empleando la tecnología IntelliMirror.	Coherencia de los parámetros aplicados y operaciones realizadas mediante objetos de directiva de grupo, en inglés GPO (*Group Policy Object*).
Servicios de seguridad para las empresas de todos los tamaños a través del soporte de Kerberos V5, SSL (*Secure Socket Layer*) 3.0, TLS (*Transport Layer Security*) y los servicios de clave pública (PKI, *Public Key Infrastructure* y certificados X509 V3).	Los servicios de autenticación y control de acceso garantizan un soporte dentro de la red privada y también en Internet.
Gestión de la seguridad y delegación de la gestión de la administración.	La granularidad desciende hasta el atributo y el alcance de gestión se ejerce sobre los objetos de tipo Sitio, Dominio y UO.
Soporte de los estándares de Internet: un dominio Windows es un dominio DNS (*Domain Name System*), un dominio de autenticación es un reino Kerberos, los certificados son utilizables para la autenticación (inicio de sesión por tarjetas inteligentes Smart Logon) y la seguridad de la información (firmas digitales y cifrado de datos locales y a través de la red).	La empresa ve garantizada la continuidad de sus opciones a través de la participación activa de Microsoft con los estándares de la industria. TCP/IP v4 y v6, DNS, DDNS (*Dynamic DNS*), IPSec, DHCP (*Dynamic Host Configuration Protocol*), Kerb5, Radius (*Remote Authentication dial-in User Service*), EAP (*Extensible Authentication Protocol*), PEAP (*Protected EAP*), LDAP (*Lightweight Directory Access Protocol*), LT2P (*Layer 2 Tunneling Protocol*), PPTP (*Point to Point Tunneling Protocol*), SSL3, TLS, Infraestructura de clave pública (PKI), certificados X509 V3, autenticación por tarjetas inteligentes y autenticación biométrica.

Introducción a los servicios de resolución de nombres DNS

Este capítulo introduce los mecanismos de resolución y gestión de nombres con el sistema DNS, *Domain Name System*.

Los objetivos son importantes porque nos permitirán:

- comprender los principios de la resolución de nombres DNS;
- comprender y configurar las zonas DNS;
- comprender la replicación y la transferencia de las zonas DNS;
- comprender la problemática de integración de los servidores DNS de Windows dentro de una infraestructura DNS existente y gestionar los problemas de interoperabilidad.

El siguiente paso consistirá en estudiar las características propias del servicio DNS de Windows Server al emplear la integración de Active Directory cuando un dominio DNS ofrece sus servicios para garantizar un funcionamiento normal del directorio Active Directory.

1. Un poco de historia

Cada equipo que pertenece a una red TCP/IP debe poseer una dirección IP (*Internet Protocol*) que será utilizada en el contexto de las comunicaciones con los demás equipos. Los servicios TCP/IP, aparte de las funciones inherentes a los protocolos de transporte y enrutamiento entre las redes, fueron concebidos para soportar aplicaciones distribuidas en escala de redes cuyo tamaño puede alcanzar el de Internet.

Aunque hoy se plantean grandes cuestiones en torno a las arquitecturas de tipo cloud híbrido y otras plataformas de virtualización hiperconvergentes, sabemos que el protocolo TCP/IP forma parte de nuestras bases. Para convencernos, basta observar el inmenso éxito de los equipos Windows en las empresas, pero también de manera más amplia en nuestras vidas con los teléfonos móviles, las tabletas y los nuevos dispositivos que introducen nuevos factores de forma, como por ejemplo, los portátiles híbridos tales como Microsoft Surface Book.

Todas estos equipos son por supuesto capaces de manipular con las direcciones IP. Por contra, es evidente que no es lo mismo para los usuarios que los utilizamos.

Al principio, y mucho antes de la Internet que conocemos hoy en día, la manipulación de las direcciones IP era fuente de muchos problemas dentro de la red ARPANET (*Advanced Research Project Agency Network*). En esa época, el NIC (*Network Information Center*) - no confundir con el InterNic -tenía la responsabilidad de actualizar el archivo HOSTS.TXT. Los usuarios de la red ARPANET debían a continuación, para ser capaces de resolver los nombres de los equipos a direcciones IP, disponer de la lista más actualizada posible descargando esta mediante el protocolo FTP (*File Transfer Protocol*).

El InterNic, mencionado anteriormente, tiene como objetivo proporcionar al público la información relativa a los proveedores de servicios de registro de nombres de dominio DNS en Internet. Podemos a través del sitio http://www.internic.net acceder a la lista de los organismos autorizados a nivel mundial para registrar los nombres de dominio DNS, transmitir cualquier comentario sobre posibles problemas de registro de nombres de dominio y acceder a información sobre las operaciones DNS notables que puedan tener lugar en el nivel de Internet.

Las tareas de coordinación necesarias para el correcto funcionamiento de Internet comprenden de forma principal la gestión de las direcciones IP y de los nombres de dominio DNS. Hasta 1998, eran el gobierno americano y algunos de sus organismos (Investigación y Departamento de defensa - DoD) quienes garantizaban las tareas de coordinación de Internet. La asignación de los bloques de direcciones IP se encontraba bajo la responsabilidad global de IANA (*Internet Assigned Numbers Authority*), que se encontraba subcontratada por el gobierno americano.

En referencia a la gestión de los nombres de dominio de primer nivel como .net, .gov, o .com (se habla de gTLDs de "*generic Top Level Domains*"), es la empresa Network Solutions, Inc. la que tenía el monopolio.

En 1998, la ICANN (*Internet Corporation for Assigned Names and Numbers*) se creó para coordinar la asignación de estos recursos a nivel mundial, la gestión real de los dominios DNS se delega en los instancias regionales situadas en cada continente.

Para la gestión de los nombres de dominio, podemos consultar en la dirección siguiente la lista de las instancias responsables de la gestión de los nombres de dominio dentro de cada país: http://www.iana.org/domains/root.

Por ejemplo, la zona DNS .es se encuentra gestionada por dominios.es, http://www.nic.es o http://www.dominios.es.

Para más detalles, podemos visitar los sitios de ICANN en las direcciones siguientes: https://www.icann.org/ y https://whois.icann.org/en.

La solución: ¡Gracias Dr Mockapetris!

Tras esta primera implementación de un sistema de nombres y de resolución de nombres de equipos a direcciones IP, era evidente que debía implementarse una solución más "moderna".

En 1983 el Dr. Paul V. Mockapetris -Diplomado en el reconocido MIT (*Massachussets Institute of Technology*)- propondrá los fundamentos de los servicios DNS a través de las RFC 882 y 883.

Las RFC 882 y 883 están hoy obsoletas y han sido sustituidas por las RFC 1034 y 1035, las cuales son a su vez escritas por el Dr. Paul Mockapetris. La RFC 1034 sigue siendo actual aunque objeto de actualizaciones contenidas en las RFC 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308 y 253. La RFC 1035 es también corriente aunque objeto de actualizaciones contenidas en las RFC 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425 y 3658. Podemos buscar y consultar estas RFC en el sitio:http://www.rfc-editor.org y a través de la URL https://www.rfc-editor.org/retrieve/.

2. ¿Qué son los servicios DNS?

Como se explicó antes, DNS es el protocolo estándar de resolución de nombres definido por la IETF (*Internet Engineering Task Force*). Permite a los equipos cliente registrarse y resolver los nombres de equipos pertenecientes a dominios DNS. Una vez resuelto el nombre del equipo destino, es posible acceder al equipo al igual que a sus recursos.

DNS está, por definición, constituido por tres componentes principales:

1. El espacio de nombres de dominio (*Domain Namespace*): comprende los registros de los recursos asociados a este espacio. Los registros de recursos se llaman RR de *Resources Records* y clarifican el tipo de cada registro.

2. Los servidores de nombres DNS (*DNS Name Servers*): se trata de equipos en los que se ejecuta el proceso que ofrece el servicio "Servidor DNS". Estos servidores hospedan todo o parte del espacio de nombres gestionado al igual que los registros de recursos. Garantizan de esta forma el correcto funcionamiento de las resoluciones de nombres completamente cualificados FQDN (*Fully Qualified Domain Name*) iniciados por los clientes DNS.

3. Los clientes DNS (*DNS Resolvers* o DNR): se trata de equipos que invocan uno o más servidores DNS. Estos equipos deben disponer de un cliente que les permita solicitar uno o varios servidores DNS

Los conceptos de resolución de nombre DNS nos llevarán a tratar los siguientes puntos:

- la resolución de los nombres,
- las solicitudes de resolución directas e inversas,
- los mecanismos de caché del lado del servidor DNS y del lado del cliente DNS.

Lo que vamos a descubrir:

- El servicio DNS se basa en la solicitud de resoluciones (en inglés *Lookup Queries*).
- Los servidores de nombres DNS ayudan a resolver las demandas de resolución directas e inversas.
- Las peticiones de resolución directas permiten asociar un nombre DNS a una dirección IP.
- Las peticiones de resolución inversas permiten asociar una dirección IP a un nombre DNS.
- Un servidor de nombres DNS puede resolver una petición para una zona para la que cuenta con autoridad.
- Si un servidor de nombres DNS no puede resolver la petición, puede solicitar a otro servidor DNS que le pueda asistir para resolver la petición.
- Los servidores de nombres DNS saben como poner en caché las resoluciones exitosas y que hayan fallado para reducir el tráfico de la red.
- El servicio DNS emplea un modelo cliente/servidor.

3. Terminología del sistema DNS

El protocolo DNS fue concebido para gestionar la casuística propia de las redes de equipos que funcionan bajo TCP/IP. Los siguientes puntos recuerdan algunos principios fundamentales:

- La resolución de nombres DNS es el proceso que permite resolver un nombre DNS en una dirección IP.
- Una dirección IP identifica cada nodo que debe comunicarse empleando el protocolo TCP/IP.
- Una dirección IP es un valor de 32 bits, segmentado en 4 palabras de 8 bits cada una (4 bytes) y compuesta de dos partes:
  - La parte más a la izquierda se refiere a la red y se llama **Net ID** o **dirección de red**. Ella permite identificar de forma única un segmento de red dentro de una inter-red TCP/IP mucho mayor.
  - La parte más a la derecha se refiere al equipo y se llama **Host ID** o **dirección de host**. Ella permite identificar de manera única un nodo TCP/IP dentro de una red dada.
  - Las direcciones IP, que técnicamente son valores binarios, se expresan en notación decimal y se separan por puntos.

a. El espacio de nombres DNS (Domain Namespace)

El espacio de nombres del sistema DNS se implementa bajo la forma de una jerarquía de nombres que se presentan como un árbol estructurado. El nombre de este árbol es por convenio indefinido pero será llamado **raíz** del espacio y tomará la forma de un punto. Por ejemplo, el dominio microsoft.com es real y técnicamente llamado "microsoft.com.", concluido con el carácter (.).

Puntos clave:

- El espacio puede estar compuesto por una o varias ramas.
- Cada rama puede estar compuesta por N nombres.
- Cada nombre de host está limitado a 63 caracteres.
- El nombre completo de un nodo situado en el espacio de nombres DNS se llama FQDN (*Fully Qualified Domain Name*) lo que significa "nombre de dominio totalmente cualificado".

Se recomienda respetar la RFC 1123, la cual define las convenciones de nombres:

- Utilizar los caracteres A-Z, a-z, 0-9 y el caracter "-".
- El FQDN no debe exceder 255 caracteres.

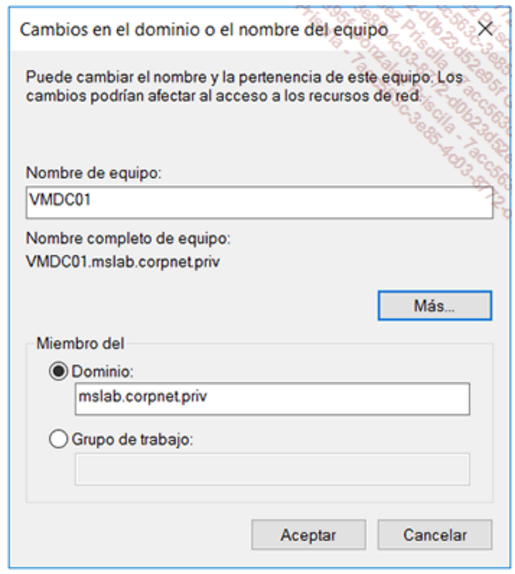
Observe: el nombre de dominio completo de los controladores de dominio no debe exceder 155 bytes. Además, algunos nombres de equipos host están reservados por el IETF. Son por ejemplo el caso de los nombres GATEWAY, GW y TAC. Para más información consulte el sitio http://Tools.ietf.org/html/rfc952.

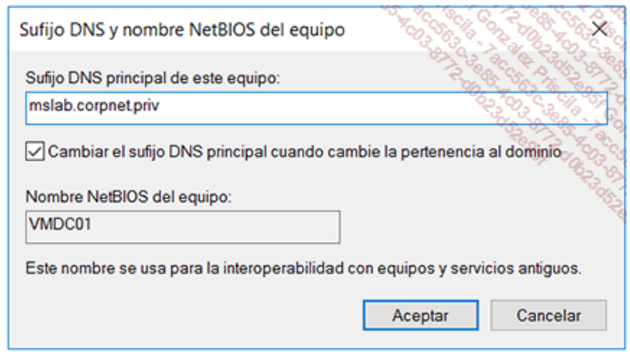
Otros puntos a tener en cuenta:

- En las plataformas Windows modernas como Windows 7 y las últimas versiones como Windows 10, el nombre del equipo está basado en el FQDN y permite de esta forma deducir el nombre NetBIOS. Está formado añadiendo al Computer Name, el sufijo DNS principal (*Primary DNS Suffix*), que por defecto es el nombre del dominio de Active Directory al que pertenece el equipo.

Sufijo de dominio primario y nombre del dominio de Active Directory: aunque esta posibilidad de cambio no sea una buena práctica, debemos tener en cuenta que el sufijo DNS principal del equipo puede ser diferente del nombre de dominio de Active Directory.

- Cabe señalar también que en las plataformas antiguas basadas en Windows NT, el nombre NetBIOS será utilizado para formar el nombre de dominio totalmente cualificado en lugar del nombre de host (hostname).





Estas pantallas muestran hasta qué punto Windows se basa en el espacio de nombres DNS. El nombre del equipo se escribe en minúsculas, a la inversa que el nombre NetBIOS, donde sólo están permitidas las letras mayúsculas.

El nombre completo del equipo también se ve de forma muy claro en la interfaz gráfica (VMDC01.mslab.corpnet.priv). También observaremos que la interfaz no muestra directamente el nombre NetBIOS. Para acceder a este, tendremos que pasar por el botón **Más...**.

Los antiguos sistemas como Windows 9x y Windows NT son en primer lugar equipos NetBIOS, que pueden a su vez apoyarse en el sistema de resolución DNS. Prestemos atención al hecho de que a partir de Windows 2000, Windows XP, Windows 7, Windows 8.1 y Windows 10 el nombre de equipo (hostname) controla el nombre NetBIOS dentro de los límites de 15 letras mayúsculas permitidas por el marco de la interfaz NetBIOS.

Con respecto a las minúsculas y mayúsculas: RFC 1034

Los nombres de dominio podrán registrarse en minúsculas, mayúsculas o con cualquier combinación de ambas. Sin embargo, la RFC 1034 especifica que, de forma independiente a la que el nombre está registrado, las operaciones no serán sensibles a las mayúsculas y minúsculas.

A propósito de NetBIOS

Espacio de nombres e interfaz de programación

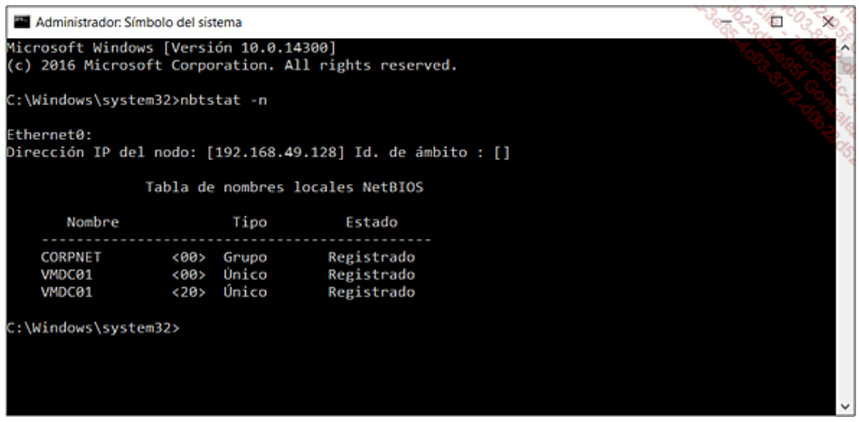
El término NetBIOS (*Network Basic Input/Output System*) puede tener varios significados. En efecto, puede tratarse de los servicios de registro de nombres en la red NetBIOS, los métodos de resolución disponibles dentro de este espacio de nombres y también de la interfaz de programación necesaria para el correcto funcionamiento de las aplicaciones NetBIOS.

Tenga en cuenta que no es posible contemplar la desactivación de la interfaz NetBIOS mientras que la red emplee aplicaciones basadas tanto en los servicios de resolución como en la interfaz de programación NetBIOS. Cabe señalar, sin embargo, que en el momento en que se escriben estas líneas, las aplicaciones NetBIOS, han por así decirlo, desaparecido.

También es posible:

- que una aplicación NetBIOS se registre en una red NetBIOS sobre el protocolo de transporte TCP/IP. Los clientes se basarán en los servicios de resolución de nombres NetBIOS tales como WINS (*Windows Internet Naming Service*) para localizar el servicio solicitado en el equipo objetivo. A posteriori, esta misma aplicación hará uso de los servicios de gestión de sesiones NetBIOS utilizando las API NetBIOS ofrecidas por el sistema operativo. Podrá también invocar otra interfaz de red, tal como las MSRPC (*Remote Procedure Call*) o bien la interfaz de Windows Sockets.
- que una aplicación NetBIOS se base en los servicios de resolución de nombres DNS. En este caso, no será posible utilizar los códigos de servicio asociados a las aplicaciones NetBIOS.

Evolución con Windows 7 o versiones posteriores, tales como Windows 10:



Sólo los códigos de <00> Servicio Estación de trabajo y <20> Servicio Servidor se encuentran en la interfaz NetBIOS.

Para simplificar, recordemos que con respecto al modelo OSI (*Open System Interconnection*), los servicios NetBIOS se sitúan:

- En el nivel 4, en lo que respecta a los servicios de transporte de datos. No hablaremos del nivel 3 en la medida en que NetBIOS no es un protocolo encaminable, pero sólo "source routable" en las redes Token-Ring IBM. Estos servicios se implementan mediante el Protocolo NetBEUI (*NetBIOS Extended User Interface*) desarrollado por IBM y Microsoft en 1985. Este protocolo de bajo nivel ofrece servicios elementales en modo conectado y modo desconectado.
- En el nivel 5, en lo que respecta a los servicios de nombres y de sesión. Estos servicios genéricos son indispensables para cualquier aplicación repartida o distribuida en la red. Encontraremos en este nivel la interfaz NetBT (*NetBIOS over TCP/IP*) que tiene por objeto permitir la correspondencia entre los nombres y servicios NetBIOS y las direcciones IP.
- En el nivel 7 del modelo en lo que respecta a las aplicaciones basadas, por ejemplo en las tuberías con nombre (*named pipes*). En este caso, se tratará de la interfaz de programación NetBIOS.

Un poco de historia...

En el tiempo Internet, NetBIOS es una tecnología obsoleta. Cabe recordar que sus servicios básicos pero fundamentales han permitido el desarrollo de miles de aplicaciones, con una gran independencia con respecto a los protocolos de transporte. En ese momento, Windows NT se basaba en este protocolo estándar para una interfaz con redes mediante los múltiples protocolos de transporte que soportaba desde la primera versión, Windows NT 3.1 en 1993. De esta forma, el tándem Windows NT/NetBIOS permitió la implementación de servidores de aplicaciones competitivos integrables con facilidad en redes que utilizan protocolos de transporte como DECnet, OSI TP4, IPX/SPX, NetBIOS y por supuesto, TCP/IP.

Y después..., de NT al Open Source, pasando por Microsoft Azure

El desarrollo de Windows NT 5.0, que se llamará poco antes de su salida Windows 2000, comenzó en 1997, un año después de la salida de Windows NT 4.0. El camino ha sido largo, pero los miles de desarrolladores del equipo NT lo consiguieron. En retrospectiva, es interesante notar que la estrategia "Internet" de Microsoft se encuentra ya muy avanzada: el sucesor de NT 4.0 se basará en IP, DNS, LDAP y Kerberos. Luego, los esfuerzos de Microsoft se centraron en los servicios web, la gestión de documentos, los servicios de colaboración, la seguridad de los sistemas, aplicaciones y del sistema de información en su conjunto.

Hoy en día, la innovación es siempre la palabra clave de la estrategia de Microsoft llevada a cabo con éxito por el CEO de Microsoft, Satya Nadella. Es el verdadero arquitecto de la estrategia de Microsoft y ahora, el futuro es otro. Con su cloud público Azure, Microsoft ofrece a las empresas una amplia gama de soluciones IaaS, *Infrastructure as a Service*, y SaaS - *Software as a Service*. Ya se trate de Office 365 para la parte ofimática, la plataforma Azure es rica en servicios para la fabricación de soluciones de cloud híbrido basadas en Microsoft AAD - *Azure Active Directory*, OMS - *Operations Management Suite* y EMS - *Enterprise Mobility Suite*. Solo nos encontramos en el inicio, pero el futuro está en marcha ya que en paralelo al desarrollo de Azure, otra mutación se opera en Microsoft con un compromiso sin precedentes en torno a las comunidades open source.

Ya se trate de Linux, de Docker, de Hadoop o de Apache Mesos -en que se basa una buena parte de la oferta Azure Container Service, esto causa mucho movimiento en Microsoft.

Para más información sobre las actividades open source de Microsoft, utilice el siguiente enlace: http://openness.microsoft.com/en-cee/blog/

b. Jerarquía DNS y espacio de nombres de Internet

Cada nodo dentro del espacio DNS tiene un nombre que le es propio. Este nombre debe siempre respetar la RFC 1035, la cual define el conjunto de principios y buenas prácticas de DNS. Tal como hemos explicado antes, el nombre, también conocido como **etiqueta**, no debe exceder de 63 caracteres, para un FQDN completo que no supere los 255 caracteres.

4. DNS: base de datos distribuida

Acabamos de ver que el sistema de nombres DNS nos permite desplegar un espacio sobre la base de una jerarquía de nombres de dominio. Ahora, podemos imaginar que con este sistema y a partir del momento en que el espacio se encuentre dividido en varios árboles y sub-árboles, resulta fácil repartir de forma técnica el espacio DNS como una base de datos distribuida.

De hecho, utilizar una base de datos distribuida significa que la información de todo el espacio DNS se almacena en N equipos, las cuales pueden estar situados en cualquier ubicación de la red.

Esto es especialmente cierto en el caso de Internet. En el caso de una red basada en un sistema de nombres privado (fuera de Internet), la información del espacio DNS tendrá la escala de esta red. Además, con los mismos principios que los que se aplican para la red Internet, y si la red privada de la empresa se compone de sitios múltiples, será por supuesto necesario prever una disponibilidad del espacio DNS en cada uno de los sitios. Volveremos sobre este importante punto cuando discutamos la relación DNS/Active Directory.

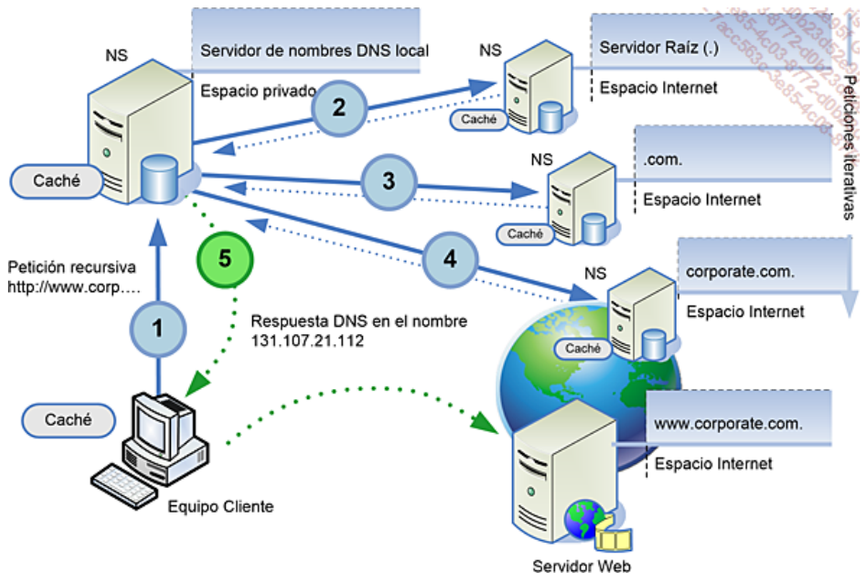
Por último, cada servidor DNS mantiene sólo una parte de la base de datos del espacio DNS. La base de datos "total" se divide en diferentes partes denominadas **zonas**, cada zona correspondiente a una parte del espacio DNS, por lo tanto, un dominio o un subdominio particular. Volveremos sobre este tema más adelante.

Los archivos de zona podrán luego ser replicados hacia múltiples servidores empleando lo que se denomina la **transferencias de zonas**. Así, podemos representar el espacio DNS de Internet de la siguiente manera:

- El dominio raíz (.) se solicita a través de los trece servidores DNS de la raíz. Estos servidores contienen la información que permiten localizar los servidores DNS de primer nivel como .com, .org, .net o .es.
- Tenga en cuenta que los servidores de la raíz no contienen toda la información de los dominios del primer nivel. Sólo conocen los servidores que tienen la responsabilidad de estos dominios.
- Bajo el mismo principio, para ser capaz de resolver el nombre de un equipo situado en el dominio microsoft.com, será necesario enviar

una petición de resolución hacia el dominio de primer nivel .com (recuerde, TLD - *Top Level Domain*), el cual no es capaz de forma directa resolver la petición, pero podrá volver a las direcciones de los servidores de nombres DNS que tienen autoridad sobre el dominio de segundo nivel microsoft.com.

El siguiente esquema muestra el proceso de resolución de nombres dentro del espacio de nombres jerárquico de Internet.



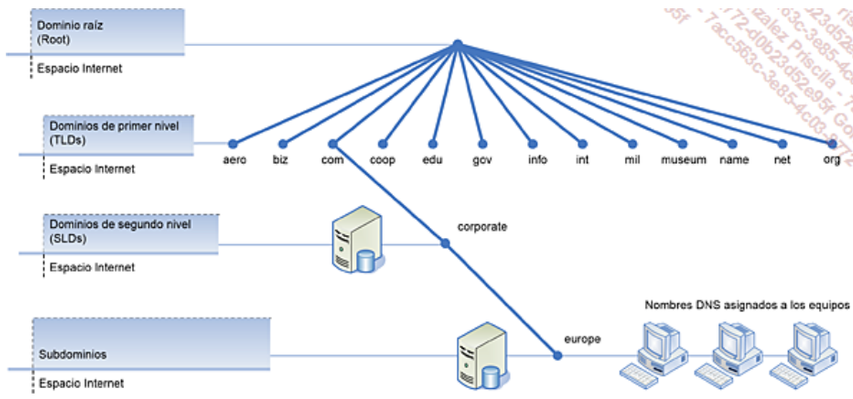
Proceso vinculado a la petición de resolución de nombres directa

Recordemos los siguientes puntos:

- Por definición, el sistema de resolución DNS ofrece un espacio de nombres jerárquico y distribuido.
- El sistema DNS tiene varias técnicas para implementar un espacio distribuido. De esta forma podemos determinar qué servidor del espacio posee la información solicitada. Los mecanismos son simples pero muy potentes. El sistema DNS es, gracias a su diseño, capaz de hacerse cargo de espacios de cualquier tamaño, como por ejemplo Internet. Se emplea de hecho con mucha frecuencia en las redes privadas empresariales.
- Los medios de los que dispone DNS para lograr un espacio de nombres distribuido son:
  - La delegación de dominios.
  - Los reenviadores condicionales o no condicionales.
  - Las indicaciones de raíz.

Estos temas serán abordados más adelante.

Estructura del espacio DNS y jerarquía de los dominios



1. El dominio raíz

Se trata del punto de vista más alto del árbol, el cual representa un nivel sin ningún nombre particular. Podemos también decir que la raíz no tiene nombre o es de tipo "no denominado". A veces se muestra en forma de dos comillas vacías (""), indicando un valor nulo. Sea como sea, cuando se utiliza como nombre de dominio DNS, se indicará mediante un punto a la derecha (.) para indicar que el nombre está situado en la raíz o nivel superior de la jerarquía del dominio. El nombre de dominio DNS se considera como completo y designará a un emplazamiento exacto del árbol de nombres.

Un servidor DNS puede gestionar el dominio raíz o no, mientras que otros servidores DNS deberán basarse en un servidor DNS que gestione el dominio raíz para poder resolver la totalidad o parte del espacio de nombres DNS.

Con los servicios DNS de Windows Server 2008 R2 y versiones posteriores, la zona raíz representada por el (.) en las zonas de búsqueda directa no es añadido de forma automática. En Windows 2000, la zona raíz (.) era añadida de forma automática durante la primera inicialización del servidor DNS, si el servidor no era capaz de ponerse en contacto con los servidores de la raíz (Root Hints). El hecho de disponer de esta zona tenía el efecto negativo de impedir el uso de los reenviadores así como los servidores de la raíz de Internet. El Administrador tendrá que crear manualmente la zona raíz (.), si es necesario.

2. Los dominios de primer y segundo nivel

Los dominios de primer nivel son también conocidos como **TLD** de *Top Level Domains*. Este primer nivel en la jerarquía DNS -ubicado por debajo de la raíz- permite estructurar el espacio de partida en función del tipo de organización utilizando un nombre o también en función de una región o de un país.

La lista siguiente describe estos dominios y sus roles.

aero	El uso de este dominio de primer nivel está reservado para la industria aeronáutica.
biz	El uso de este dominio de primer nivel está reservado a las grandes y pequeñas empresas a nivel mundial.
com	El uso de este dominio de primer nivel está reservado a las empresas de carácter comercial, tales como Microsoft, con el dominio microsoft.com. Casi todas las empresas tienen como principal función vender sus productos. De hecho, podremos constatar más adelante en este capítulo hasta qué punto la zona .com es mucho más voluminosa que todas las demás.
coop	Este dominio de primer nivel está reservado para el uso de las escuelas y universidades.
gov	El uso de este dominio de primer nivel está reservado a las agencias gubernamentales americanas. Aquí encontraremos por ejemplo, el sitio del FBI (*U.S. Federal Bureau of Investigation* - http://www.fbi.gov/) y el sitio de la NASA (*National Aeronautics and Space Administration* - http://www.nasa.gov/).
info	Este dominio no dispone de ninguna restricción en particular. Está en particular centrado en el suministro de información sobre el consumo mundial.
int	Este dominio está dedicado a las autoridades y otros organismos vinculados por tratados internacionales. Acoge, por ejemplo, el sitio de la OTAN - *North Atlantic Treaty Organisation* - http://www.nato.int).
mil	Este dominio está dedicado al ejército estadounidense. Aquí encontraremos por ejemplo el sitio de la Fuerza Aérea de los Estados Unidos (U.S. Air Force) - http://www.af.mil/.
museum	Este dominio está reservado a los museos, organizaciones y personas afiliadas.
name	Dominio global para el uso de personas individuales.
net	Este dominio está dedicado a los equipos de los proveedores de red, organismos dedicados a Internet y otros proveedores de acceso a Internet (ISPs). Aquí encontraremos al bien conocidohttp://www.internic.net/ del antiguo *Internet Network Information Center* (InterNIC).
org	Dominio de primer nivel dedicado a los grupos y organizaciones sin fines de lucro y no gubernamentales.
pro	Un dominio de primer nivel para los profesionales como médicos, abogados y contables.

La gestión de las zonas de primer nivel es muy voluminosa. Para convencernos, basta con consultar algunas estadísticas de Internet.

Los dominios de primer nivel

Los dominios de primer nivel son gestionados por organismos como Network Solutions en los Estados Unidos, o para Francia Transpac, una filial conocida de France Télécom. Por definición, el conjunto de estas autoridades llamadas **Registrars** están bajo control de ICANN.

La Internet Corporation for Assigned Names and Numbers (ICANN) es una organización de derecho privado sin fines de lucro. Su personal y sus miembros proceden del mundo entero. La función de la ICANN es fundamental ya que se encarga de asignar el espacio de direcciones del protocolo Internet (IP), asignar los identificadores de Protocolo, administrar el sistema de nombres de dominio de primer nivel (Top Level Domains) para los códigos genéricos (gTLD) y los códigos nacionales (ccTLD), y también garantizar las funciones de gestión del sistema de servidores raíz (DNS Root Servers).

Para más información sobre la gestión de los registradores realizada por la ICANN, podemos consultar la dirección http://www.icann.org/.

Los dominios de segundo nivel y sus subdominios

Los dominios de segundo nivel son nombres de longitud variable asignados a un individuo o una organización, para su uso en Internet. Estos nombres están siempre asociados a un dominio de primer nivel adecuado, según el tipo de organización o la ubicación geográfica en la que el nombre se utiliza. Puede ser, por ejemplo en el dominio de Microsoft Corporation, cuyo nombre es microsoft.com.

Los registros de recursos

Una base de datos DNS está compuesta por uno o varios archivos de zona, los cuales serán utilizados por el servidor DNS. Cada zona, representada por un archivo aparte contiene un conjunto de registros. Estos registros, que son realmente almacenados en las zonas DNS, se llaman **registros de recursos** o **RR** (de *Resource Records*).

Por último, un archivo de base de datos de zona contiene todos los registros de recursos que describen el dominio y su contenido.

Los servidores DNS que funcionan en Windows Server siguen la evolución de las RFC Internet relativas a los servicios DNS.

La siguiente tabla muestra las características de los registros de recursos utilizados con mayor frecuencia.

Tipo de registros de recursos (RR)	Descripción: Rol
Start of Authority (SOA)	Identifica al servidor designado como primario para la zona. Este registro también permite gestionar los parámetros de la zona como las transferencias de zona, el tiempo de expiración de la zona y el TTL (*Time to Live*) por defecto de los registros. Los tipos y funciones de los distintos registros de recursos del sistema DNS.
Name Server (NS)	Identifica todos los servidores designados para el dominio.
Host (A)	Identifica la dirección IP de un nombre de host específico. Este registro de dirección IP del host mapea un nombre de dominio DNS completo con una dirección IP versión 4 de 32 bits.
Pointer (PTR)	Identifica los nombres de host en relación a una determinada dirección IP. Estos registros se almacenan en la zona de búsqueda inversa.
Canonical Name (CNAME)	Identifica un nombre falso para un host en el dominio.
Mail Exchanger (MX)	Identifica los servidores de mensajería Internet. Este registro es empleado por otros servidores de mensajería para localizar los servidores de mensajería de un dominio determinado. Por último, este importante registro permite el encaminamiento de mensajes a través de Internet.
Service Locator (SRV)	Identifica un servicio ofrecido a nivel del dominio de Active Directory. El directorio de Active Directory hace un uso avanzado de este registro. Permitirá en particular a los controladores Active Directory replicar el directorio y a los clientes Windows 2000 y XP localizar los controladores de dominio.

- Los registros presentados en esta tabla se colocan en un orden lógico que no revela el lado fundamental -incluso crítico- de los registros vitales necesarios para el buen funcionamiento de Active Directory.

- La fuerte relación que existe entre Active Directory y el DNS se presentará más adelante.

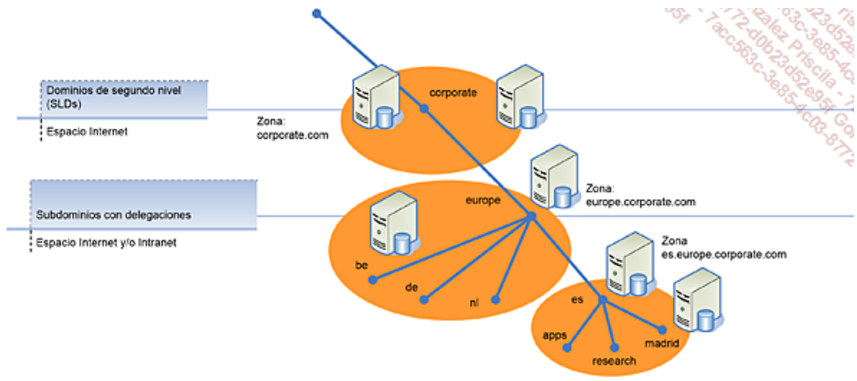
- Para más información sobre los formatos y la sintaxis de los registros de recursos soportados por los servicios DNS de Windows Server, consulte la ayuda en línea buscando "Referencia de los registros de recursos".

Dominios, zonas y servidores DNS

Para entender cómo una infraestructura DNS debe implementarse técnicamente, es importante identificar los elementos que la componen y la manera de utilizarlos. Una vez tratados estos puntos, ¡todo se aclarará!

1. Dominios DNS y zonas DNS

Como todas las tecnologías, el sistema DNS introduce sus propios conceptos y su propia terminología. En efecto, las diferencias que pueden existir entre los dominios DNS y las zonas DNS deben comprenderse bien. De esta forma, evitaremos las trampas, errores de diseño y los problemas de funcionamiento de las resoluciones dentro de nuestro espacio DNS. Un dominio DNS es una parte del espacio de nombres en el sentido lógico del término, mientras que una zona es realmente la información almacenada acerca de todo o parte del espacio de nombres. En el primer caso, se trata de un elemento de estructuración lógica, mientras que en el segundo caso, se trata de un espacio de almacenamiento físico compuesto por una parte del espacio de nombres. Por ejemplo, una empresa posee un dominio DNS llamado *privnet.corporate.com*. Para implementar este dominio lógico, tendremos que implementar de forma física el dominio, a través de un archivo de base de datos de la zona, en inglés - *database zone file*.



Dominios DNS y zonas

La figura anterior muestra los elementos siguientes:

- El dominio *corporate.com* se implementa empleando el archivo de base de datos de zona *corporate.com.dns*.
- El dominio *europe.corporate.com* se implementa empleando el archivo de base de datos de zona *europe.corporate.com.dns*.
- El dominio *europe.corporate.com* contiene los subdominios *be*, *de* y *nl* (Bélgica, Alemania y los Países Bajos).
- El dominio *es.europe.corporate.com* se implementa empleando el archivo de base de datos de zona *es.europe.corporate.com.dns*.
- El dominio *es.europe.corporate.com* contiene los subdominios *apps*, *research* y *madrid*.

De hecho, los dominios DNS y zonas DNS permiten y respetan los puntos enumerados a continuación:

- La organización del espacio de nombres DNS: tal y como aparece en la figura anterior, las zonas que albergan la información específica de un espacio contiguo de dominios.
- Dos dominios discontinuos requieren por necesidad de dos zonas.
- Los servidores DNS no replican los dominios sino las zonas, las cuales contienen uno o varios dominios y subdominios.
- La división de un espacio de dominios de gran tamaño en varias zonas permitirá evitar los grandes volúmenes de tráfico asociados a la replicación, ya que sólo las zonas DNS se replican.
- El despiece de un espacio lógico en varios trozos (por lo tanto en zonas) permite, conservando el espacio lógico, dividir una zona en varias y de esta forma distribuir la replicación.

Esta subdivisión hace posible la delegación de la gestión de las zonas en distintas entidades de administración y responsabilidades.

El hecho de implementar un espacio contiguo empleando varias zonas implica la declaración de las delegaciones que permitirán bajar a través de las resoluciones -de arriba hacia abajo en el espacio. A continuación tratamos este punto fundamental.

2. Zonas y archivos de zona

Acabamos de ver que el sistema DNS permite dividir un espacio de nombres en zonas. Estas zonas almacenan información relativa a uno o varios dominios DNS. Para cada nombre de dominio DNS de una zona, la zona se convierte en fuente de referencia (o de autoridad) de información sobre este dominio.

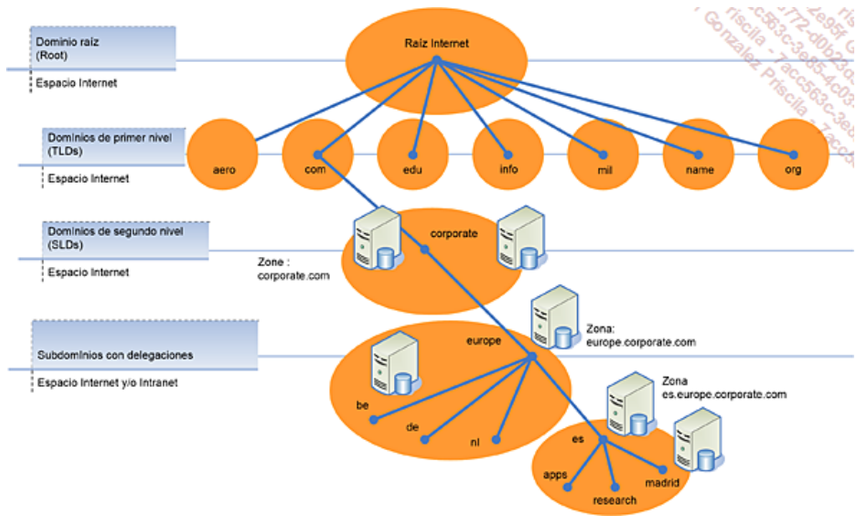
De partida, una zona es un archivo de base de datos para un solo nombre de dominio DNS. Por defecto, un archivo de base de datos de zona está situado en el directorio %system root%\System32\dns\.

Para las zonas estándar (por lo tanto, no integradas en Active Directory), el sistema de nombres por defecto de los archivos es muy práctico ya que el nombre generado será simplemente "nombre de dominio gestionado.dns".

En caso que se añadan otros dominios por debajo del dominio gestionado por la zona, será posible "incluir" el nuevo subdominio dentro de la misma zona o bien crear una nueva zona. Es conveniente decidir si un nuevo subdominio añadido a una zona se incluirá dentro de la zona original, o fuera de ésta. En este caso, veremos más adelante que la gestión de dicho subdominio se conoce como **delegada** a otra zona.

El esquema siguiente muestra la aplicación de varias zonas para el dominio de segundo nivel, *corporate.com*. De partida, el dominio*corporate.com* existe mediante la zona *corporate.com*.

La continuación del espacio de nombres requiere la aplicación de diversos subdominios. Estos subdominios podrían estar incluidos en la zona o delegados dentro de otra zona.



La configuración ilustrada muestra:

- La zona dedicada a la raíz. En los servidores DNS que funcionan bajo Windows Server, el archivo Cache.DNS se crea en el directorio %Systemroot%\system32\dns\.
- La zona dedicada al dominio de Internet de primer nivel .com.
- La zona dedicada al dominio de Internet de segundo nivel, *corporate.com*. Esta zona contiene solamente este dominio, al igual que la información de la delegación de los servidores DNS que tienen la autorización para el subdominio delegado *europe.corporate.com*.
- La zona dedicada al dominio de Internet de segundo nivel, *europe.corporate.com*. Esta zona contiene la información de este dominio, así como la información de los subdominios *be*, *de* y *nl.europe.corporate.com*. El dominio *europe.corporate.com* contiene también una delegación de los servidores DNS que tienen la autorización para el subdominio *es.europe.corporate.com*.
- La zona dedicada al dominio de Internet *es.europe.corporate.com*. Esta zona contiene la información de este dominio, así como la información de los subdominios *apps*, *research* y *madrid.es.europe.corporate.com*.

Recordemos los siguientes puntos:

- Cuando un servidor DNS desempeña el rol de servidor raíz, es decir, que administra la zona (.) a través del archivo de base de datos de la zona Root.dns, no puede ni solicitar ayuda a los reenviadores, ni hacer llamadas a los servidores raíz.
- La creación de un nuevo dominio de segundo nivel requiere la creación de un nuevo archivo de base de datos de zona.
- Si un subdominio de la zona *europe.corporate.com* no es delegado, todos los datos del subdominio se conservan en la zona e*urope.corporate.com*.
- En el sistema DNS, se denomina **dominio** a cualquier árbol o subárbol que se encuentren en el espacio de nombres de dominio.

Existen dos tipos de zonas:

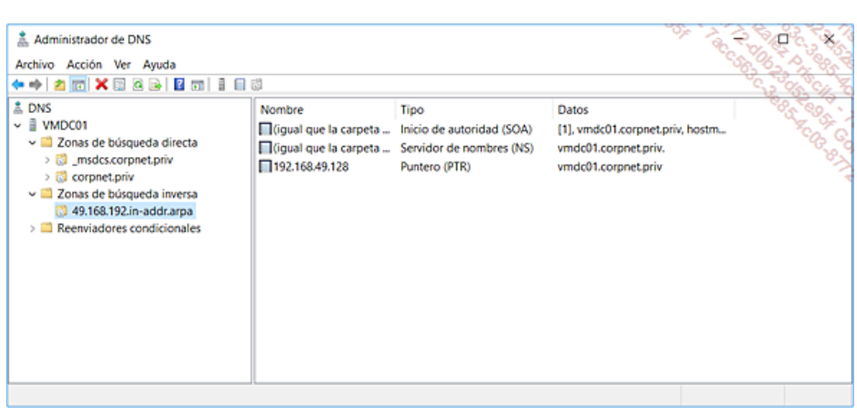
Las zonas de búsqueda directa: una zona de búsqueda directa se emplea para resolver nombres de hosts en direcciones IP. Este será el caso, cada vez que un cliente DNS interrogue al servidor DNS para localizar la dirección IP de un equipo en la red. Dentro de las zonas, los registros de recursos de tipo A ofrecen esta funcionalidad. La zona de búsqueda directa también incluye los registros de recursos de tipo SOA y NS indispensables para el buen funcionamiento de la zona. De forma adicional, encontraremos también los registros necesarios para el buen funcionamiento de determinados servicios, CNAME para los alias, MX para los conectores SMTP de los servidores de correo electrónico, SRV para los registros de servicios de Active Directory o cualquier otra aplicación.

Las zonas de búsqueda inversa: este tipo de zona permite resolver no un equipo en su dirección IP, sino una dirección IP en su equipo. La solicitud de resolución (o petición) es inversa. Dicha solicitud de resolución solo podrá ejecutarse cuando se conoce la dirección IP, pero no el nombre. Como todas las zonas, esta zona dispone de los registros de tipo SOA y NS necesarios. Por contra, no contendrá ningún registro de tipo A, pero su equivalente inverso. Estos registros llamados **registros de tipo PTR** (puntero), permiten apuntar de una u otra dirección IP a uno u otro nombre DNS completo.

Las zonas de búsqueda inversa se denominan de manera especial. De hecho, el nombre de la zona debe estar relacionado con las direcciones IP solicitadas para su resolución. Por lo tanto, el nombre de la zona deberá hacer constar el número de red o de subred IP. Para su implementación en Internet, y también en redes privadas, el nombre de dominio deberá por necesidad comenzar por *in-addr.arpa*. Se trata de un nombre reservado en concreto en el espacio DNS para especificar que la petición se refiere a una zona de búsqueda inversa y no a una zona de búsqueda directa.

Luego, el nombre de la zona se completará con la dirección de la red, pero a la inversa. Así, para las direcciones IP referentes a la red 192.168.1.0, será necesario declarar una zona de búsqueda inversa cuyo nombre deberá ser 1.168.192.in-addr.arpa.

La consola de gestión MMC (*Microsoft Management Console*) del servicio DNS es muy intuitiva. Aquí encontraremos todas las funciones básicas de un servicio DNS.



Zonas de búsqueda directa, inversa, indicaciones de raíz y reenviadores

Archivos de configuración de un servidor DNS

Los siguientes archivos permiten implementar la configuración de los servidores DNS.

El archivo de arranque: este archivo se llama **Archivo de configuración de -arranque BIND** y no se crea por defecto en la consola de gestión

del servicio DNS. Sin embargo, como opción de configuración del servicio de servidor DNS, puede copiarse a partir de otro servidor que ejecute una implementación de DNS de tipo BIND (*Berkeley Internet Name Domain*).

En Windows, el soporte de este archivo no reviste ningún interés para el funcionamiento normal del servicio de servidor DNS. Será útil funcionar en este modo sólo durante la fase de migración de una configuración DNS procedente de un sistema DNS BIND.

El archivo cache.dns: este archivo se llama **archivo cache**. Permite, al iniciar el servicio Servidor DNS, la carga previa de los registros de recursos en la caché del servidor DNS. Los servidores DNS utilizan este archivo para localizar los servidores raíz presentes en su red o directamente en Internet. Tenga en cuenta que, por defecto, este archivo contiene los registros de recursos DNS que proporcionan el caché local del servidor con las direcciones de los servidores raíz presentes en Internet.

Para los servidores DNS que funcionan exclusivamente en nuestra red interna, la consola DNS puede transferir y por lo tanto sustituir el contenido de este archivo por los servidores raíz internos de la red. Esta operación será posible siempre que sean accesibles a través de la red cuando instalamos y estamos configurando nuevos servidores DNS. Su actualización puede realizarse mediante la consola DNS, desde la pestaña **Sugerencias de raíz** situada en las propiedades del servidor específico.

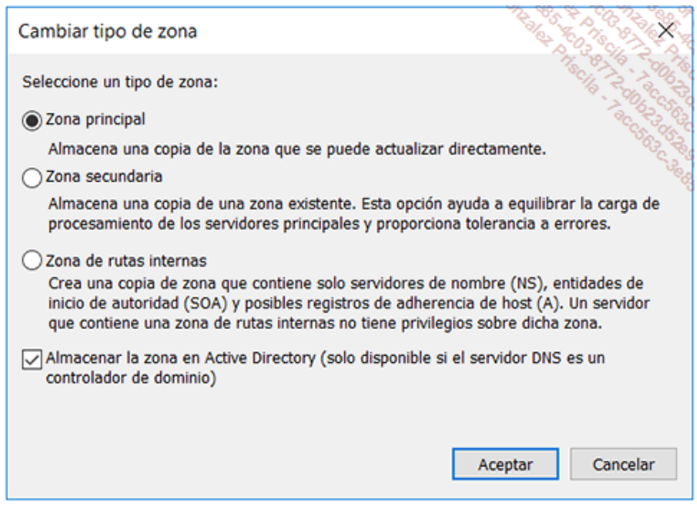
Acceso al dominio raíz (.) empleando el archivo **cache.dns** y resolución: si consideramos el caso de la red Internet, se conoce que el nombre de resoluciones en los servidores raíz es importante. Sin embargo, este punto puede ser relativo porque los nombres de host no son por lo general resueltos en este nivel. El papel fundamental del archivo de direcciones de servidores raíz **cache.DNS** es solo permitir la redirección de las resoluciones de nombres a otros servidores de referencia para los dominios y subdominios situados bajo la raíz.

El archivo de la zona raíz Root.dns: este archivo se encuentra en un servidor DNS cuando éste se encuentra configurado como servidor raíz de la red. Se trata de un archivo de zona clásica. Está particularidad estriba en el hecho de que gestiona la zona (.), que se encuentra en los más alto del espacio de nombres DNS.

Los archivos de zona nombre_zona.dns: cada zona estándar establecida requerirá su propio archivo de zona con independencia del tipo de zona (principal o secundaria). Estos ficheros se ubican en la carpeta System32\dns del servidor. Por supuesto, los archivos de este tipo no son creados ni utilizados por las zonas principales integradas en Active Directory, las cuales se almacenan en la base de datos Active Directory.

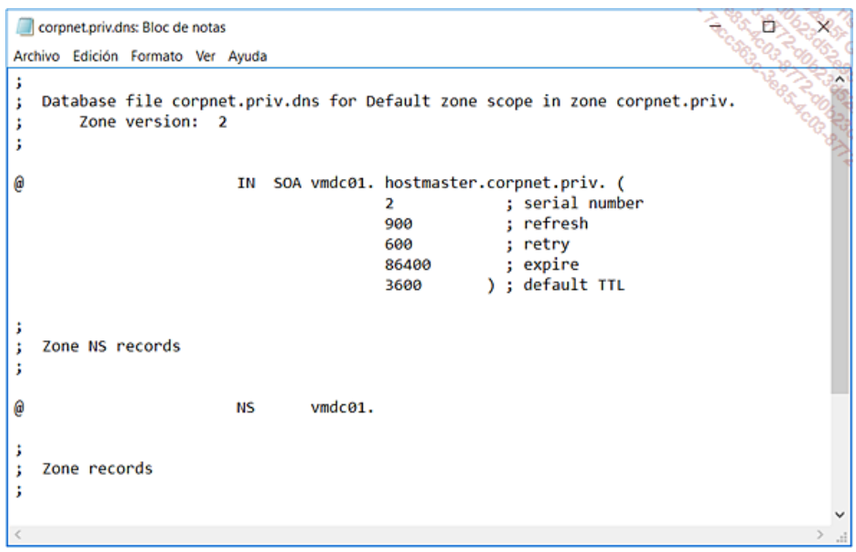
El hecho de que el archivo de zona se encuentre en el directorio system32\dns quiere decir que no puede tratarse de una zona integrada en Active Directory. A la inversa, una zona integrada en el directorio Active Directory no se encontrará visible en forma de un archivo en el directorio system32\dns.

La consola MMC de gestión DNS ofrece la posibilidad de cambiar a placer el tipo de zona. Así, cuando una zona DNS integrada en Active Directory se convierte en una zona primaria estándar, la información necesaria se extrae del directorio e integra en un nuevo archivo de zona. La operación inversa tendrá como consecuencia la integración en Active Directory de todos los registros de recursos contenidos en el archivo de zona y la eliminación de este último del directorio system32\dns.



Estructura de un archivo de zona

A continuación presentamos el detalle de la base de datos de zona para la zona *corpnet.priv*.



La estructura de un archivo de zona se explica a continuación con los diferentes tipos de registros necesarios.

La línea *@ IN SOA vmdc01.corpnet.PRIV. hostmaster.corpnet.priv* seguida de los diferentes periodos permite fijar el comportamiento de la zona en términos de replicación. El carácter @ permite apuntar al "dominio actual" sabiendo que el dominio o la zona en cuestión se especifica a su vez en el comentario en la parte superior del archivo.

El registro de recurso SOA (*Start Of Authority*) sigue siendo el primer registro declarado en una zona estándar. Se permite especificar el servidor DNS original o que actualmente desempeña el papel de servidor principal para la zona.

Este registro de recurso también se utiliza para almacenar las propiedades mas importantes, como la información de versión (en inglés, el Serial Number) y los plazos que afectan a la renovación o la expiración de los registros de propiedad de la zona y también de la zona misma. Estas propiedades afectarán la periodicidad de las transferencias entre los servidores que actúan como servidores de nombres de la zona.

Los servidores de nombres de una zona se conocen a su vez como **servidores de referencia de la zona**.

El registro de recurso SOA contiene los siguientes datos:

- **Servidor principal (propietario)**: este campo proporciona el nombre de host del servidor DNS principal de la zona.
- **Responsable**: este campo se refiere a la dirección de correo electrónico del responsable de la administración de la zona. Tenga en cuenta que en esta dirección de correo electrónico, un punto (.) se utiliza en lugar del signo (@).
- **El número de serie**: este campo es el número de versión o revisión del archivo de zona. Este valor aumenta de forma automática en 1 cada vez que se modifica un registro de recurso de la zona. Es indispensable que este valor cambie para que la replicación de las modificaciones parciales o totales de la zona puedan tener lugar.
- **Intervalo de actualización**: este campo define el plazo (en segundos) que un servidor DNS secundario deberá respetar antes de consultar a su fuente de zona para tratar de renovar la zona. Cuando el plazo de actualización expira, el servidor DNS secundario pide a su fuente una copia del registro SOA corriente para la zona. El servidor DNS secundario compara entonces el número de serie del registro SOA actual del servidor fuente (como se indica en la respuesta) con su propio registro SOA local. Si ambos valores son diferentes, entonces el servidor DNS secundario solicita una transferencia de zona para el servidor DNS principal. Observe que el valor por defecto es de 900 segundos, o sea 15 minutos.
- **intervalo de reintento**: este campo se refiere al plazo (en segundos) que un servidor secundario deberá respetar antes de retenter una transferencia de zona después de un fallo. Este valor es generalmente más corto que el intervalo de actualización. Observe que el valor por defecto es de 600 segundos, o sea 10 minutos.
- **Intervalo de expiración**: este campo es en especial importante ya que designará el plazo (en segundos) que precede a la expiración de la zona de un servidor secundario y que sigue un intervalo de actualización durante el cual la zona no se ha actualizado. El paso de la zona al estado "expirado" ocurre porque los datos locales no se consideran fiables. El servidor DNS, se encuentra entonces en estado no operativo para la zona. El valor por defecto es de 86.400 segundos, o sea 24 horas.
- **Duración de vida (TTL, *Time-To-Live*) mínima por defecto**: este campo se refiere a la duración de vida por defecto de la zona y el valor del intervalo de caché de las respuestas DNS. El valor por defecto es de 3600 segundos, o sea 1 hora.

Si el valor TTL individual es atribuido y aplicado en un registro de recurso específico utilizado en la zona, anula y sustituye el TTL mínimo a nivel del registro SOA.

El registro de recurso de tipo servidor de nombres (NS) puede ser utilizado de dos maneras para designar a los servidores de referencia para un nombre de dominio DNS:

- Permite designar a los servidores de referencia en el dominio de tal manera que sean comunicados a los que solicitan información sobre este dominio.
- Permite también designar a los servidores DNS de referencia para los subdominios que serían "delegados en el exterior de la zona". En este caso, el registro NS desempeña el papel de puntero hacia los servidores DNS que soportan la gestión de los subdominos cuya gestión se delega a un nivel inferior.

El registro de NS se utiliza para asignar un nombre de dominio DNS al nombre de los hosts que ejecutan los servidores DNS. El registro de NS se utiliza de forma simple como se indica en el siguiente ejemplo.

Por ejemplo, la línea *dom1.company.com. IN NS srv-dns1.dom1.company. com* indica que el servidor DNS srv-dns1.dom1.company.com actuará como servidor DNS de referencia para el dominio dom1.company.com.

Utilización del carácter @ con el registro de Tipo NS:

- La línea @ *NS vmdc01.corpnet.priv* quiere decir que el servidor DNS vmdc01.corpnet.priv funcionará como servidor DNS de referencia para el dominio específico. En este caso, el valor del campo será el establecido como comentario en la cabecera del archivo, la cual se declara en el archivo de arranque en un servidor DNS de tipo BIND o en el registro de un servidor DNS Windows Server.

El archivo BOOT se describe más adelante en la sección Opciones de arranque del servidor DNS.

Con respecto a los nombres de servidores DNS

El hecho de que el nombre "muestre" que el servidor DNS forma parte del mismo dominio carece de consecuencias. En efecto, un servidor DNS dado puede gestionar múltiples zonas DNS.

El sistema de nombres del servidor DNS se verá influido principalmente por la posición de dicho servidor dentro de la red Intranet o dentro de la red Internet. En el caso de un proveedor de servicios Internet, es evidente que no puede haber ninguna dependencia entre las zonas alojadas, las cuales pertenecen a terceros. A la inversa, cuando el servidor DNS está ubicado en la empresa, es probable que su nombre completo esté derivado de o de los espacios de nombres existentes en la empresa.

Sea como sea, un servidor DNS deberá ser declarado dentro de una zona DNS empleando un nombre de dominio completamente cualificado (FQDN) para poder actuar como un host designado como servidor de nombres para dicha zona. Luego, el nombre debe corresponder a un registro de recursos de host (A) válido en el espacio de nombres de dominio DNS.

Observe que la consola MMC DNS crea por defecto de forma automática un registro de recurso NC único para el servidor DNS local en el que fue creada en principio la zona.

3. Nombres de dominio DNS y nombres de dominio Active Directory

El espacio ofrecido por Active Directory puede ser derivado de la zona de Internet o estar completamente disociado. Por ejemplo, la empresa*corporate.com* podrá disponer de un dominio Active Directory con el mismo nombre, o bien crear la separación del nombre de dominio de diferentes maneras. Los puntos anteriores muestran a grandes rasgos las estrategias de nombres, sin embargo volveremos sobre estos puntos en detalle más adelante.

Las distintas interrupciones del espacio se presentan de forma breve a continuación:

- *privnet.corporate.com*, para implementar un subdominio del espacio existente oficialmente declarado.
- *privnet.corp.com*, para implementar un nuevo dominio derivado del nombre oficial de Internet (corp en lugar de corporate) y un subdominio dedicado a la raíz de Active Directory (privnet).
- *privnet.corporate.local*, para implementar un nuevo dominio derivado del nombre oficial de Internet (Corp o corporate), un subdominio dedicado a la raíz de Active Directory (privnet) y un espacio de resolución privado utilizando como dominio de primer nivel del dominio .local.

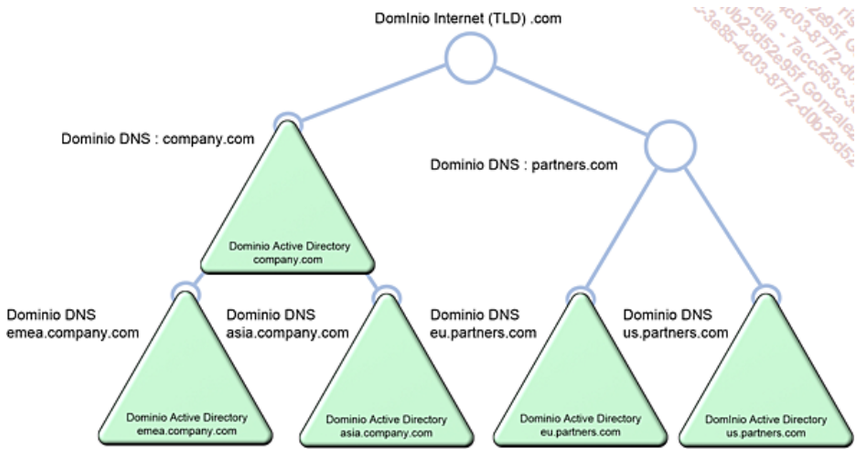
Con respecto a los nombres de dominio DNS y Active Directory: aunque no se recomiende, Active Directory no impone el uso de un dominio de nivel superior válido como .com o .net. Observe sin embargo que las mejores prácticas consisten en respetar los TLD (*Top Level Domains*) conocidos.

Los nombres de dominio DNS utilizados para llamar a los directorios Active Directory no coinciden necesariamente con el espacio DNS completo. De hecho, aunque se parecen, no se deben confundir.

El cuadro siguiente muestra una configuración posible.

Nombre de dominio DNS	Dominio Active Directory
Dominio (.)	No recomendado.
company.com	Si. Este dominio puede desempeñar el papel de raíz Active Directory.
emea.company.com	Sí (Europe Middle East and Africa).
asia.company.com	Si.
us.partners.com	Si Este dominio está reservado para los socios US.
eu.partners.com	Si. Este dominio está reservado para los socios de la Unión Europea.

El dominio partners.com existe a nivel DNS pero no existe como dominio de Active Directory.



DNS ofrece sus servicios en Active Directory para el sistema de nombres de dominio y nombres de hosts.

Por lo tanto, **cualquier dominio de Active Directory es por fuerza un dominio DNS, pero todo dominio DNS no es por necesidad un dominio Active Directory**.

4. Tipos de zonas y servidores de nombres DNS

La configuración de un servidor DNS dependerá del papel que queramos asignar al servidor en función de múltiples parámetros como la topología de red, la estructura o el tamaño del espacio DNS que quiera mantenerse.

Con independencia de sus limitaciones, los componentes básicos de cualquier infraestructura DNS se basarán en los tres tipos de zonas que figuran a continuación:

- Las zonas primarias;
- Las zonas secundarias;
- Las zonas de rutas internas.

En función de los casos, el hecho de utilizar varias zonas puede facilitar la implementación de una solución que de partida parecía muy compleja. A modo de analogía, ¡podemos imaginar la enorme problemática de gestión de servicios DNS en la escala de Internet!

¡Por fortuna, los millones de zonas que componen el espacio DNS de Internet y los conceptos de delegación hacen que esta inmensa red se pueda administrar y esté plenamente operativa a escala planetaria!

a. Servidores de nombres y zonas primarias

Un **servidor primario** (también llamado **principal**) para una determinada zona es el único servidor con una copia de la zona disponible en escritura. Este punto significa que cualquier modificación de la zona requiere un acceso al único servidor primario para dicha zona.

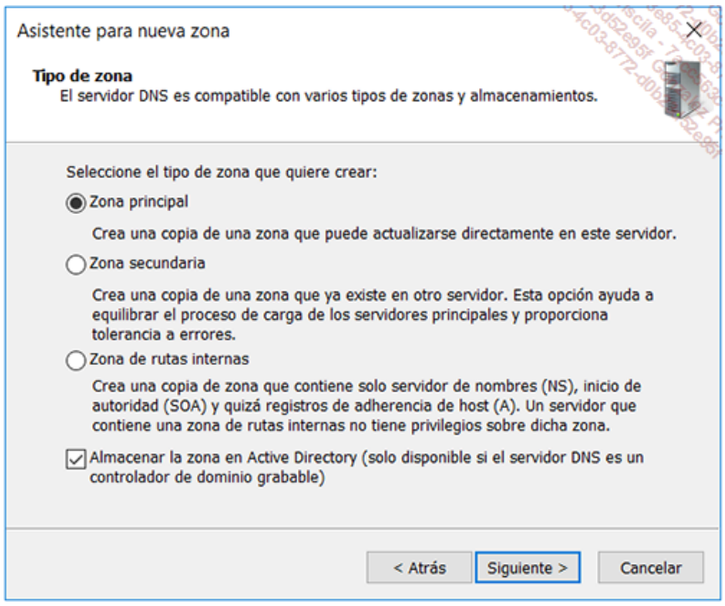
Una vez aportadas las operaciones de cambio, los datos serán automáticamente replicados en el o los otros servidores DNS que actúan como servidores de nombres DNS secundarios para la zona. Estas operaciones de replicación de zonas son por supuesto indispensables para asegurar la disponibilidad de una zona en múltiples servidores DNS locales y remotos.

Las zonas principales pueden ser de dos tipos:

Zonas principales estándar: cuando se trata de una zona principal estándar, un único servidor DNS podrá alojar y cargar la copia principal de la zona. Ningún servidor principal adicional estará autorizado para esta zona. Además, sólo el servidor DNS principal para la zona estará autorizado para aceptar las actualizaciones dinámicas y tratar las modificaciones que afecten a la zona. Este modelo presenta un punto de fallo, ya que la falta de disponibilidad del servidor de gestión de la zona principal tendrá el efecto de no permitir las actualizaciones de la zona, tanto a través de las funciones de administración como a través del protocolo de actualización dinámica de los registros DNS (DDNS, *Dynamic DNS*). Sin embargo, los otros servidores DNS que actúen como servidores secundarios para la zona, podrán seguir respondiendo a las peticiones de los clientes, hasta la extinción de la misma.

La expiración de las zonas secundarias se explica más adelante.

Zonas principales integradas en Active Directory: podemos crear una zona principal en la que los datos y otros parámetros se almacenan en el directorio Active Directory. En el mismo orden de ideas, también podemos incorporar una zona primaria existente en Active Directory modificando la plantilla de la zona en el servidor principal de origen.



Esta pantalla muestra cómo cambiar el tipo de una zona DNS. Las zonas de tipo zona principal y zona de rutas internas pueden crearse de forma normal o dentro de Active Directory. Por lógica, las zonas secundarias no pueden hacerlo porque no tienen ningún significado dentro de los mecanismos soportados por Active Directory.

Grandes ventajas de la integración Active Directory

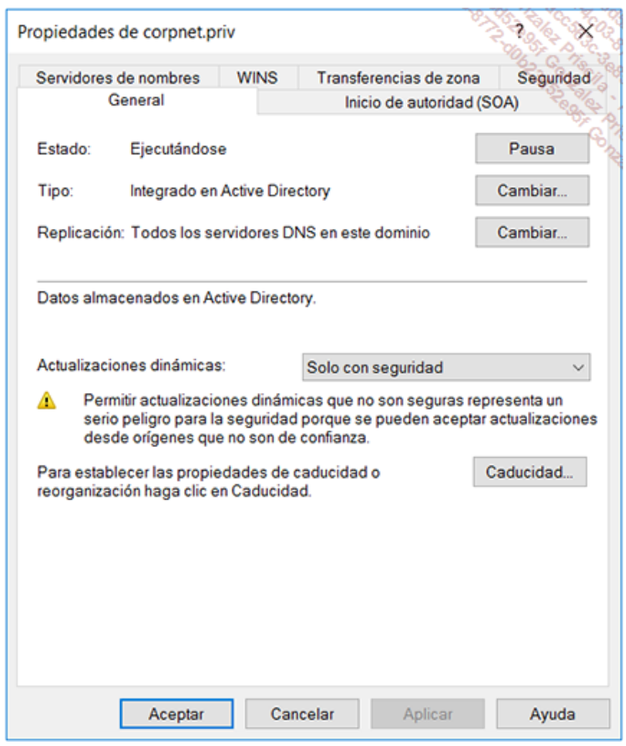
Veremos más adelante que los mecanismos soportados por los servicios de dominio de Active Directory permiten a los servidores DNS que funcionan en Windows 2000 Server y versiones posteriores resolver la casi totalidad de las problemáticas propias de DNS.

Sin embargo, podemos de partida señalar que la integración de Active Directory nos permite disponer de varios servidores principales para la misma zona. Esta configuración es posible porque los controladores de Active Directory son, por definición, iguales y disponibles en lectura y escritura.

De esta forma, es igual decir que todos los servidores DNS se beneficiarán de este mecanismo y pueden soportar el modo de actualización dinámica de DNS para una determinada zona.

Así, el punto de fallo constituido por el servidor DNS primario para una zona queda suprimido gracias al hecho de que todos los controladores de dominio actúan como múltiples servidores primarios.

La interfaz gráfica de la consola de gestión del DNS nos permite ver y modificar las zonas administradas.



Ejemplo de las propiedades de una zona: estados, tipo, naturaleza de la replicación de la zona y soporte de actualizaciones dinámicas.

Podemos añadir una nueva zona principal en cualquier servidor DNS cada vez que sean necesarios dominios o subdominios adicionales en nuestro espacio de nombres DNS.

Podemos realizar otras tareas de configuración de las zonas en función de las necesidades.

Recordemos los siguientes puntos:

- El servidor DNS principal de una zona desempeña el papel de punto de actualización para la zona. Toda nueva zona creada es una zona principal.
- En el uso de las zonas principales estándar, no es recomendable que otro servidor DNS se configure para actuar como servidor principal para una zona ya existente. Aunque parezca que esto funciona, esta configuración no está soportada. En efecto, podría generar errores o incoherencias entre los servidores que se encargan de versiones distintas de la misma zona.
- Existen dos tipos de zonas principales: las zonas principales estándar y las zonas principales integradas en Active Directory. La integración de las zonas en Active Directory se aborda en el capítulo Integración de las zonas DNS en Active Directory.

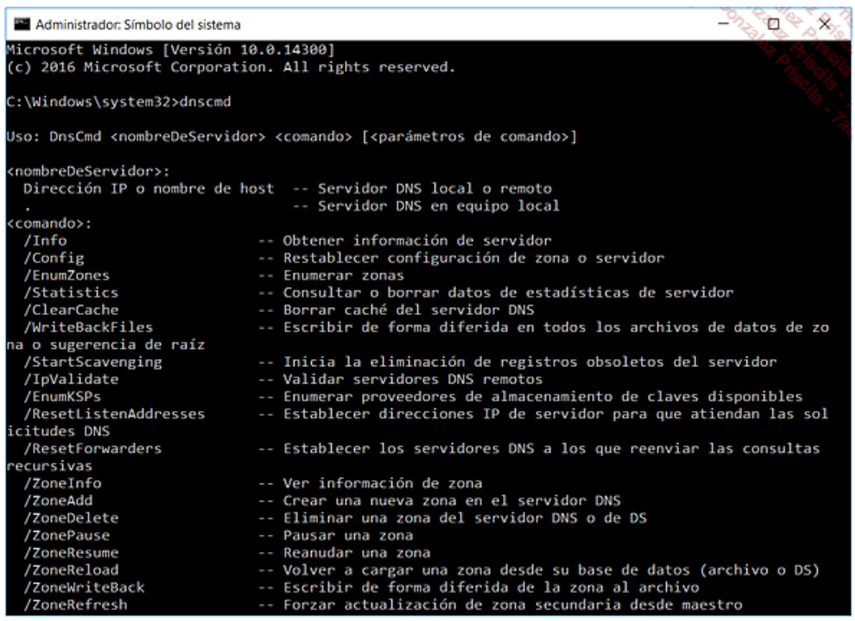
b. Servidores de nombre y zonas secundarias

Un servidor secundario a una determinada zona posee una copia no editable del archivo de base de datos de la zona. El único modo de actualizar los datos e información de zona consiste en realizar una transferencia de zona a partir de uno de los servidores que actúan como fuente para la zona.

El servidor de nombres secundario para una determinada zona conoce su fuente de contenido mediante una declaración de la dirección IP del servidor DNS que actúa como servidor DNS maestro. Los puntos siguientes resumen las características que permiten a los servidores DNS intercambiar información:

- El servidor maestro puede ser el servidor primario.
- El servidor maestro también puede ser cualquier servidor DNS secundario para la zona.
- El servidor maestro también puede ser cualquier servidor DNS con autoridad para una zona integrada en Active Directory.
- Un servidor secundario puede basarse en varios servidores maestros.
- La topología es por completo libre. De esta forma, el servidor A puede ser maestro para el servidor B, que puede ser maestro para el servidor C y así sucesivamente.

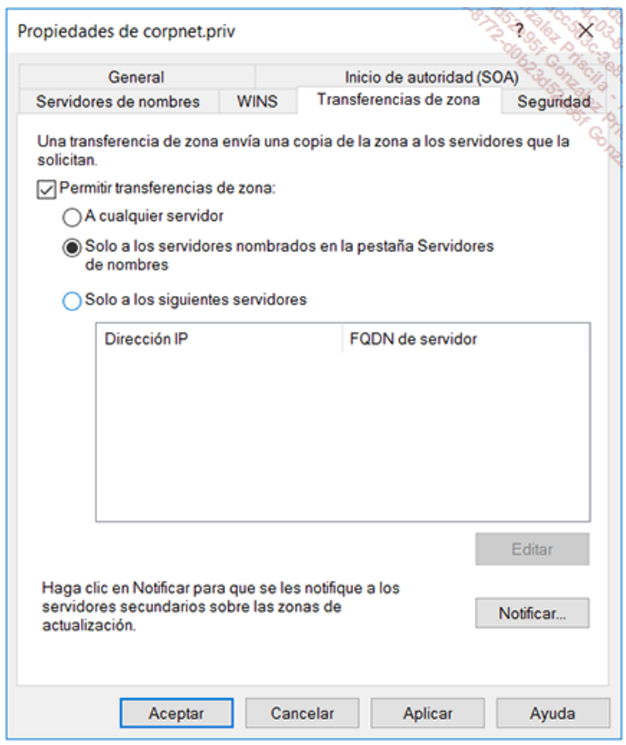
Todas las operaciones de creación, supresión, modificación y replicación de las zonas pueden efectuarse a través del comando **dnscmd.exe** o a través de la consola MMC de DNS.



Una vez creada la zona secundaria, la última etapa consiste en declarar las direcciones IP de los servidores maestros que pueden ser contactados para obtener información de registro de actualizaciones de esta zona. Esta zona de lista solo se muestra cuando el tipo de zona se define como secundaria o stub. Cuando una zona del servidor debe replicarse, el servidor DNS usa esta lista para ponerse en contacto con un servidor maestro y obtener una actualización de la zona. Si la zona ha sido modificada y es necesaria una actualización, se lleva a cabo una transferencia parcial o total de la zona. Observe que esta lista nos permite controlar el orden en que los servidores maestros serán solicitados.

Las primeras versiones de los servidores DNS realizaban transferencias de zona completas.

La RFC 1995 publicada en 1996 implementa un mecanismo más eficaz de transferencia de zona. Se trata de la transferencia de zona incremental mediante la cual sólo se replicarán las modificaciones al servidor o los servidores secundarios para la zona.



*Autorización de transferencias solo a los servidores listados en la pestaña **Servidores de nombres** para la zona corpnet.priv.*

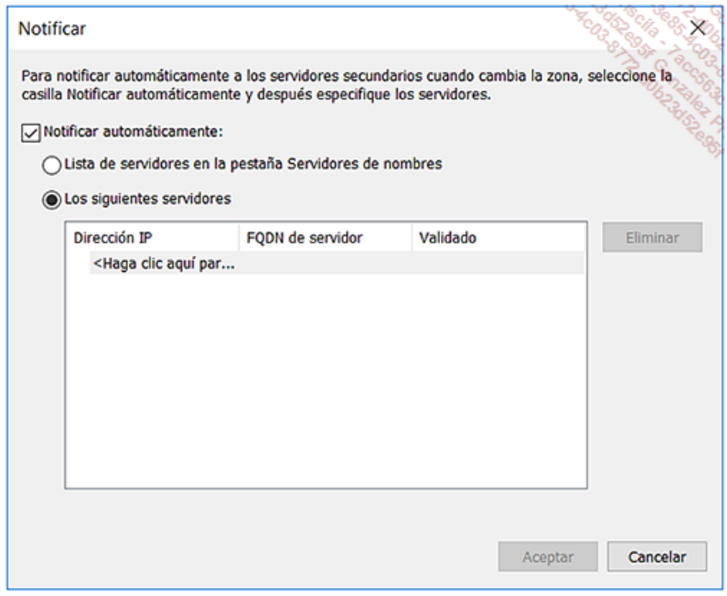
A diferencia de las zonas estándar donde las transferencias de zonas se activan por defecto hacia los servidores listados en la pestaña**Servidores de nombres**, las transferencias de zona no están autorizadas en las áreas integradas en Active Directory.

De hecho, esto es normal en la medida en que las áreas integradas en Active Directory se replican mediante la replicación de Active Directory y no a través de los mecanismos de transferencia de zonas DNS.

En el caso en que una zona Active Directory deba estar disponible como zona secundaria en un servidor que no sea Controlador de Dominio, debemos autorizar estos servidores para replicar la zona.

La RFC 1996 publicada en 1996 implementa otra mejora al proceso de transferencia de zona. Se describe un mecanismo de notificaciones que permite al servidor primario alertar a los servidores secundarios cuando se realizan cambios en la zona.

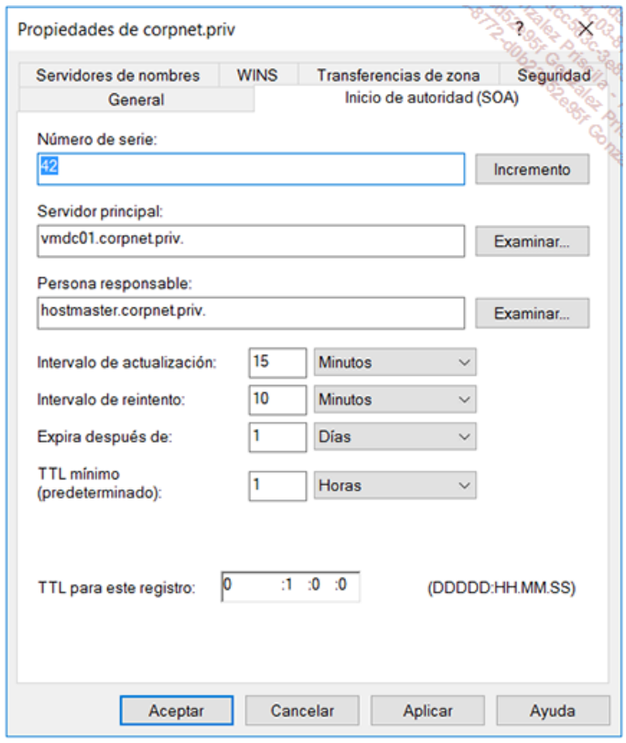
La pantalla siguiente muestra que este método permite notificar al o los servidores DNS especificados por una determinada dirección IP o, de manera más sencilla, a todos los servidores DNS que especifiquemos para desempeñar el rol de servidores de nombres para la zona.



En cuanto a lo que respecta a las transferencias de zonas, la función de notificación se activa para todos los servidores enumerados en la pestaña **Servidores de nombres** cuando se trata de zonas primarias o secundarias estándar. Recordemos que no ocurre lo mismo cuando se trata de zonas integradas en Active Directory. Siempre en cuanto a las zonas estándar, podemos optimizar las comunicaciones en enlaces de red sobrecargados, declarando solo los servidores que deseamos notificar.

En el caso de redes sobrecargadas, la solución óptima consiste en utilizar la replicación de Active Directory.

En el caso de que decidamos no utilizar la función de notificación presentada más arriba, entonces el servidor secundario no podrá contar con las propiedades del registro SOA.



Parámetros de replicación de una zona mediante el registro SOA.

Como se muestra en la pantalla anterior, el servidor secundario entrará en contacto con el servidor de nombres primario para la zona:

- La primera vez en base al intervalo de actualización, es decir, al cabo de 15 minutos.
- Luego, en base al Intervalo de reintento, es decir, cada 10 minutos, durante un máximo de un día, el valor del período de caducidad de la zona. Observe que estos parámetros de replicación se definen en el registro de SOA a nivel de cada zona.

La dirección de correo de la persona responsable no debe contener el símbolo habitual @. En efecto, este carácter es considerado por DNS como un símbolo genérico que significa la zona misma.

La duración de vida del registro de SOA (valor por defecto de 1 hora) se envía de forma automática a todos los registros de recursos de la zona, a menos que un valor -específico no esté asignada a un registro determinado.

Recordemos que cuando un servidor Windows Server gestiona las zonas DNS integradas en Active Directory, las transferencias de zona son soportadas por el motor de replicación de Active Directory y no por las transferencias de zona completas o incrementales.

El componente que se hace cargo de las operaciones de replicación entre controladores de dominio se llama DRA (*Directory Replication*

Agent). Este componente es en particular importante, y puede requerir de supervisión. Muchos contadores de rendimiento se exponen en el analizador de rendimiento bajo el nombre DirectoryServices.

Los parámetros de SOA son sólo útiles y utilizables por los servidores secundarios de la zona. En efecto, una zona integrada en Active Directory deberá ser replicada tanto en los servidores que soporten la integración de Active Directory como hacia los servidores DNS estándar que solo soporten los mecanismos de replicación tradicionales (es decir, completos e incrementales).

c. Tipos de transferencia de zona DNS

Acabamos de ver que las zonas DNS se mantienen en un estado de actualización coherente mediante el registro SOA definido a nivel de la zona principal.

Los servidores DNS que disponen de una zona secundaria cumplen los parámetros de refresco de SOA. Además, también pueden ser notificados empleando el protocolo DNS NOTIFY definido en la RFC 1996 "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)".

Vamos a descubrir más tarde que las transferencias de zona pueden realizarse de diferentes maneras.

Transferencia de zona inicial

Cuando un nuevo servidor DNS se declara como un servidor secundario de una determinada zona, se negocia la transferencia de zona completa (AXFR) a fin de obtener una copia completa de los registros de recursos para la zona.

Las antiguas versiones de servidores DNS, tales como la implementación realizada bajo NT 4.0, soportan únicamente las transferencias de zona completas.

Transferencias de zona incrementales y servidores BIND de Unix

Con respecto a las transferencias de zona incrementales sobre plataformas Unix, observemos que las primeras versiones realmente operativas requieren una versión de tipo BIND (*Berkeley Internet Name Domain*) 8.2.3.

Las versiones BIND 9.x funcionan correctamente con los servidores Windows Server 2008 R2 y versiones posteriores, así como con las versiones anteriores de BIND 8.2.3.

En las plataformas Unix que utilizan un servidor DNS de tipo BIND, se recomienda que los cambios se lleven a cabo en la zona en el modo de actualización dinámica.

En este caso, es el cliente DNS dinámico el que efectúa la operación de creación o actualización del registro de recurso. Luego, el servidor DNS asumirá la gestión del número de versión de este registro para las replicaciones y actualizaciones posteriores. Esto significa que para aprovechar al máximo las transferencias de zonas incrementales (IXFR - *Incremental Transfer*), hay que evitar editar directamente los archivos de zona.

Esta observación se refiere únicamente a las implementaciones de BIND. Los servidores DNS de Windows Server se basan en las transferencias de zonas incrementales cuando las operaciones se realizan a partir de la Consola de administración MMC de DNS o bien aprovechando la replicación de Active Directory, que por definición, réplica los objetos, atributos y valores.

El almacenamiento de las zonas en el directorio Active Directory se trata en el capítulo Integración de las zonas DNS en Active Directory.

Verificación de transferencia de zona incremental

Sea cual sea el método de transferencia de zona utilizado (AXFR o IXFR), la primera cosa realizada por el servidor DNS consiste en comprobar si es necesario llevar a cabo o no una transferencia de zona. Este control se realiza en función del valor del intervalo de actualización incluido en el registro de recurso de tipo SOA (*Start Of Authority*) cuyo valor por defecto será de 15 minutos.

Para poder determinar si es necesario o no iniciar una transferencia de zona, el servidor DNS secundario para la zona considerada verifica el valor del número de serie a partir del registro de recurso SOA. En el caso de que las dos versiones sean idénticas, no se efectúa ninguna transferencia.

Si por el contrario el número de serie de la zona es más alto en el servidor maestro que en el servidor secundario, entonces se efectúa una transferencia. Si el servidor maestro tiene un historial de cambios incrementales, entonces el protocolo IXFR será negociado.

Evidentemente, el proceso de transferencia incremental definido en la RFC 1995 mucho menos tráfico de red. Otra ventaja concierne a la rapidez de la operación de replicación, ya que sólo las modificaciones viajan entre los dos servidores.

¿Cuando puede producirse una transferencia de zona?

- Cuando el intervalo de actualización de la zona expira (es decir, por defecto cada 15 minutos).
- Cuando un servidor secundario es advertido por su servidor maestro que la zona ha cambiado. Las notificaciones son implementadas por la RFC 1996.
- Cuando el servicio Servidor DNS se inicia en un servidor secundario de la zona.
- Cuando la consola DNS se utiliza en un servidor secundario de la zona para arrancar manualmente una transferencia de zona a partir de su servidor maestro.

Transferencias de zona: temas generales, puertos TCP/IP y tramas

Recordemos los siguientes puntos:

- No es posible configurar una lista de notificación para una zona de rutas internas. Las zonas de rutas internas son tratadas más adelante en este capítulo (véase sección Zonas de rutas internas).
- La notificación DNS debería ser utilizada solo para informar a los servidores que funcionan como servidores secundarios para la zona. En efecto, las zonas integradas en Active Directory se replican por Active Directory que tiene sus propios mecanismos de notificación.
- El uso de notificaciones con las zonas DNS integradas en Active Directory puede degradar el rendimiento del sistema creando peticiones de transferencia adicionales para la zona actualizada, cuando esto no es necesario.

Tenga en cuenta que el tráfico relacionado con las resoluciones y replicaciones DNS son bajos en comparación con los tráficos generados por los usuarios.

El protocolo DNS usa el puerto 53 TCP y UDP. El detalle de las operaciones realizadas en cada transporte (TCP o UDP) se especifica a continuación:

Puerto Fuente UDP 53 con destino al mismo puerto

El Protocolo User Datagram Protocol (protocolo de tipo no orientado a la conexión) se utiliza en principio para las solicitudes de resolución entre un cliente DNS y el servidor DNS solicitado. Sin embargo, si la respuesta supera un cierto plazo, entonces el cliente DNS (la parte DNR) repetirá su petición de resolución a través de TCP, siempre en el puerto 53. Por definición, el protocolo de transporte UDP es rápido, pero no garantiza que los datos enviados sean recibidos.

El protocolo Transport Control Protocol (Protocolo orientado a la conexión) se utiliza en peticiones más largas, como las transferencias de zona. A diferencia del protocolo UDP, el protocolo TCP garantiza que los datos enviados serán recibidos.

En la configuración de un firewall, asegúrese de permitir el tráfico UDP y TCP 53. En efecto, el hecho de solo declarar uno de los dos protocolos de transporte provocará un fallo aleatorio de los servicios DNS.

d. Servidores de caché y servidores DNS

Por definición, un servidor de caché no controla ni administra ninguna zona. Se limita a hacer caché de todas las resoluciones de nombres que realiza. Un servidor de caché puede ser utilizado cuando, por ejemplo, el ancho de banda disponible entre un sitio y otro es insuficiente para considerar la replicación de una o varias zonas.

Ya que el servidor de caché no dispone de zona, es evidente que no hay tráfico de transferencia de zona DNS. Por defecto, el servidor de caché almacena durante una hora todas las resoluciones exitosas.

Por último, un servidor DNS que gestiona zonas (primarias, secundarias, Active Directory), es por naturaleza, también un servidor de caché. De hecho, la única diferencia es que los servidores "caché" no tienen ninguna información de zona.

La pantalla detallada permite visualizar el contenido del caché del servidor DNS. Se activa mediante un clic derecho sobre el objeto servidor DNS y **Ver/Avanzada**.

En el caso de que una información del caché pase a no ser válida, pero activa en caché, contaremos con la posibilidad de eliminar el registro. Tenga en cuenta que no es posible modificar una información puesta en caché. La única operación autorizada es la eliminación.

Implementación de zonas estándar: buenas prácticas

Con independencia de la tecnología utilizada (Apple, IBM, Novell, Microsoft, sistemas Unix) la aplicación de dominios DNS -¡Y con mayor motivo los dominios DNS dentro de una infraestructura Active Directory!- requiere el cumplimiento de una serie de buenas prácticas.

Encontraremos a continuación los puntos esenciales y otras buenas prácticas a respetar.

Consideraciones propias de los servidores y zonas DNS

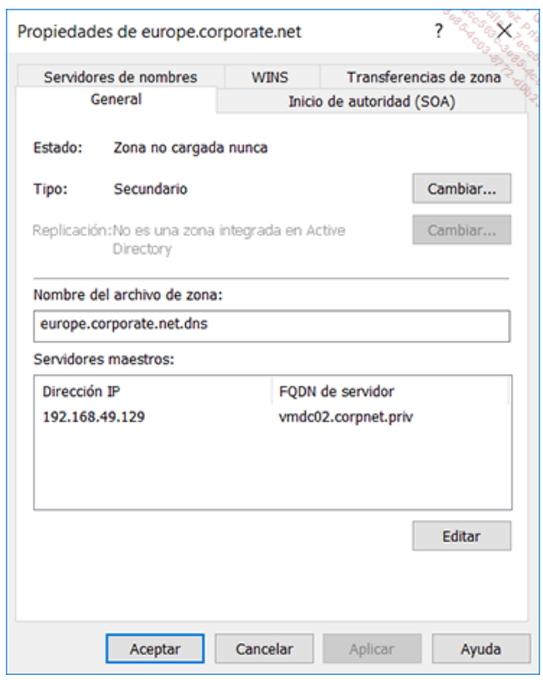
Utilice un mínimo de dos servidores DNS para cada zona del espacio. Por lo tanto, para cada zona DNS, necesitaremos como mínimo de una zona principal estándar y un servidor secundario para la zona.

Para las zonas principales integradas en el directorio Active Directory, podemos basarnos de forma exclusiva en servidores Windows que actúen como controladores de dominio de Active Directory. Esta solución es considerada como "la" mejor práctica ya que el servicio DNS si bien es necesario para la infraestructura de dominio se beneficia a su vez de las funciones de redundancia y tolerancia a fallos inherentes a los controladores de dominio Active Directory.

Los servidores secundarios nos permiten distribuir el tráfico de peticiones DNS en algunas partes de la red donde existe una zona muy utilizada.

Los servidores secundarios garantizan una disponibilidad total de la zona, fuera de la posibilidad de modificar su contenido. En el caso de que el servidor primario para la zona no se encuentre disponible de forma prolongada, contaremos a pesar de todo la posibilidad de "promover la zona" de un servidor secundario a primario mientras esperamos que el servidor principal original esté de nuevo disponible.

Mensaje sistema indicando que la zona ha expirado



Modificación del tipo de zona de secundaria a principal

Una zona cuyo estado ha expirado deja de responder. El cambio del tipo de zona de secundaria a principal permite hacerla autónoma. De hecho, la zona estará de nuevo operativa.

Ubicación de los servidores DNS

Para optimizar los flujos generados por las resoluciones DNS, deben instalarse servidores secundarios lo más cerca posible de los clientes. En el caso de que un elemento de la red (router, firewall, elementos activos) pueda ser un punto de fallo para ponerse en contacto con el servidor DNS por defecto, asegurarse de declarar otro servidor DNS. De esta manera, un componente defectuoso no afectará a las resoluciones.

En el caso de los servicios de dominio de Active Directory, es frecuente considerar los servicios de infraestructura como un elemento que forma un todo. Así, cada sitio debe disponer de sus propios servicios de infraestructura, es decir, un controlador de dominio, un servidor

DNS, un catálogo global y por qué no, un servidor que actúe como servidor DFS (*Distributed File System*) raíz, si se emplea DFS en el sitio. Esta lista de servicios no es, por supuesto, exhaustiva, pero podemos considerar que tales servicios son por definición los servicios de infraestructura y, pueden de hecho sumarse con facilidad en el mismo servidor. Este servidor será considerado como un **Servidor de infraestructura**.

Influencia de las ubicaciones en relación a las transferencias de zona

Las transmisiones pueden variar de forma considerable entre una configuración que implemente la aplicación de las transferencias de zonas completas (AXFR - *All Transfer*) e incrementales (IXFR). Tenga especial cuidado en el hecho de que las transferencias IXFR pueden fallar.

Replicación de las zonas de búsqueda inversa y número de servidores DNS

La cuestión que se plantea se refiere al número de zonas y el número de registros por zona que habrá que replicar en los N servidores DNS. De todos modos, se notará que hay tantos nombres registrados como direcciones IP asociadas. Además, las buenas prácticas DNS nos animan a establecer zonas de búsqueda inversa.

Por lo tanto, la problemática puede minimizarse y la cuestión puede reducirse a lo siguiente: ¿Es conveniente replicar las zonas de búsqueda inversa en todos los servidores que cuentan con zonas de búsqueda directa?

La conclusión es que los servidores secundarios son en principio utilizados para las zonas de búsqueda directa. Parece que en general, un servidor secundario de una zona de búsqueda inversa no es utilizado fuera de la red y de la subred que atañe a la zona indirecta. Este punto se debe de forma fundamental al hecho de que la parte más importante del tráfico entre los equipos cliente y los servidores tiene lugar en la misma red o subred IP.

La buena práctica puede limitar el número de servidores secundarios para las zonas de búsqueda inversa o bien limitar el tráfico utilizando zonas integradas en Active Directory para aprovechar las replicaciones comprimidas, incrementales, seguras y controladas por la topología de replicación de Active Directory.


El almacenamiento de las zonas en el directorio Active Directory se trata en el capítulo Integración de las zonas DNS en Active Directory.

Delegación de las zonas

Este poderoso mecanismo permite la creación de espacios de dominio casi infinitos. El mejor ejemplo de utilización de la delegación es la red Internet. Cada dominio comprado es por supuesto una zona cuya gestión se delega a un tercero responsable.

Así, la delegación de las zonas DNS implica por necesidad una división del espacio de nombres en una o varias partes, que luego pueden ser almacenadas, distribuidas y replicadas en otros servidores DNS.

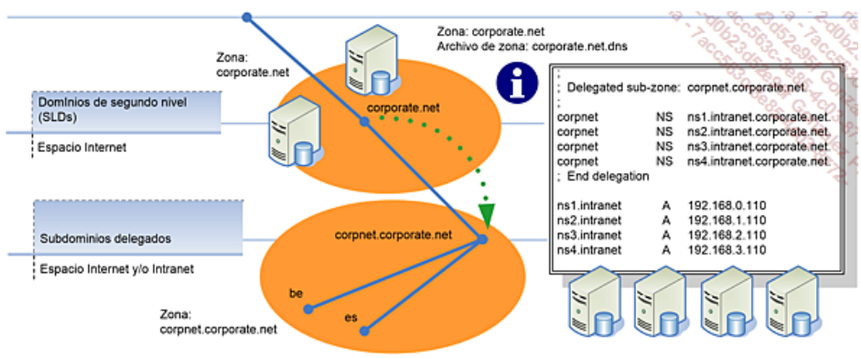
Cabe recordar que hemos visto antes que la utilización de zonas adicionales permite satisfacer las necesidades siguientes:

- Transferir la gestión de una parte de su espacio de nombres a otro lugar geográfico u otra autoridad ejecutiva.
- Dividir una zona muy voluminosa en varias zonas más pequeñas para distribuir el tráfico entre las diferentes regiones geográficas de la red.
- Dividir un espacio compuesto por N dominios DNS en varias zonas para implementar una mejor tolerancia a fallos en caso de fallo de la zona.

El punto más importante para conseguir la implementación de la delegación de una zona consiste en que se declaren los registros de delegación.

Estos registros desempeñarán el papel de "punteros" a los servidores DNS que tiene -autoridad para resolver nombres pertenecientes a los subdominios delegados.

Para ilustrar esta técnica, podemos basarnos en el ejemplo presentado a continuación.



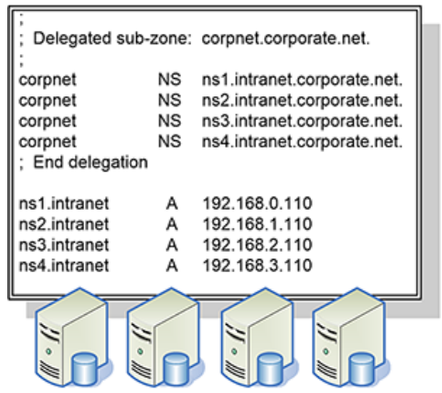
Registros de delegación en el archivo de zona corporate.net.dns

De partida, la empresa implementa un dominio llamado *corporate.net*. Como siempre, el dominio es implementado bajo la forma de una zona hospedada en uno o varios servidores DNS. Estos servidores pueden estar situados tanto en Internet como en la intranet de la empresa, sabiendo que el concepto de delegación es rigurosamente idéntico en ambas partes de la red.

Una zona de tipo primario será por lo general creada, y de hecho, el archivo básico de datos de la zona llamada *corporate.net.dns* estará situado en el directorio *%Systemroot%\ system32\dns*.

Luego, conviene disponer de los registros que permitan localizar el subdominio en cuestión. En nuestro ejemplo, es necesario que sea posible referirse a los servidores con autoridad para el dominio DNS *corpnet.corporate.net*.

Podemos declarar estos registros agregando las líneas necesarias en el archivo de zona de la zona *corporate.net* -tal como se especifica a continuación, o utilizar los asistentes de la consola de gestión del servicio DNS.



Ubicación de los servidores de referencia para la zona corpnet.corporate.net empleando los registros de recursos de tipo NS y A

Las declaraciones encontradas en el archivo muestran que el subdominio *corpnet.corporate.net* es administrado por cuatro servidores DNS, los cuales están situados en cuatro subredes diferentes. De esta forma, se puede resolver el contenido del subdominio *corpnet.corporate.net* en los cuatro puntos geográficos.

Por último, solo queda asegurarse de que es posible resolver esos nombres de servidores DNS.

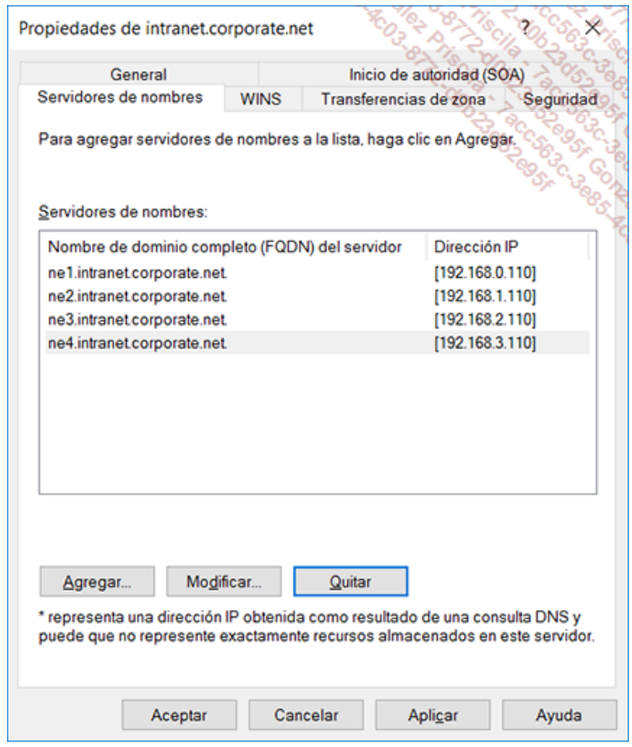
Resolución de los nombres de los servidores DNS

Durante la asignación de servidores con los nombres de host en la misma zona, se emplean de forma ideal los correspondientes registros de recursos A (Dirección IP) .

Para los servidores especificados utilizando un registro de recurso como parte de una delegación de la zona a otro subdominio o si simplemente el nombre completo es diferente, entonces los nombres de estos equipos se llaman nombres fuera de zona.

Resolución de los nombres de los servidores DNS fuera de la zona

Para la resolución de nombres fuera de la zona, los registros de recursos A para los servidores fuera de zona especificados son obligatorios. Tenga en cuenta que cuando los registros NS y A de fuera de la zona son necesarios para efectuar una delegación, se llaman **registros para peticiones sucesivas**. Este caso es bastante clásico y por lo tanto nada atípico.



Propiedades del subdominio corpnet.corporate.net

La pantalla anterior muestra que el dominio corpnet.corporate.net es administrado por cuatro servidores DNS situados en dominios o subdominios diferentes del dominio que contiene los registros de delegación.

En relación con el FQDN del registro de NS y registros A, la interfaz gráfica puede poner de relieve las direcciones IP recuperadas a través de una consulta DNS. En este caso, aparece una estrella al lado de la dirección IP.

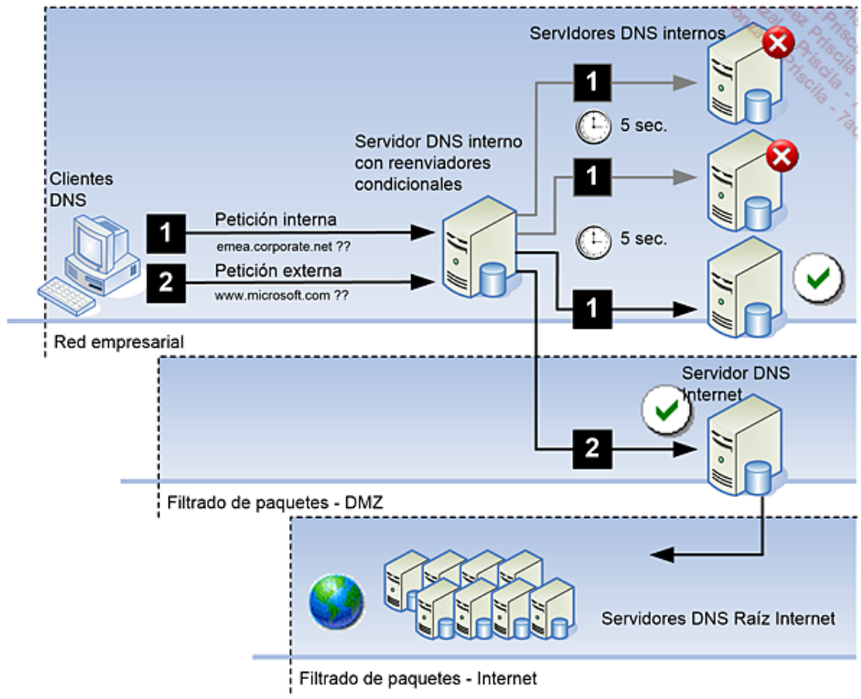
Acabamos de ver que la delegación de las zonas permitía la implementación de un espacio lógico distribuido de forma física en múltiples puntos de red. Las delegaciones permiten la resolución de las áreas directamente inferiores, por lo tanto, hacer descender las peticiones de resolución. A la inversa, para cambiar o remontar en el espacio de resolución, será necesario remontarse a lo más alto de la jerarquía, es decir, hasta el dominio raíz (.), mediante la utilización de las indicaciones de raíz.

Utilización de los reenviadores

Por lo general, un reenviador es un servidor DNS configurado para redirigir las peticiones de nombres DNS externos a los servidores DNS situados fuera de la red de la empresa. Sin embargo, tenga en cuenta que es posible redirigir las peticiones para un dominio no contemplado pero situado en la red privada de la empresa.

Para que un servidor DNS desempeñe el papel de reenviador, es necesario que los otros servidores DNS de la red redirijan las peticiones que no pueden resolver de forma local al servidor particular.

De esta manera, el reenviador le permitirá gestionar la resolución de nombres situados fuera de su red, es decir, hacia Internet. La imagen siguiente muestra cómo los reenviadores son seleccionados y transmiten las peticiones de nombres externos hacia Internet.



Utilización de los reenviadores entre las redes intranet e Internet

Como podemos ver, el servidor DNS es en especial importante, ya que desempeña un papel tanto a nivel de las resoluciones internas como externas. Los apartados siguientes se refieren a la conexión a Internet, al buen uso de los reenviadores así como la posible desactivación de las consultas recursivas.

1. Exposición de la red privada en Internet

Cuando no existe un servidor DNS designado en concreto como reenviador, todos los servidores DNS pueden enviar peticiones fuera de la red utilizando sus indicaciones de servidores raíz.

Si bien es cierto que las indicaciones de raíz permiten resolver la totalidad del espacio gestionado, el inconveniente es que este método de resolución tiene el efecto de generar un volumen adicional de tráfico. En el caso de una conexión a Internet lenta o saturada, esta configuración será ineficiente y costosa en términos de ancho de banda consumido.

Observe: las solicitudes de resolución no satisfechas, por ejemplo, en el caso de avería de un servidor DNS interno -podrían tener como consecuencia exponer en Internet información DNS interna que pueden ser confidencial.

a. Correcto uso de los reenviadores para optimizar las resoluciones DNS

Si implementamos un servidor DNS como reenviador, entonces convertimos este servidor en responsable de la gestión de las resoluciones externas pudiendo disfrutar de las ventajas siguientes:

- La exposición de su red es eliminada ya que solamente las solicitudes no resueltas de forma interna estarán dirigidas hacia el reenviador y luego a Internet.
- El reenviador desempeñará el papel de servidor de caché en la medida en que todas las peticiones DNS externos de la red serán resueltas mediante él. En poco tiempo, el reenviador será capaz de resolver la mayor parte de las peticiones DNS externas explotando directamente su caché, lo que tendrá el efecto de reducir también el tráfico de resolución hacia Internet.
- En el caso de una conexión a Internet sobrecargada, el uso de la caché del reenviador servirá también para mejorar el tiempo de respuesta para los clientes DNS.

b. Comportamiento de los servidores DNS con o sin el uso de un reenviador

Un servidor DNS no se comporta de igual manera si está o no configurado para usar un reenviador. Cuando un servidor DNS está configurado para usar un reenviador, entonces se comporta de la manera siguiente:

- Cuando recibe una petición, el servidor DNS intenta resolverla empleando las zonas principales y secundarias que alberga y también en base a las resoluciones ya presentes en su caché.
- Si no logra resolver la solicitud con estos datos, entonces lo envía al servidor DNS designado como reenviador. Para contar con reenviadores siempre disponibles, tenemos la posibilidad de declarar varios reenviadores, fijar el orden de selección en una lista, así como el plazo de espera que provocará la utilización de otro reenviador.
- El servidor DNS espera un momento la respuesta del reenviador antes de tratar de ponerse en contacto con los servidores DNS estipulados en sus indicaciones de raíz.

Como puede ver en la etapa 3, las resoluciones que han fallado en primer lugar se desplazan hacia el reenviador antes de ser remitidas a las indicaciones de raíz. Por lo general, las indicaciones de raíz deberían ser servidores internos.

c. Reenviadores y tipos de consultas DNS

Por lo general, cuando un servidor DNS envía una solicitud de resolución a otro servidor DNS, se trata de una petición iterativa.

Por contra, cuando un servidor DNS envía una consulta a un reenviador, se comporta como un simple cliente y remitirá a éste una petición recursiva. De hecho, el servidor DNS, desempeña el papel de un simple cliente DNS, esperando a que la solicitud sea resuelta.

Cuando las delegaciones de zonas están configuradas, la referencia normal en una zona puede fracasar de forma aleatoria si el servidor DNS aparece configurado para utilizar reenviadores.

Zonas de rutas internas

Una zona de rutas internas es una copia de una zona que contiene sólo los registros de recursos necesarios para identificar a los servidores DNS que tiene autoridad para dicha zona. Este tipo de zona se utiliza para asegurar que un servidor DNS que alberga una zona principal conozca los servidores DNS con autoridad sobre su zona secundaria.

De esta manera, se mantiene la eficacia de las resoluciones.

Observe que las zonas de rutas internas están soportadas por servidores DNS de Microsoft Windows Server 2003 y versiones posteriores, y por supuesto por los servidores DNS BIND modernos.

Las zonas de rutas internas no están soportadas en los servidores DNS que funcionen bajo Windows 2000 Server.

1. Contenido de una zona de rutas internas

Como ya hemos explicado, una zona de rutas internas contiene un subconjunto de los datos de la zona compuesto solo por el registro de SOA (*Start Of Authority*), así como registros de NS (*Name Server*) y A. Estos últimos registros, llamados **Glue records**, permiten determinar de forma directa dentro de la zona las direcciones IP de los servidores de nombres (NS).

De hecho, una zona de rutas internas actúa como tabla de punteros permitiendo localizar directamente los servidores de nombres con autoridad para una determinada zona.

La creación de una zona rutas internas requiere la declaración de las direcciones TCP/IP de uno o varios servidores maestros. Estas declaraciones se utilizarán -como es el caso de las zonas secundarias- para actualizar la zona de rutas internas.

Los servidores maestros asociados a una zona de rutas internas son uno o varios servidores DNS que tienen la autorización para la zona secundaria. En general, se trata del servidor DNS que alberga la zona principal para el dominio delegado.

2. Ventajas de las zonas de rutas internas

Las zonas de rutas internas ofrecen muchas ventajas, entre otras cosas, en particular comparadas con las delegaciones de zona tradicionales. Los puntos presentados a continuación nos animarán sin duda a utilizar las zonas de rutas internas:

- Los datos relativos a las zonas delegadas son mantenidos de forma dinámica dentro de la zona de rutas internas.

La declaración de los registros necesarios para la implementación de la delegación de un subdominio es una información que puede evolucionar en función de la política de administración definida a nivel de la zona delegada. Es evidente que puede ser útil para planificar la modificación de las delegaciones en las zonas de rutas internas.

- Las resoluciones de nombres son mucho mejores.
- Se simplifica la administración de las zonas DNS.

Observe: las zonas de rutas internas no tienen el mismo objetivo que las zonas secundarias. En efecto, una zona secundaria contiene todos los registros, mientras que una zona de rutas internas sólo contiene los registros SOA, NS y de tipo Glue records.

Las zonas de rutas internas no deben utilizarse para sustituir las zonas secundarias, las cuales permiten una auténtica redundancia y una distribución de la carga de las resoluciones.

Eliminación de la delegación y creación de una zona de rutas internas

El problema expuesto se resuelve creando en el servidor DNS con autoridad sobre la zona principal company.com, una zona de rutas internas que corresponda al subdominio puesto en la delegación, europe.company.com. De esta forma, los administradores de la zona principal podrán basarse en los servidores maestros declarados para mantenerse informados sobre los posibles cambios de configuración del servidor DNS con autoridad sobre la zona secundaria puesta en delegación.

3. Actualización de las zonas de rutas internas

Las actualizaciones de las zonas de rutas internas funcionan siguiendo el mismo principio que las actualizaciones de las zonas DNS secundarias.

Durante las actualizaciones de la zona de rutas internas

El servidor DNS pregunta al servidor maestro para solicitar los registros de los mismos tipos solicitados en el paso anterior. Al igual que en el caso de las zonas DNS secundarias, el intervalo de actualización del registro de recurso SOA condiciona entonces el inicio (o no) de la transferencia de zona que provocará la actualización.

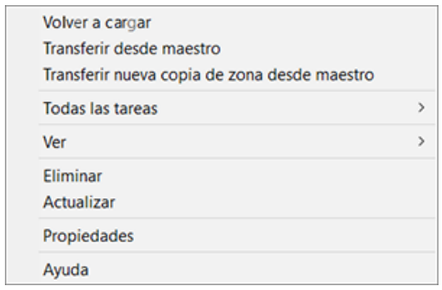
Expiración de las zonas de rutas internas

El fallo repetido de nuevos intentos de actualización a partir del servidor maestro puede alcanzar el valor del parámetro de expiración especificado en el registro SOA. Cuando se alcanza este valor, el estado de la zona de rutas internas pasará al estado expirado y el servidor DNS dejará de responder a cualquier solicitud de resolución de la zona.

a. Operaciones en las zonas de rutas internas

Las operaciones relativas a las zonas de rutas internas son similares a las operaciones que se refieren a las zonas secundarias. La gran diferencia es el almacenamiento. Por definición, una zona secundaria no puede ser almacenada dentro del directorio Active Directory, mientras que una zona de rutas internas si.

Las operaciones disponibles en una zona de rutas internas pueden efectuarse mediante la Consola MMC de gestión del DNS:



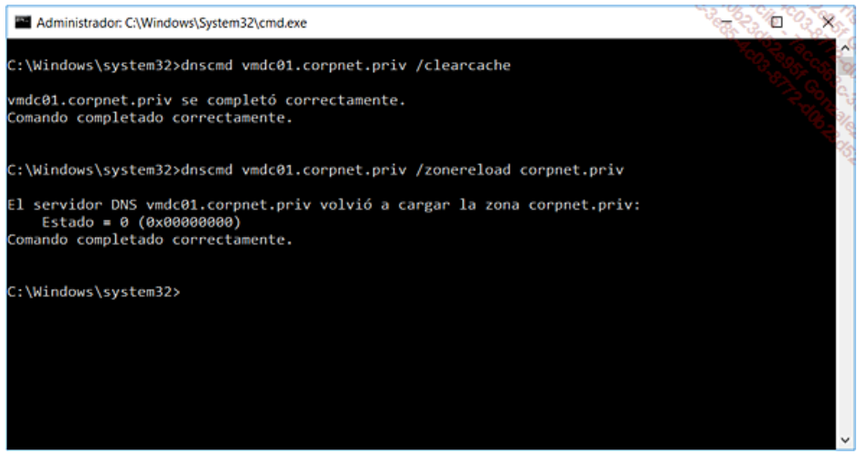
Volver a cargar: la zona de rutas internas se vuelve a cargar a partir del almacenamiento local del servidor DNS que posea una copia de la zona de rutas internas.

Transferir desde maestro: esta operación nos permite forzar el servidor DNS que mantiene la zona de rutas internas comprobar si el número de serie (o número de versión) del registro de SOA de la zona ha cambiado, y luego a realizar una transferencia de zona a partir del servidor maestro de la zona de rutas internas, si es necesario.

Transferir nueva copia de zona desde maestro: la zona de rutas internas se vuelve a cargar empleando una transferencia de zona a partir del servidor maestro cualquiera que sea el valor del número de serie indicado en el registro SOA. Esta operación es por supuesto muy útil cuando una zona de rutas internas se niega a sincronizar de forma normal.

Uso del comando DNSCMD para recargar una zona defectuosa

El comando **dnscmd** dispone de todos los parámetros para realizar todas las operaciones disponibles en la consola de gestión MMC del DNS. Encontraremos a continuación dos operaciones importantes realizadas empleando este comando. La primera operación vacía la cache de resoluciones realizadas por el servidor DNS, mientras que la segunda recarga la zona defectuosa:



El comando `dnscmd` es un comando de sistema incluído con todas las versiones de Windows Server a partir de Windows Server 2008 R2.

En los sistemas que funcionen con Windows Server 2003, la instalación de esta herramienta se realiza mediante la instalación de las herramientas de soporte desde el directorio \Support Tools del CD-Rom de Windows Server 2003. Para obtener ayuda sobre el uso de este comando, escriba `dnscmd /?` en el intérprete de comandos o utilice la herramienta de soporte de Windows.

Para más información sobre el comando `dnscmd`, busque "Administración del servidor empleando Dnscmd" en la ayuda en línea de Windows Server. Aquí encontraremos muchos ejemplos útiles que permitirán escribir scripts para automatizar la gestión y la actualización de la configuración de los servidores DNS.

Reenviadores, zonas de rutas internas y delegación: buenas prácticas

Aunque diferentes sistemas y métodos de resolución parecen dar los mismos resultados, hay sutiles diferencias entre estos métodos. El uso de uno u otro método dependerá de las circunstancias.

Es la razón por la cual es muy importante reconocer las diferencias que les caracterizan para utilizarlos de manera adecuada.

Todos estos mecanismos soportan los estándares RFC. Por lo tanto, podemos encontrar los límites, ventajas y desventajas de los distintos métodos en todos los servidores DNS Windows Server y también sobre las otras plataformas estándar del mercado.

Antes efectuar nuestra elección, podemos consultar el cuadro siguiente. Nos permitirá comprender mejor las mejores prácticas que se esconden detrás de la utilización de los reenviadores condicionales, las zonas de rutas internas y las zonas de delegación.

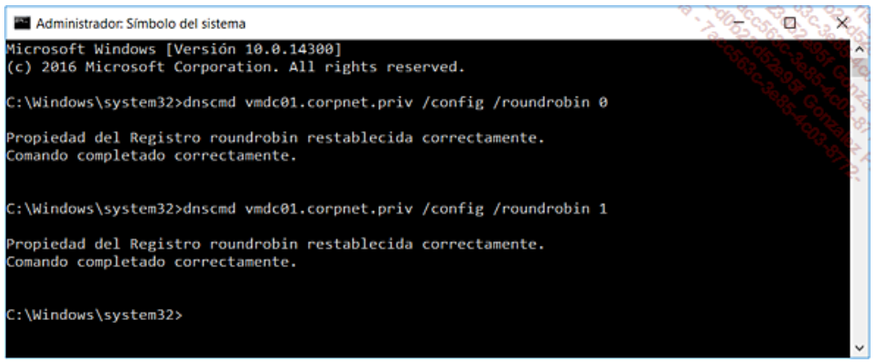
Características de los mecanismos de resolución DNS entre espacios de nombres distintos:

	Reenviadores condicionales	**Zonas de rutas internas**	**Delegaciones**
Espacio de resolución	Cualquier nombre situado en el mismo nivel o a un nivel superior a las zonas locales.	Cualquier nombre situado en el mismo nivel o en un nivel inferior o superior a las zonas locales.	Limitado a los subdominios de las zonas locales.
Consultas DNS utilizadas	El servidor intentará las peticiones iterativas y luego recursivas.	El servidor resuelve la petición o pasa una referencia al cliente para realizar una consulta iterativa (en función de la demanda).	
Seguridad y Firewall	Soporta los firewalls.	Puede verse afectado por los firewalls que impiden a los clientes ponerse en contacto con algunos servidores DNS.	
Nivel de configuración	A declarar en cada servidor DNS.	Replicación automática cuando la integración de Active Directory se utiliza.	Siempre replicada a las NS de la zona principal.
Reconfiguración necesaria	Debe ser reconfigurado cuando los servidores de nombres se añaden a los dominios de destino.	Actualización automática cuando los NS se añaden a la zona de destino.	Debe ser reconfigurado cuando los NS se añaden a la zona de destino.
Soporte de la tolerancia a fallos	Puede ser tolerante a fallos		

Para más información acerca de las elecciones requeridas, buscar «Administración de servidores» en la ayuda en línea de Windows Server 2016. Aquí encontraremos enlaces a las normas de obligado cumplimiento para los temas como la utilización de los servidores primarios y secundarios, la protección del Servicio Servidor DNS, la utilización de servidores de caché, la modificación de los parámetros por defecto del servidor, el uso de reenviadores, el envío de peticiones empleando reenviadores, la actualización de las indicaciones de servidores raíz, así como la administración del servidor empleando el comando Dnscmd incluido en las herramientas de soporte.

Gestión de los nombres multi host

La gestión de los nombres multi host se implementa mediante la activación de la función Round Robin integrada en DNS. Podemos controlar la activación de la función Round Robin empleando la consola de gestión del DNS o mediante el comando dnscmd.



Desactivar/activar la función Round Robin

Caducidad y limpieza de los registros DNS

Los servidores DNS Windows Server soportan las funcionalidades de vencimiento y limpieza. Estas características permiten efectuar la eliminación de los registros de recursos obsoletos que pueden acumularse a lo largo del tiempo en las zonas DNS.

En efecto, con las actualizaciones dinámicas, los registros de recursos son añadidos de forma automática a las zonas durante el arranque de los equipos en la red. Sin embargo, no siempre son eliminados de forma automática cuando los equipos abandonan la red. En efecto, si un equipo que graba su propio registro de recurso de tipo A es luego desconectado de la red de forma incorrecta, el registro de recurso no será siempre eliminado.

Además, si la red está constituida por ordenadores portátiles, esta situación puede repetirse de forma periódica y crear una contaminación importante de las zonas DNS.

Podemos recalcar los siguientes puntos negativos:

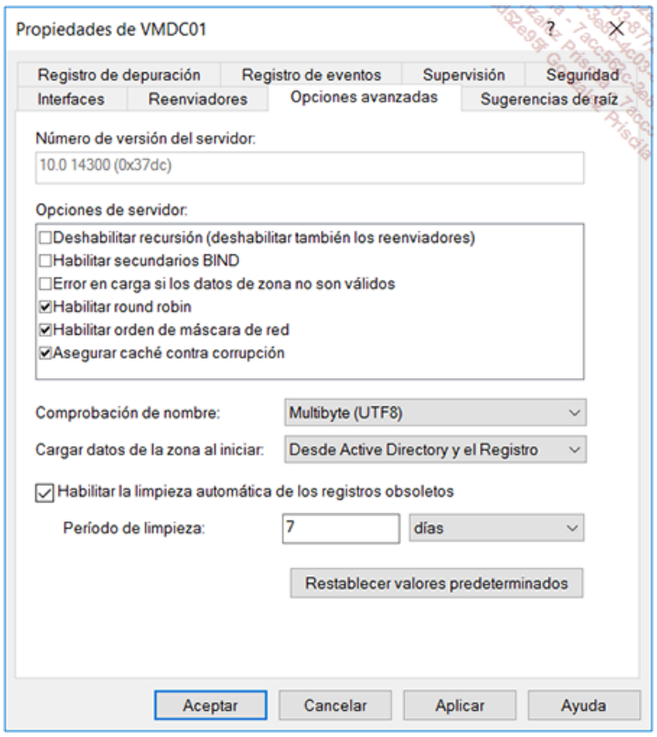
- La presencia de registros de recursos antiguos en las zonas puede acarrear problemas de espacio en disco y sobrecargar las replicaciones y otras transferencias de zona.
- Los servidores DNS que cargan las zonas que contienen registros obsoletos corren el riesgo de utilizar información obsoleta, lo que puede causar problemas de resolución de nombres en la red.
- La acumulación de registros innecesarios puede tener un impacto negativo sobre el rendimiento del servidor DNS.

Importante: por defecto, el mecanismo de vencimiento y limpieza del servidor DNS está desactivado. Preste especial cuidado al hecho de que a partir del momento en que esta función se active, es probable que un cierto número de registros sea destruido. Esta característica no debería estar disponible en los servidores DNS que alojen a zonas que contienen cientos de miles de registros con el objetivo de llevar a cabo una depuración de registros obsoletos.

Si un registro se elimina por accidente, no sólo los usuarios no lograrán resolver las consultas sobre este registro, sino que además la liberación del registro tendrá como consecuencia que cualquier usuario podrá entonces volverlo a crear y declararse propietario. El servidor utiliza un valor de temporizador para cada registro de recurso.

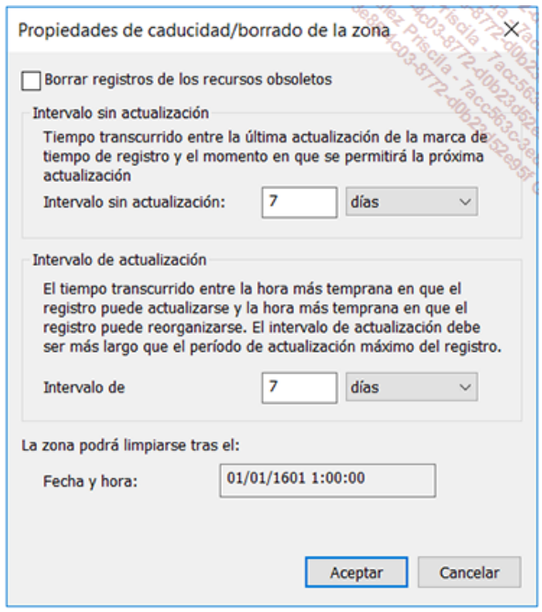
Cuando un servidor DNS desencadena una operación de limpieza, determinará los registros de recursos que caducan y elimina los datos de la zona. Los servidores pueden funcionar de modo que se efectúen las operaciones de forma automática, pero podemos también iniciar la operación actuando sobre las propiedades del servidor.

Para iniciar la limpieza de las zonas DNS, utilice la consola de gestión MMC del DNS. Seleccionamos la opción **Habilitar la limpieza automática de los registros obsoletos** en la pestaña **Opciones avanzadas** del objeto servidor DNS, y luego lo mismo en la o las zonas DNS para las que deseamos activar la función.



Esta opción especifica si puede o no efectuarse una limpieza para el servidor seleccionado. Cuando esta opción está desactivada, la limpieza no puede realizarse y los registros no son eliminados de la base de datos DNS. Este parámetro se aplica tanto a la limpieza automática como manual.

Cada zona DNS tiene la posibilidad de utilizar las funciones de limpieza cuando los registros han caducado. El botón **Caducidad** permite acceder a los diferentes ajustes.

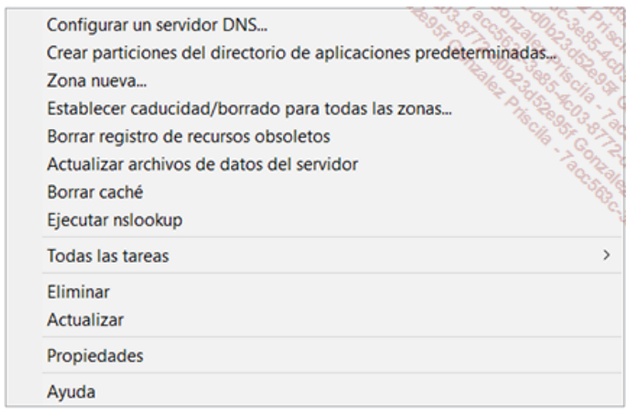


Una vez más, la función no se activa por defecto. Como información, la zona utilizada en nuestros ejemplos es la zona *_msdcs.corpnet.priv*, que gestiona los controladores de dominio del dominio raíz del bosque. Es evidente que esta zona no debe utilizar las funciones de limpieza de los registros DNS.

La eliminación por error de un registro de recurso utilizado por un controlador de dominio puede tener efectos negativos sobre las autenticaciones de los clientes Active Directory o también, y mucho más grave, sobre las replicaciones Active Directory.

Para poder beneficiarse de las operaciones de caducidad y de limpieza, los registros de recursos deben ser añadidos a las zonas DNS de forma dinámica. La pantalla siguiente muestra las diferentes acciones que podemos ejecutar en un servidor DNS Windows Server.

Observe la acción **Establecer caducidad/borrado para todas las zonas...** y la acción **Borrar registro de recursos obsoletos**.

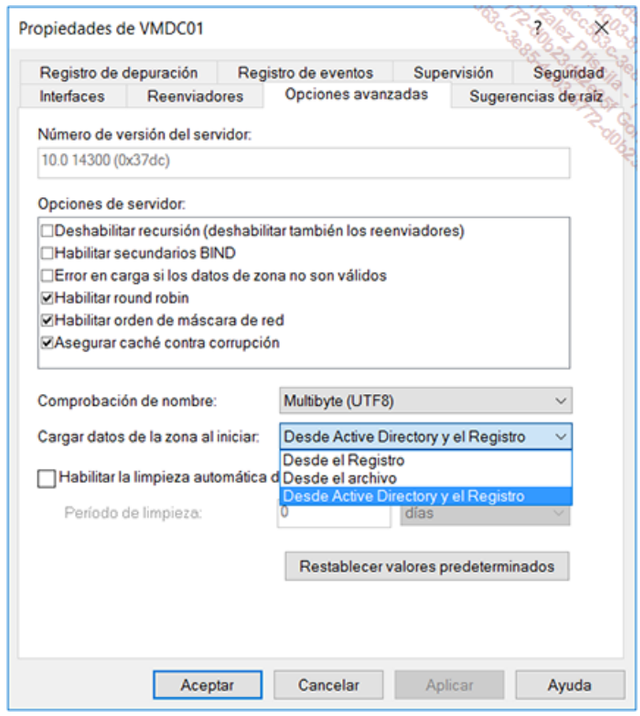


Las propiedades del servidor DNS y limpieza de registros

Tenemos también la posibilidad de arrancar la operación de limpieza empleando la consola de gestión del DNS o mediante el comando `dnscmd /startscavenging`.

Opciones de arranque del servidor DNS

Un servidor DNS de Windows Server nos permite especificar cómo deberá el servicio servidor DNS cargar los datos de la zona inicial. La pantalla siguiente muestra cómo elegir estas opciones.



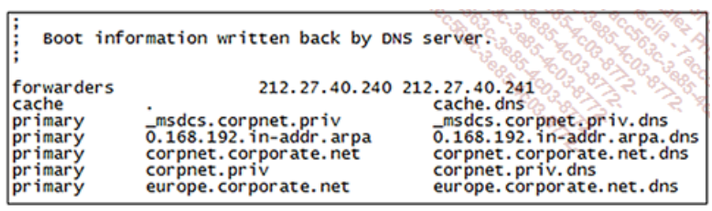
Opción de carga: Desde el Registro

Cuando seleccionamos esta opción, el servidor DNS se basa en los parámetros de carga de las diferentes zonas almacenadas en el registro, como se muestra a continuación.

Opción de carga: Desde el archivo

Cuando seleccionamos esta opción el servidor DNS se basa en los parámetros de carga de las diferentes zonas almacenados en el registro, pero también usa el archivo BOOT de la misma manera que en las implementaciones de servidores DNS de tipo BIND.

La figura siguiente muestra un archivo BOOT.



```
;
;  Boot information written back by DNS server.
;

forwarders              212.27.40.240 212.27.40.241
cache       .                       cache.dns
primary     _msdcs.corpnet.priv     _msdcs.corpnet.priv.dns
primary     0.168.192.in-addr.arpa  0.168.192.in-addr.arpa.dns
primary     corpnet.corporate.net   corpnet.corporate.net.dns
primary     corpnet.priv            corpnet.priv.dns
primary     europe.corporate.net    europe.corporate.net.dns
```

El archivo contiene las declaraciones de las zonas DNS con su tipo, así como algunos parámetros globales del servidor DNS. Las palabras clave más importantes se explican a continuación:

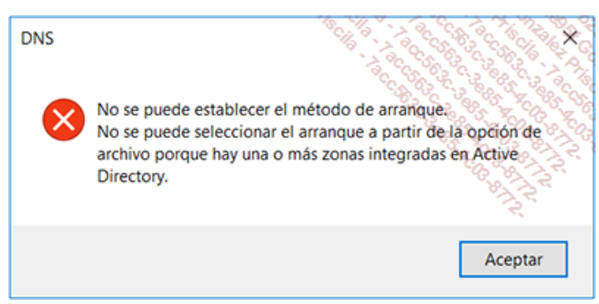
forwarders: este parámetro se refiere a la o las direcciones IP de los servidores DNS a utilizar como reenviadores.

cache: este parámetro indica el nombre del archivo que declara los servidores de dominio raíz.

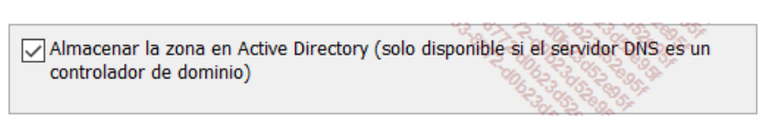
primary: este parámetro indica el nombre de una zona de tipo primaria, así como el archivo de zona asociado.

secondary: este parámetro indica el nombre de una zona de tipo secundaria, así como el archivo de zona asociado.

Observe que para utilizar el modo de arranque **Desde el archivo**, ninguna zona debe estar integrada en el directorio Active Directory. De lo contrario, obtendremos el mensaje de error que aparece a continuación:



Si es imprescindible que un servidor determinado utilice el archivo BOOT y experimentamos este problema, debemos desmarcar la opción**Almacenar la zona en Active Directory** en las propiedades de cada una de las zonas afectadas. Esta opción está disponible a través de las propiedades de la Zona, haciendo clic en la pestaña **General** y pulsando el botón que permite cambiar el modelo de la zona.



Las propiedades de una zona nos permiten gestionar muchas características

Opción de carga: Desde Active Directory y el Registro

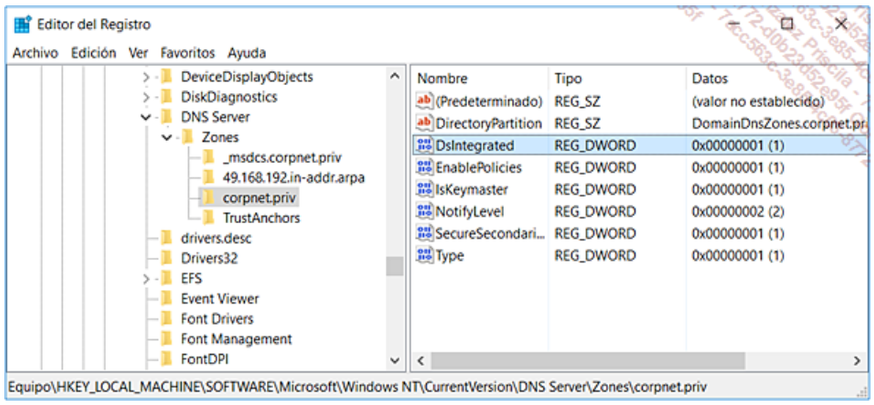
Cuando seleccionamos esta opción, el servidor DNS se basa en los parámetros de carga situados en el registro, sabiendo que el contenido real de las zonas será almacenado en el directorio Active Directory. Esta opción se activa de forma automática cuando el servidor DNS es también un controlador de dominio. Como explicado antes, los parámetros de las zonas siguen almacenados en el registro, pero esta vez el archivo BOOT no es necesario. De hecho, si éste existía de forma previa, se moverá al directorio de respaldo \dns\backup. Un nuevo archivo de información llamado boot.txt lo reemplazará en el directorio \dns.

```
El servidor DNS está arrancando ahora desde el Registro o el
directorio. El servidor DNS ya no leerá el archivo de arranque del
servidor existente al iniciarse. Para cualquier zona nueva que
agregue o cualquier cambio que realice en la información de zona,
debe usar la consola DNS. %nEl anterior archivo de arranque del
servidor DNS se movió al directorio %SystemRoot%\System32\Dns
\backup. %nPara volver a usar un archivo de arranque, use la
consola DNS y configure de nuevo el método de arranque del
servidor. Para obtener más información, consulte la sección sobre
cómo cambiar el método de arranque usado por el servidor DNS en la
Ayuda en pantalla.
```

El archivo de información boot.txt ubicado en el directorio \system32\dns informa que el archivo BOOT no se utiliza

El Registro sigue desempeñando su papel de base de datos de configuración de servicios y otros módulos de Windows. En nuestro caso, podemos observar que para la zona DNS *Corpnet.net*, la integración de Active Directory debe realizarse.

La siguiente imagen muestra esta opción.



*El parámetro **DsIntegrated** especifica la integración en Active Directory*

Recursión de los servidores DNS y protección de los servidores

Por defecto, un servidor DNS de Windows Server soporta la recursión. La recursión es fundamental en la medida en que permite a un servidor DNS de ser capaz de resolver los nombres para los que no dispone de archivos de zona. La pestaña **Reenviadores** de las propiedades del servidor DNS nos permitirá utilizar la recursión para cada uno de los dominios declarados que deban ser objeto de reenvío. Podemos a veces decidir evitar por completo la recursión. La pestaña **Opciones avanzadas** de las propiedades del servidor nos permitirá hacerlo a través de la opción del servidor **Deshabilitar recursión** (deshabilitar también los reenviadores).

1. Bloqueo de los ataques de tipo Spoofing DNS

Los servidores DNS que soportan la resolución de las consultas recursivas pueden ser víctimas de ataques de este tipo. Este tipo de ataque tiene como objeto contaminar la caché del servidor DNS. El ataque se basa en la posibilidad de predecir el número de secuencia de la consulta DNS. Así, el atacante puede presentar una solicitud de resolución para el equipo www.microsoft.com y mientras que el servidor determina la respuesta a esta consulta, el atacante engaña a su servidor con una "respuesta malintencionada". Esta "respuesta malintencionada" incluirá por supuesto una "dirección IP falsa" y también una duración de vida (*Time to Live*) muy alta. Una vez detectado el ataque, la solución será purgar el o los registros ilegales de la caché del servidor DNS.

Por supuesto, desactivar las consultas recursivas nos protegerá de este tipo de ataque. Sin embargo, no podremos pasar consultas recursivas si los usuarios de este servidor deben resolver dominios no gestionados. En efecto, cuando la recursión se encuentra desactivada por completo, el servidor DNS solo es capaz de resolver los nombres en relación con las zonas DNS que alberga.

2. Bloqueo de los ataques de tipo Spoofing DNS en los servidores de tipo Internet

Se recomienda desactivar la recursión en los servidores DNS disponibles en Internet. De esta manera, el servidor será capaz de responder a las peticiones de otros servidores DNS, pero impedirá a los clientes de Internet utilizar el servidor DNS para resolver otros nombres de dominio en Internet. Como se recordará, también hemos visto antes que un servidor DNS en el que la recursión se encuentra por completo desactivada al nivel del servidor no puede utilizar los reenviadores .

Resumen de los roles de los servidores DNS

Acabamos de ver que el servidor DNS puede ser configurado para trabajar de diferentes maneras y utilizarse en diferentes situaciones. Estas diferentes funciones se resumen a continuación:

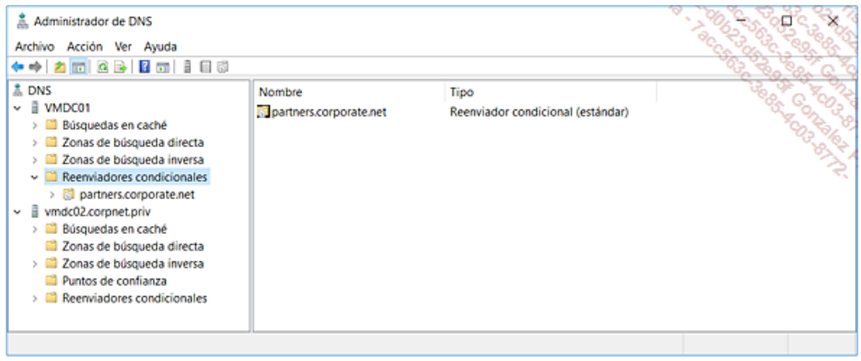
Servidor de caché: el servidor de caché tendrá sólo el efecto de reducir el tráfico en una red extendida. El servidor soporta las resoluciones de los clientes y los resuelve sin poseer ninguna zona, por lo tanto sin ninguna sobrecarga de replicación.

Servidor reenviador solo: un servidor configurado para utilizar reenviadores intenta resolver el nombre solicitado basado en su caché local, las zonas almacenados de forma local y luego empleando los reenviadores especificados. Si ninguno de estos medios permite la resolución, entonces se emplea la recursión estándar. Contamos con la opción de desactivar las resoluciones recursivas para evitar estas búsquedas tras el fallo de los reenviadores. En este caso, el servidor DNS solo puede contar con su caché, sus zonas y el uso exclusivo de sus reenviadores.

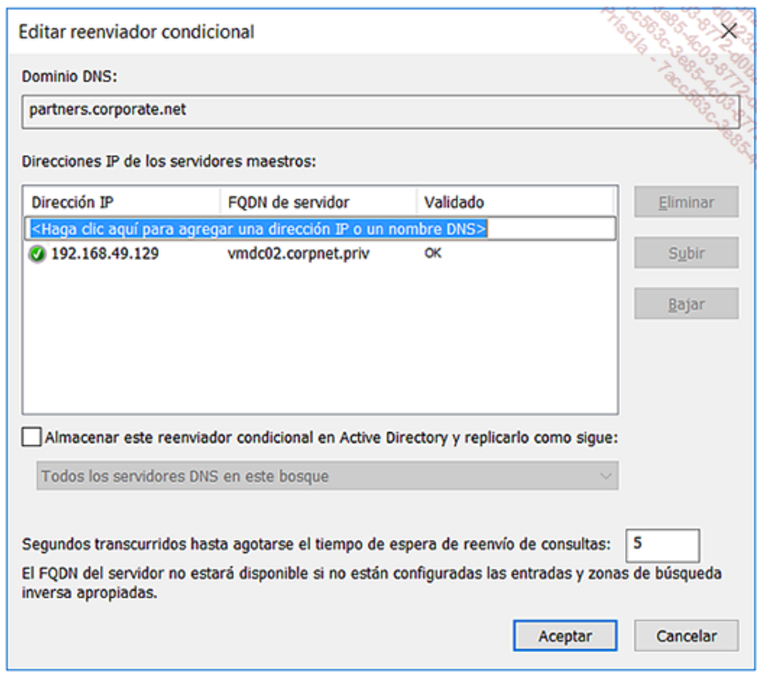
El uso correcto de los reenviadores consiste, por supuesto en permitir que los servidores DNS de su espacio privado resuelvan el espacio DNS de Internet. Seleccione uno de sus servidores DNS para hacer uso de los reenviadores. Luego configure su firewall para que sólo este servidor esté autorizado a transmitir y recibir tráfico DNS de Internet (puertos TCP y UDP 53).

Servidor reenviador condicional: cuando un servidor configurado para utilizar los reenviadores puede consultar uno o varios reenviadores para resolver el nombre solicitado, el reenviador condicional redirigirá las peticiones de resolución en función del nombre de dominio DNS de la petición.

Como se ha visto antes, la configuración es muy simple, ya que basta con declarar las direcciones TCP/IP de los servidores DNS que soportarán el dominio especificado para cada dominio de resolución redirigido.



Declaración de reenviadores específicos en función de los dominios



Modificación de un reenviador condicional

Los servidores DNS que funcionan con Windows Server permiten comprobar la disponibilidad real de los servidores maestros. Tenga en cuenta la opción de almacenar esta información en Active Directory para garantizar una utilización de estos parámetros para todos los servidores DNS, así como el tipo de reenviador condicional (estándar o integrado en Active Directory).

Comandos de gestión del servicio DNS

La estimación de costos de administración y mantenimiento de los servidores DNS indispensables para el buen funcionamiento del directorio Active Directory es de manera teórica difícil de cuantificar. Sin embargo, la experiencia demuestra que la utilización del servicio DNS no requiere de recursos humanos y materiales adicionales.

Esto no significa que no sea necesario disponer de recursos, conocimientos y herramientas necesarias para la correcta administración y supervisión de este importante servicio. Así podremos utilizar los comandos y herramientas como NSLookup, DNSCmd, DNSLint y Netdiag. Estas herramientas y su uso correcto se presentan a continuación.

1. El comando ipconfig

a. Gestión de la caché del cliente DNS y los registros dinámicos

Con respecto a las anteriores versiones de este comando, esta herramienta incluye ahora opciones de línea de comando adicionales destinadas a facilitar la resolución de problemas y el soporte de los clientes DNS. Así, además de las funciones conocidas bajo Windows NT, dispondremos de la posibilidad de consultar y reconfigurar la caché de resolución del módulo cliente DNS así como renovar la inscripción del cliente DNS. Estas opciones del comando ipconfig se listan a continuación.

ipconfig /displaydns

El comando `ipconfig /displaydns` muestra la caché de resoluciones, que está implementada dentro del servicio cliente DNS.

El contenido de la caché del cliente DNS incluye las entradas pre-cargadas a partir del archivo %Systemroot%\system32\drivers\etc\Hosts del equipo local, así como las grabaciones de recurso recientemente obtenido a través de las solicitudes de nombres ya resueltas. Estos datos son luego utilizados por el servicio cliente DNS para resolver de forma directa los nombres buscados con frecuencia antes de interrogar realmente a los servidores DNS configurados.

Si resultara necesario añadir entradas dentro del archivo **hosts** local, estas entradas serán añadidas de forma automática a la caché DNS.

Visualización de la caché y registros de resoluciones negativas

No olvide tampoco que la caché de resolución DNS incluye en caché negativa los nombres DNS no resueltos. Estas entradas negativas están en caché durante una corta duración para que el servidor DNS no sea consultado de nuevo. Esta característica tiene por objeto garantizar que los servidores DNS no puedan recibir miles de peticiones por segundo por parte de una aplicación mal codificada, o incluso malintencionada. De esta manera, las resoluciones negativas en caché garantizan de la mejor manera posible la disponibilidad del servicio de resolución en su totalidad.

La clave de registro siguiente nos permitirá configurar el tiempo (en segundos) durante el cual una entrada permanecerá almacenada en la caché DNS: **HKLM\SYSTEM\CurrentControlSet\Services\DnsCache\Parameters\NegativeCacheTime**.

Es un valor de tipo REG_DWORD comprendido entre 0x0 y 0xFFFFFFFF. El valor por defecto de producción en el sistema se define en 0x12C, es decir, 300 segundos, o sea 5 minutos. Una vez la duración especificada expira, el servicio cliente DNS elimina el registro de la caché.

Con respecto a la duración de vida de las resoluciones negativas, el valor por defecto de la vida de los registros negativos no requiere ser modificado a posteriori. Además, tenga en cuenta que este parámetro no se aplicará a los registros de tipo SOA. El valor del período de tiempo para los registros SOA negativos es determinada por el parámetro específico **NegativeSOACacheTime**. Por defecto, el valor de**NegativecacheTime** se encuentra definido en 0x78, es decir 120 segundos, o sea 2 minutos.

No se requiere disponer de la condición de administrador para efectuar esta operación. Por lo tanto, por razones de seguridad se recomienda llevar a cabo esta tarea como un usuario normal.

ipconfig /flushdns

El comando `ipconfig /flushdns` permite vaciar y limpiar la caché de resolución del cliente DNS.

Cuando sea necesario, nuestras búsquedas acerca de la resolución de problemas DNS nos podrán llevar a utilizar este comando para excluir las entradas de caché negativas molestas.

¡Observe! Esta operación vacía toda la caché. Así, todas las demás entradas añadidas de forma dinámica también serán borradas. En cambio, el reinicio de la caché no elimina las entradas precargadas a partir del archivo Hosts. Para eliminar estas entradas, debemos borrarlas del archivo hosts.

¡El comando `ipconfig` existe desde las primeras versiones de Windows 95! Los parámetros `/displaydns` y `/flushdns`aparecieron con Windows 2000. El comando `ipconfig /?` lista de todos los parámetros que hoy en día son muy numerosos.

b. Renovación de la inscripción del cliente DNS

ipconfig /registerdns

Este comando será muy útil para renovar la inscripción del cliente DNS tras un cambio de configuración, o también para resolver un problema de fallo de la inscripción o actualización dinámica entre un cliente y un servidor DNS, sin reiniciar el equipo. Esta última observación se refiere en especial a los servidores.

En la medida en que un ordenador puede estar equipado con varias tarjetas de red, el hecho de no especificar la misma provocará la grabación de las direcciones IP presentes en todas las tarjetas en el nombre declarado como nombre completo principal del equipo. Si desea grabar solo una tarjeta en particular, entonces debemos ingresar el comando `ipconfig /registerdns [tarjeta]` donde `tarjeta` es el nombre de una tarjeta de red específica instalada en el equipo en el que desee renovar o actualizar las inscripciones.

Los nombres de todas las tarjetas que pueden ser utilizadas en un equipo determinado serán mostrados cuando se escribe sin parámetros el comando `ipconfig`.

El comando ipconfig /registerdns y las concesiones DHCP

Acabamos de ver que el comando `ipconfig /registerdns` permite iniciar de forma manual el registro dinámico de nombres DNS y

direcciones IP. Sin embargo, debemos tener en cuenta que este comando refresca también todos las concesiones DHCP.

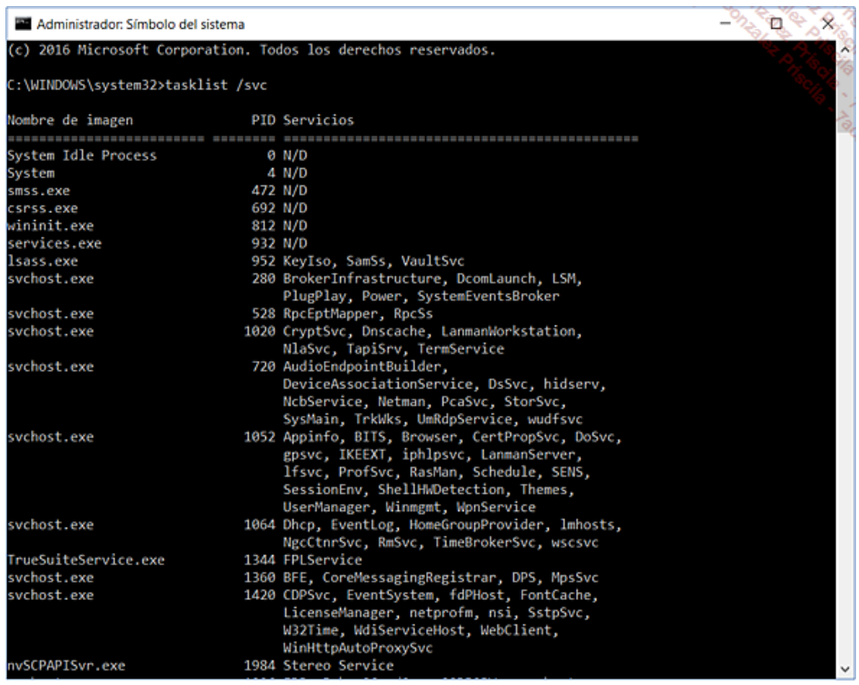
A partir de Windows 2000, es el servicio Cliente DHCP el que se emplea para realizar la inscripción y actualización dinámica que el equipo utiliza de un servidor DHCP o una configuración TCP/IP estática. Esta implementación no ha cambiado con las últimas versiones de Windows 10 o Windows Server 2016.

En el caso en que nos viéramos obligados a resolver un problema de fallo de inclusión dinámica del DNS para un equipo y sus nombres DNS, debemos comprobar que la causa del problema no es una de las siguientes:

- La zona para que la cual se solicita la actualización o la inclusión del cliente no acepta actualizaciones dinámicas.
- Los servidores DNS configurados en el cliente no soportan el protocolo de actualización dinámica del DNS.
- El servidor DNS -primario o integrado en Active Directory- de la zona denegó la solicitud. Por lo general, los permisos del cliente son insuficientes y no le permiten actualizar su propio nombre.
- El servidor o la zona hospedada por el servidor no están disponibles. En este caso, podría tratarse de diversos problemas, como la falta de disponibilidad del sistema o de la red.

Con respecto a los registros DNS dinámicos, actualizaciones de la caché y servicios Cliente DHCP y Cliente DNS integrados en el sistema

El servicio cliente DHCP es responsable de la inscripción y las actualizaciones de las direcciones IP y los registros DNS para el equipo. Asi mismo, aunque un equipo esté provisto de una configuración TCP/IP estática, no debemos detener este servicio. En el caso de que este servicio sea detenido, el equipo presentaría dos tipos de problemas. Por una parte, si espera una configuración IP dinámica, no la recibirá, y por otra parte, no va a ser capaz de realizar las actualizaciones de DNS dinámicas necesarias. En versiones anteriores a Windows 8, los servicios Dhcp y Dnscache estaban implementados en el mismo módulo svchost.exe. El comando `tasklist /svc` de la imagen -siguiente muestra que ahora estos dos componentes están aislados en dos procesos -diferentes (PID 1020 y 1064).



Procesos con los servicios Cliente DHCP y cliente DNS

c. Nuevas opciones del comando ipconfig

Las versiones de Windows 7 / Windows Server 2008 R2 y posteriores incluyen nuevas funcionalidades IP que tienen necesidad de modernizar el conjunto de comandos de sistema como el comando ipconfig o el comando Netsh. Los parámetros relativos al comando Ipconfig y su objeto se listan a continuación:

- `ipconfig /allcompartments`: muestra información para todos los compartimentos.
- `ipconfig /release`: libera a la dirección IPv4 para la tarjeta especificada.
- `ipconfig /release6`: libera a la dirección IPv6 para la tarjeta especificada.
- `ipconfig /renew`: renueva la dirección IPv4 para la tarjeta especificada.
- `ipconfig /renew6`: renueva la dirección IPv6 para la tarjeta especificada.

Con respecto a los compartimentos de enrutamiento (Routing compartments)

Windows Server 2008 introdujo una nueva implementación del protocolo TCP/IP (Next Generation TCP/IP). La pila de protocolos TCP/IP que equipaba antes a Windows XP y Windows Server 2003 se desarrolló a comienzos de los años 90 y ha sufrido muchas modificaciones para seguir la evolución del protocolo. El protocolo TCP/IP NextGen es una nueva arquitectura y un rediseño completo de todas las pilas IPv4 y IPv6. Una de las muchas funcionalidades implementadas se conoce como "compartimentos de enrutamiento".

Un compartimiento de enrutamiento es una combinación de un conjunto de interfaces asociadas a una sesión de usuario dado que disponen de su propia tabla de enrutamiento privada. Así, un equipo puede tener varios compartimentos de enrutamiento, aislados todos entre sí, sabiendo que una interfaz solo puede pertenecer a un único compartimiento. Esta característica es muy poderosa, ya que permite evitar el tráfico no deseado entre interfaces virtuales como VPNS, las sesiones de administración a través de RDP (servicios de escritorio remoto), etc.

Para más información, busque "Next Generation TCP/IP Stack" en el sitio Microsoft Technet o utilice el siguiente enlace:http://technet.microsoft.com/enus/network/bb545475.aspx

2. El comando nslookup

Uso del comando nslookup para comprobar los registros de los controladores de dominio Active Directory

El comando **nslookup** es un comando que se utiliza con frecuencia para diagnosticar posibles problemas de resolución de nombres de host

dentro de la infraestructura DNS. Es en particular potente para enviar a un determinado servidor DNS solicitudes de resolución de nombres y presentar a su vez las respuestas detalladas a las consultas. El comando **NSLookup** presenta la particularidad de poder funcionar en modo interactivo o en modo no interactivo.

En modo interactivo: cuando usamos este modo, recibimos de forma dinámica los resultados relativos a los comandos. Por supuesto, este método es el más útil cuando debemos escribir varios comandos para realizar una serie de operaciones.

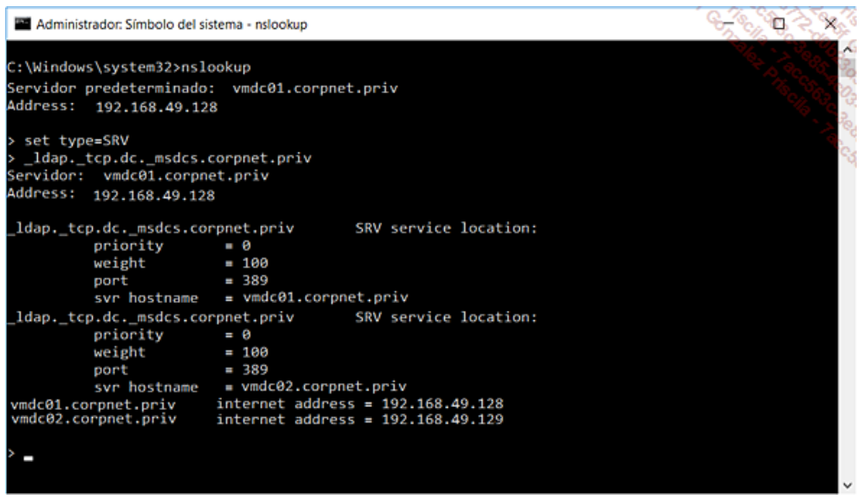
En modo no interactivo: cuando usamos este modo, podemos pasar parámetros en la misma línea de comando y así realizar operaciones que podrán ser luego insertadas en un script de administración. En este caso, el retorno del comando pasado podrá redirigirse a un archivo. Por ejemplo, podemos usar el siguiente procedimiento para controlar los registros de controladores de dominio:

Escriba el comando `NSLookup` en la línea de comandos.

Escriba `set q=SRV`. También podemos usar la sintaxis `set type=SRV`.

Escriba `_ldap_tcp.dc._msdcs.Nombre_dominio_Active_Directory`.

El retorno de este comando muestra todos los registros SRV para el nombre solicitado _ldap_tcp.dc._msdcs.corpnet.priv, es decir, todos los controladores del dominio requerido. En función del resultado, podremos determinar si se requiere una acción adicional. En nuestro ejemplo, el dominio corpnet.priv dispone de dos controladores de dominio (vmdc01 y vmdc02.corpnet.priv).



Filtrado de los registros de tipo SRV

Si este es el caso, la solución consiste en corregir los registros erróneos o faltantes. Para añadir los registros de recursos de tipo SRV necesarios para un controlador de dominio determinado, abrimos el archivo Netlogon.dns. Este archivo se crea de forma automática por el Asistente para Instalación de Active Directory en el momento en que el servidor es elevado al rol de controlador de dominio.

Está situado en la ubicación: %SystemRoot%\System32\ Config\Netlogon.dns

Las operaciones realizadas solo prueban la disponibilidad de los registros deseados. Se trata de una operación normal que no requiere disponer de privilegios de administrador. La mejor práctica consiste en no utilizar esa identidad.

En algunos casos, el procedimiento anterior reenvía varias fechas de vencimiento sucesivas. Esto ocurrirá cuando los registros de recursos inversos no estén presentes. En este caso, el administrador deberá verificar la presencia de la zona de búsqueda inversa para la red o redes IP utilizadas por los controladores de dominio, así como las opciones de registro dinámico en la zona.

3. El comando DNSCmd

Como la mayoría de las herramientas utilizadas por el personal de soporte, el comando DNSCmd es un comando sistema que soporta la mayoría de las tareas de administración incluidas en la consola de administración MMC Administrador DNS.

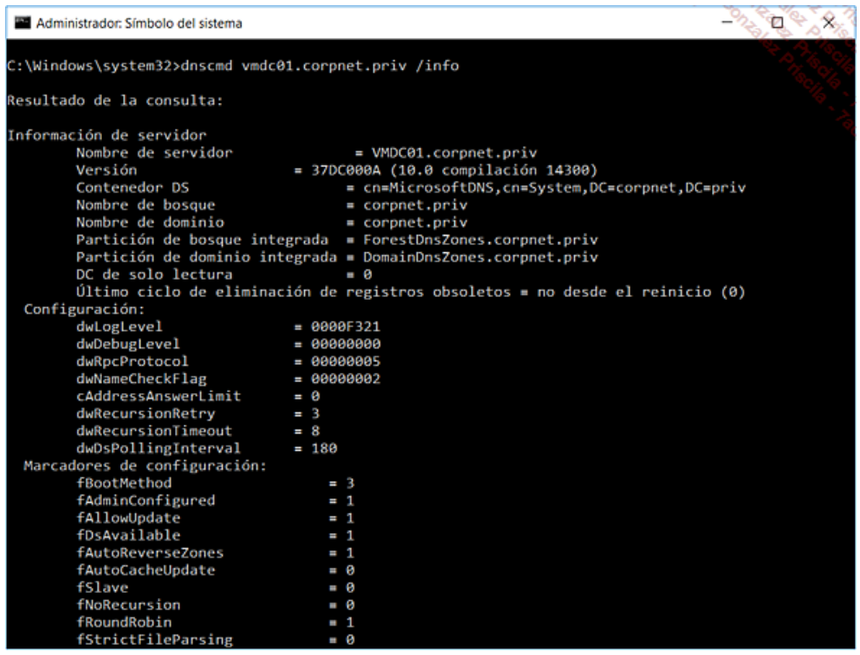
Este comando es muy interesante cuando es necesario realizar una operación especial en los diferentes servidores DNS. Será en particular eficaz para automatizar las tareas de administración en varios servidores DNS, como podría ser el caso en un entorno Active Directory de gran tamaño con decenas de controladores de dominio que dispongan del rol servidor DNS o también en el caso de un proveedor de servicios de Internet.

El administrador podrá utilizar el comando DNSCmd de dos maneras: o bien para la administración local o remota, o en el marco de archivos por lote genéricos transferidos y ejecutados de forma remota. De hecho, todos los escenarios de ejecución son posibles y nos permitirán gestionar la mayoría de los casos que se presenten.

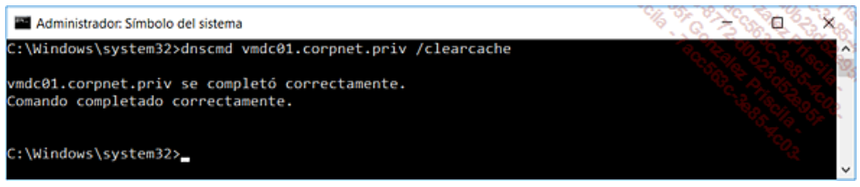
El comando DNSCmd se utiliza de la siguiente manera:

```
dnscmd Nombre_de_Servidor Comando [Parámetro Comando]
```

Por ejemplo, el comando `dnscmd vmdc01.corpnet.priv /info` retornará una página completa de parámetros tales como la información general del servidor, la configuración de los mecanismos DNS, la configuración de las opciones de limpieza de los registros de recursos, la utilización de los reenviadores, de la recursión, etc.



Otro comando útil es el comando `dnscmd Nombre_de_Servidor /clearcache`.



Vaciado de cache DNS en caso de corrupción

El parámetro `/clearcache` permite purgar de forma completa el contenido de la -caché del servidor DNS y eliminar así los registros inválidos.

No confunda la caché del servidor DNS con la caché del cliente DNS. La caché del servidor puede ser purgada empleando el comando`dnscmd /clearcache` mientras que la caché del cliente lo será empleando el comando `ipconfig /flushdns`.

En el mismo orden de ideas, los privilegios necesarios para estas dos operaciones no son idénticos.

Para realizar el borrado de caché del servidor DNS, se debe ser miembro del grupo de administradores en el equipo local o haber recibido, por delegación, los permisos necesarios. Observe que si el equipo es miembro de un dominio, los miembros del Grupo Administradores del dominio pueden efectuar esta operación.

Para realizar el borrado de caché del cliente DNS se requiere disponer de privilegios de administración.

La lista siguiente presenta los parámetros del comando DNSCmd más usados:

`/primary /secondary /stub /cache /autocreated` :filtrado del tipo de zona a mostrar.

`/primary`: muestra todas las zonas de tipo principal o Active Directory.

`/secondary`: muestra todas las zonas secundarias.

`/stub`: muestra todas las zonas de rutas internas.

`/cache`: muestra todas las zonas presentes en la caché del servidor DNS.

`/auto-created`: lista las zonas creadas de forma automática durante la fase de instalación del servidor DNS.

`/forward /reverse`: permite filtrar la visualización de las zonas de un tipo determinado.

Para mostrar los muchos comandos y parámetros de DNSCmd, escriba en la línea de comando `DNSCmd /?`.

4. El comando DNSLint

El comando DNSLint es un comando muy útil que se incluyó en sus inicios con las herramientas de soporte de Windows Server 2003. A día de hoy, este comando está disponible como descarga desde del sitio de Microsoft. DNSLint es una herramienta que permite diagnosticar los problemas relacionados con la resolución de nombres de host, los nombres de dominio, la delegación de los dominios y también aspectos relativos a los registros SRV necesarios para el buen funcionamiento de los servicios de directorio Active Directory.

En efecto, este comando posee argumentos que nos permitirán verificar los registros de recursos utilizados específicamente para la replicación de los controladores de dominio de Active Directory.

Una ventaja adicional en comparación con otros comandos es que permite producir directamente informes en formato HTML. Podemos así presentar una verificación completa de la implementación del sistema de resolución DNS dentro de un bosque Active Directory. Además, DNSLint nos permite ayudar a la resolución de problemas de autenticación de clientes dentro de un dominio Active Directory, comprobando los registros SRV para los protocolos LDAP, Kerberos, así como para los catálogos globales.

Por ejemplo, el comando a utilizar para crear un informe es:

`dnslint /ad <dirección_ip_controlador_de_dominio> /s <dirección_ip_servidor DNS_>`

El parámetro `/ad` especifica que los registros concretos del directorio Active Directory deben ser analizados, el parámetro `/s` para solicitar el servidor DNS especifico. Observe que el parámetro `/s` es obligatorio si queremos hacer una prueba de Active Directory con el parámetro `/ad`. Además, el servidor DNS especificado con el parámetro `/s` deberá ser autoridad para el subdominio **_msdcs.<Raíz_del_bosque>**.

En el caso de que queramos probar los registros de recursos DNS necesarios en el directorio Active Directory del servidor local, podremos añadir al parámetro `/ad` el parámetro específico `/localhost`.

Esta prueba permite comprobar que el servidor local es capaz de resolver los registros necesarios para las replicaciones Active Directory.

Además de las funciones de prueba para Active Directory, DNSLint es también capaz de verificar el buen funcionamiento de las delegaciones de dominio y controlar un conjunto de registros de recursos DNS. Para efectuar estos dos tipos de operaciones podremos utilizar de forma respectiva los parámetros `/D y /ql`.

Para más información sobre los diferentes parámetros disponibles con el comando DNSLint, teclee `DNSLint /?`.

5. El comando Netdiag

El comando Netdiag es bien conocido por los administradores de Windows. En principio distribuido con las Herramientas de Soporte de Windows Server 2003, este comando ha sido substituido y no deberá utilizarse en adelante.

El comando Netdiag apareció con las herramientas de soporte proporcionadas en principio con Windows Server 2000. Con Windows Server 2008 y versiones posteriores, la mayoría de estas herramientas se han integrado en el sistema, eliminando la necesidad de tener que proporcionar un conjunto de herramientas adicionales. Observe que el comando de sistema Dcdiag incluye la mayoría de las opciones de pruebas de red contenidas en Netdiag.

Supervisión del servicio DNS

El servicio DNS debe controlarse, al igual que los otros servicios fundamentales. Esta supervisión se basa en el uso de la consola Monitor de rendimiento. Esta consola nos permite invocar un conjunto de contadores de rendimiento especializados en la supervisión del servicio de servidor DNS. Como los servidores DNS desempeñan un papel central en la mayoría de las infraestructuras, la supervisión de los servidores DNS nos permitirá reaccionar de manera proactiva empleando los siguientes elementos:

- La disposición de una base de rendimiento de referencia. Podemos utilizar esta información para identificar los potenciales fallos de rendimiento y así valorar las posibles actualizaciones de hardware o software necesarias para mantener o mejorar el nivel de prestaciones.
- La disposición de registros especializados para ayudar a resolver fallos y optimizar el servicio DNS.

Estos dos importantes puntos se tratan a continuación.

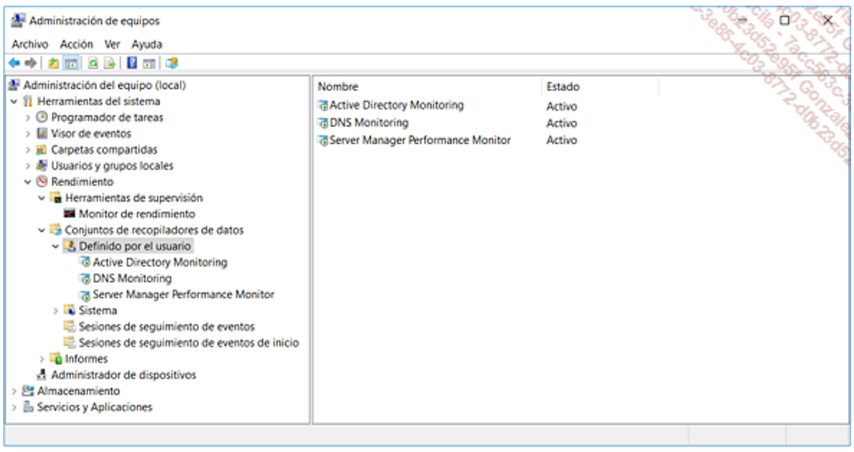
1. Definición de una base de referencia

La siguiente tabla muestra los contadores que podemos (¡O debemos!) -seleccionar para poder controlar correctamente el servicio DNS.

Contadores de supervisión de DNS y marco de utilización:

Contadores de rendimiento	Tipo de datos recopilados	Evaluación	Estrategia de supervisión
Actualizaciones dinámicas rechazadas	Número total de actualizaciones dinámicas rechazadas por el servidor DNS.	Un número importante de rechazos por parte de un servidor DNS seguro puede significar que equipos no autorizados tratan de realizar actualizaciones dinámicas.	Cualquier incremento debe iniciar un análisis detallado de esta actividad dudosa.
Peticiones recursivas por segundo	Número medio de peticiones recursivas recibidas por el servidor DNS en un segundo.	Este contador permite vigilar la actividad del servidor DNS en términos de carga de resolución de nombres.	Cualquier variación importante debe ser objeto de una acción de control de la actividad.
Peticiones AXFR enviadas	Número total de peticiones de transferencias de zona completa enviadas por el servidor DNS secundario.	El servidor secundario que mantiene una zona secundaria demanda transferencias de zona. Cuando esta cifra es elevada un número de cambios importantes se efectúan en la zona primaria.	Si este contador se incrementa de forma importante con respecto a la base, puede ser necesario revisar el número de modificaciones autorizadas, así como la metodología utilizada.

Estos contadores serán utilizados con los componentes de supervisión y conexión habituales de Windows Server.

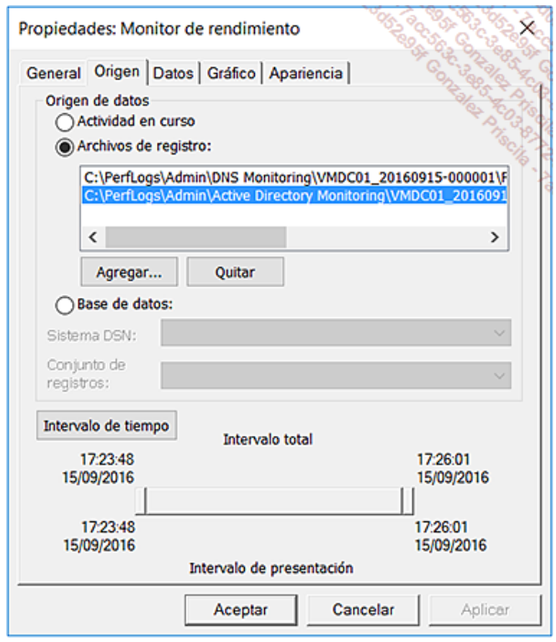


Registro de logging para la supervisión del servicio DNS

En este ejemplo, el comportamiento del equipo está supervisado mediante el registro por defecto Server Manager Performance Monitor que se inicia a través de la opción **Reiniciar el contador de rendimiento** del administrador de servidor de Windows Server 2016. Los otros registros de análisis de Active Directory Monitoring y DNS -Monitoring se añaden para la supervisión de los servicios respectivos.

Por lo general, la consola preformateada Monitor de rendimiento se encuentra accesible de forma directa a través del menú **Inicio - Todos los programas - Herramientas de administración**. Sin embargo, si desea insertar este componente en una consola personalizada, puede proceder de dos formas diferentes: añadir el componente **Monitor de rendimiento** o bien utilizar la opción **Control ActiveX/System Monitor Control**.

Este componente es en particular interesante para tener una visión instantánea de la actividad, pero sobre todo para analizar los registros durante un período de tiempo que podemos definir. Para acceder a la ventana de configuración, puede usar la opción **Propiedades del monitor de rendimiento**.



Selección del intervalo de análisis dentro del registro

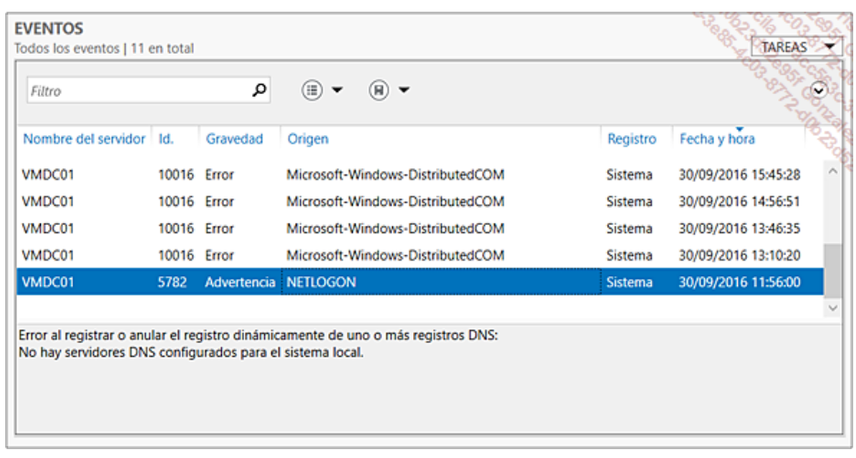
Podremos añadir otros contadores muy interesantes en función del contexto de uso del servidor DNS. De esta forma podremos por ejemplo, optar por incluir en nuestro registro de supervisión, los contadores de rendimiento que figuran a continuación:

- Total de las consultas recibidas y total de consultas recibidas/s;
- Total de respuestas enviadas y Total de respuestas enviadas/s;
- Consultas recursivas y Consultas recursivas/s;
- Tiempo agotado de envíos recursivos y Tiempo agotado de envíos recursivos/s;
- Errores de consultas recursivas y Errores de consultas recursivas/s;
- Notificaciones enviadas - Solicitudes de transferencia de zona recibidas;
- Errores en las transferencias de zona;
- Consultas AXFR recibidas - AXFR enviadas;
- Consultas IXFR recibidas - IXFR enviadas - Notificaciones recibidas;
- Solicitud de transferencia de zona SOA;
- Actualizaciones dinámicas recibidas y Actualizaciones dinámicas recibidas/s;
- Actualizaciones dinámicas rechazadas;
- Actualizaciones dinámicas en cola;
- Actualizaciones dinámicas seguras recibidas y Actualizaciones dinámicas seguras recibidas/s;
- Error de actualización segura.

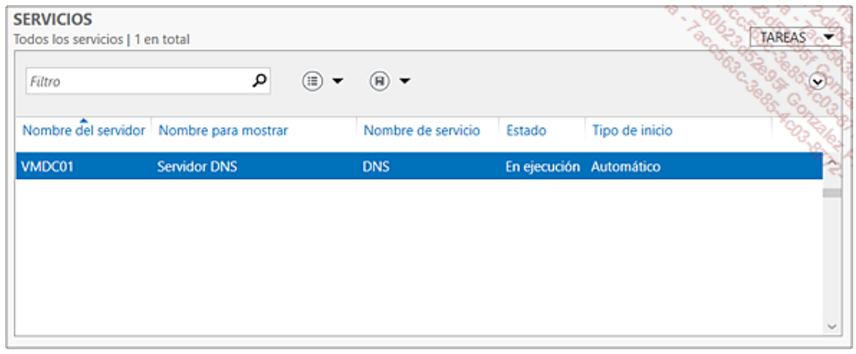
2. Uso de la consola de Administrador del servidor

Windows Server 2016 incorpora la nueva consola de administración de servidor **-Administrador del servidor**. Esta consola facilita el conjunto de las tareas de gestión y seguridad de los roles de servidor proporcionando un punto central para acceder a la información del sistema y los distintos estados de funcionamiento del servidor. A continuación presentamos de forma rápida las principales características:

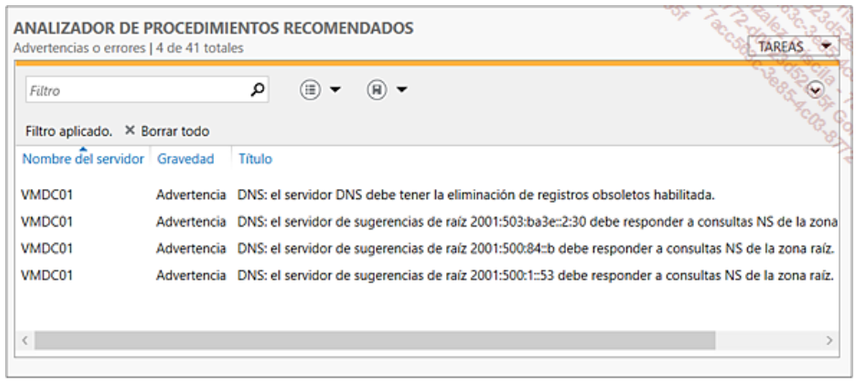
- Visualización y cambio de roles y funciones instaladas en el servidor.
- Gestión de los servicios operativos.
- Gestión de roles.
- Resumen de los estados, situaciones críticas y ayuda para el análisis y la solución de problemas con acceso a las distintas fuentes de información (buenas prácticas, recomendaciones, artículos Microsoft Technet).



Supervisión del rol «Servidor DNS» empleando el Administrador del servidor.



La figura siguiente ilustra la consola **Administrador del servidor** para poner en práctica de la mejor manera posible los servicios DNS de Windows Server 2016. Aquí encontraremos los mejores enlaces para aplicar las configuraciones recomendadas, las diferentes tareas de administración o mantenimiento, así como las mejores prácticas a observar.



Mantenimiento del rol «Servidor DNS» empleando el Administrador del servidor.

3. Utilización de los registros de eventos

Por defecto, los servidores Windows Server graban los eventos en tres tipos de registros.

- **El registro Aplicación**: este registro contiene los eventos grabados por las aplicaciones o programas.
- **El registro de Seguridad**: este diario se registran los eventos como los intentos válidos y no válidos de inicio de sesión, así como los acontecimientos relacionados con la utilización de un recurso.
- **El registro de sistema**: este registro contiene los eventos registrados por los componentes de sistemas de Windows. El fracaso de la carga de un controlador o de otro componente del sistema durante el arranque será consignado en este registro.

Sin embargo, cuando el equipo está configurado para albergar ciertos servicios adicionales, estarán disponibles registros adicionales. De esta forma, si el equipo está configurado como controlador de dominio, se crean dos registros adicionales.

- **El registro del Servicio de directorio Directory Service**: este registro contiene los eventos registrados por los servicios de dominio de Active Directory (Rol AD DS).
- **El registro del Servicio de replicación DFS**: este registro contiene los eventos registrados por el Servicio de replicación de archivos DFSR. Tenga en cuenta que con las versiones anteriores de Windows Server -de 2008 a 2012 R2, el servicio de replicación de archivos FRS (NTFRS) se utilizaba por defecto. Aunque el servicio de replicación DFRS haya hecho su aparición en Windows Server 2003 R2, es sólo con los controladores de dominio Windows Server 2008 y posteriores, que DFSR se puede utilizar para replicar el volumen SYSVOL - siempre que se utilice el nivel funcional de Dominio Windows Server 2008. La migración de NTFRS a DFSR puede realizarse con la herramienta de migración DFSRMIG.exe.

La herramienta de migración para el servicio de replicación DFS DFSRMIG.exe se instala con el servicio de replicación DFS. Cuando un nuevo Controlador de Dominio Windows Server 2008 o posterior se instala, el asistente de instalación instala y arranca el servicio de replicación DFSR.

Cuando el equipo está configurado para albergar la función de servidor DNS, los eventos de este servicio se almacenan en un registro adicional. El registro del servidor DNS contiene sólo los eventos registrados por el servicio DNS de Windows. La imagen siguiente ilustra este registro al que podemos acceder a través de las herramientas de gestión de los registros de eventos de Windows, y también de forma directa empleando la consola de gestión MMC del DNS.

El registro **Eventos DNS** está ubicado como los demás registros en el directorio **%SystemRoot%\system32\Winevt\Logs** y lleva el nombre**DNS Server.evtx**. La imagen siguiente ilustra el nivel de detalle de los mensajes contenidos en este registro.

En efecto, en este ejemplo, un problema de configuración de la dirección IP parece ser la causa de un error de socket TCP/IP.

Detección de un registro de recurso DNS no válido en la zona

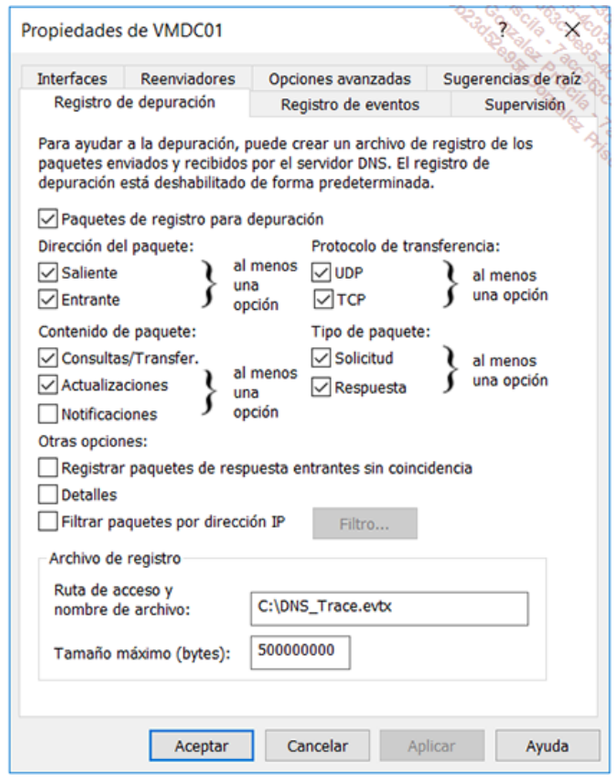
En efecto, vemos que el problema está en la línea 31 del archivo de zona cuyo nombre es europe.corporate.net.dns. Por lo general, los mensajes propios de Windows y los componentes integrados del sistema son bastante claros. Lamentablemente, habrá casos en que algunos mensajes no serán tan claros como el ejemplo anterior. Será a veces necesario buscar más detalles sobre las circunstancias de la aparición de un determinado mensaje. Podremos acceder a la descripción de los mensajes Windows utilizando los recursos que se especifican a continuación:

- Conéctese al sitio: http://www.EventID.net

4. Utilización de los registros de depuración DNS

A partir de Windows Server 2003, todas las versiones de Windows Server soportan el modo de registro avanzado que permite seleccionar los tipos de mensajes y las operaciones específicas relativas al servicio DNS.

Como ocurre con muchos productos, estos registros no están activados por defecto para evitar una posible sobrecarga del equipo. Solo se activarán en caso de necesidad, o por ejemplo, a petición del soporte de Microsoft. Por ejemplo, la activación de los registros de depuración en un servidor DNS tendrá por efecto la grabación en el registro DNS.log de los tipos de actividad que seleccionemos de forma previa. Podemos activar el registro de depuración empleando la pestaña **Registro de depuración** a través de las propiedades del objeto Servidor en el Administrador de DNS.



Este archivo, por cierto muy útil para ayudar al diagnóstico de incidentes DNS, puede consumir mucho espacio en disco, por lo que su tamaño máximo se fija por defecto en 500 Mb. Para evitar posibles problemas de espacio en disco, también podemos cambiar la ubicación física del archivo de registro ubicando el mismo en otro disco físico o en otra partición.

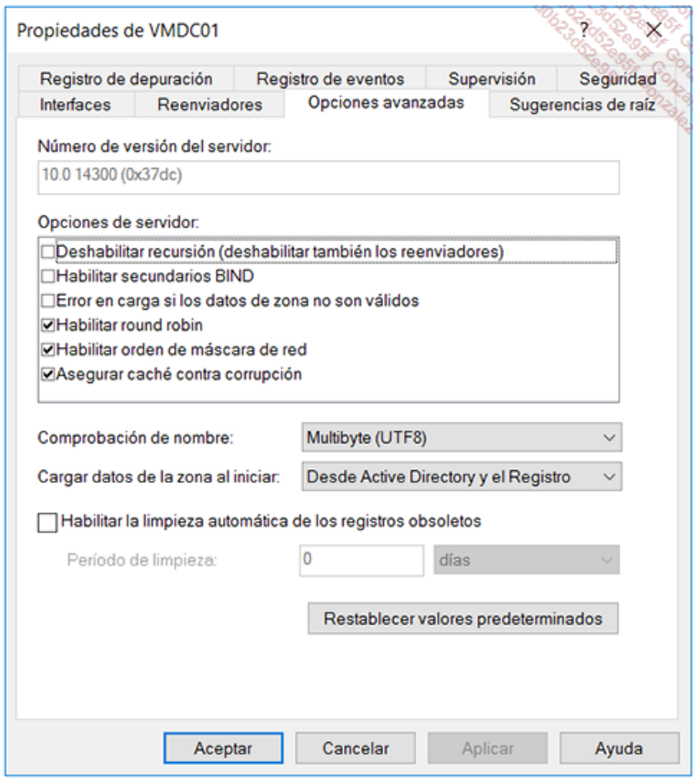
Tenga en cuenta que este tamaño por defecto permite registrar bastante información en un período de tiempo adecuado para poder ayudar en el diagnóstico y la resolución del problema. ¡Recuerde que el registro de errores no se detendrá si no se especifica o si el espacio en disco es insuficiente! Al activar la función, el registro de depuración seguirá operativo y las entradas más antiguas serán eliminadas sólo cuando el límite de tamaño se alcance.

Por defecto, el registro de depuración no está activado. Esta característica solo debería activarse para diagnosticar un problema complejo. En efecto, no debemos olvidar que este modo de depuración puede consumir muchos recursos y afectar el rendimiento general del equipo. Por lo tanto, utilice esta característica de forma temporal cuando sea necesario disponer de información más detallada.

Para más información acerca de la supervisión del servicio DNS, buscar «Supervisión y optimización de servidores DNS» en la ayuda en línea de Windows Server.

Restauración de la configuración por defecto

Puede ocurrir que después de la aplicación de muchos parámetros del servidor DNS de Windows Server 2003 o Windows Server 2008, estos no se hayan definido de forma adecuada. Para volver a establecer un comportamiento adecuado, podemos requerir restablecer los valores por defecto del servidor DNS. Para realizar esta operación empleando la consola de gestión MMC de DNS, haga un clic derecho sobre el servidor DNS adecuado y luego **Propiedades** y seleccione la pestaña **Opciones avanzadas**. Haga clic en **Restablecer valores predeterminados**, luego en el botón Aceptar.



Restauración de la configuración por defecto del servidor DNS

Los parámetros restaurados respetarán los valores correspondientes a la instalación por defecto del servicio servidor DNS en el equipo. Estos valores se presentan a continuación:

Desactivar la recursión	No seleccionado.
Habilitar secundarios BIND	Seleccionado.
Error en carga si...	No seleccionado.
Habilitar round robin	Seleccionado.
Habilitar orden de máscara de red	Seleccionado.
Proteger la caché contra corrupción	Seleccionado.
Comprobación de nombre	Multibyte (UTF8).
Cargar datos de la zona...	Desde Active Directory y el Registro.
Habilitar la limpieza automática ...	No seleccionado.

Esta operación requiere que sea miembro del grupo administradores en el equipo local, o que haya recibido por delegación las autorizaciones necesarias. Si el equipo es miembro de un dominio, los miembros del grupo Administradores del dominio pueden efectuar esta operación.

Interfaz NetBIOS y Configuración DNS del cliente Windows

1. Acerca de la interfaz NetBIOS

a. Interfaz NetBIOS y Configuración DNS del cliente Windows 10 Profesional

Los sistemas operativos Microsoft soportan TCP/IP desde hace más de veinte años. Con las primeras versiones de PC/LAN y luego con Microsoft OS/2 LAN Manager y finalmente Windows NT 3.1 a partir de 1993, y hoy con todas las tecnologías que gravitan en torno al directorio Active Directory, los servicios TCP/IP han adquirido cada vez más importancia dentro de las infraestructuras Microsoft. Esta sección presenta los conceptos y las buenas prácticas de la configuración TCP/IP del puesto de trabajo Windows 10 Profesional sabiendo que podemos volver a aplicar estos principios en los equipos que utilicen versiones anteriores que van desde Windows 2000 hasta Windows Server 2012 R2.

b. Tipos de nombres a tener en cuenta

Para empezar, conviene recordar que los sistemas operativos Windows utilizan un espacio de nombres y un sistema de resolución de nombres para asociar las direcciones IP de los nombres de equipos, los nombres de servicios y los nombres de dominio.

Aunque no se trata solo de los tipos de nombres existentes en los sistemas de redes, podemos considerar que existen hoy dos grandes tipos de nombres:

- **Los nombres de host**: los nombres de host son utilizados por los programas que utilizan la interfaz de programación Windows Sockets. Hoy en día, la mayoría de las aplicaciones se basa en esta interfaz. Por ejemplo, las aplicaciones como Microsoft Internet Explorer o las herramientas de TCP/IP como el comando **tracert** utilizan esta interfaz de programación de la red.
- **Los nombres NetBIOS**: los nombres NetBIOS son utilizados por los programas o servicios de red que utilizan la interfaz de programación NetBIOS. Por ejemplo, aplicaciones como el "Cliente de redes Microsoft" y "Compartir archivos e impresoras para redes Microsoft" son también programas que pueden utilizar la interfaz NetBIOS. Antes de que TCP/IP se impusiera mediante la aparición de Internet y la adhesión de líderes tales como IBM, Microsoft y Novell, las redes aprovechaban protocolos de transporte propietarios y cada uno más específico que el otro -IPX/SPX de Novell, DECnet de DEC, SNA de IBM, AppleTalk. Todos estos protocolos tenian sus propias interfaces de desarrollo de aplicaciones de red, mientras que NetBIOS - *Network Basic Input y Output System*, hacía su aparición para desempeñar el papel de interfaz de programación genérica para el desarrollo de aplicaciones de red. Por supuesto, todos estos protocolos se encuentran obsoletos, hoy en día, pero el hecho es que la historia se repite sin cesar y que la naturaleza aborrece el vacío, la interfaz de programación NetBIOS tuvo su momento de gloria para soportar aplicaciones de forma independiente del protocolo de transporte de red subyacente desplegado en la empresa.

c. Posicionamiento de la interfaz NetBIOS en comparación con TCP/IP

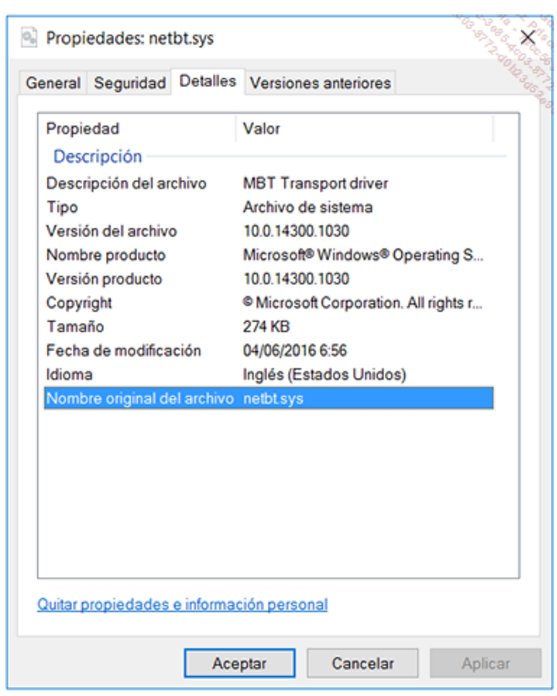
El protocolo NetBIOS existe como interfaz de tipo de sesión, es decir, el nivel 5 del modelo OSI. Sin embargo, este protocolo también existe como verdadero transporte a nivel 4 del mismo modelo. La implementación de Microsoft, conocida bajo el nombre de NetBEUI *NetBIOS Extended User Interface*, es la de mejor rendimiento. Este transporte rivalizó durante muchos años con el transporte IPX/SPX de Novell Netware y el de IBM OS/2 Warp Server vía NetBIOS 3.0, una separación del protocolo NetBEUI de Microsoft.

Al no disponer de servicios de red de nivel 3 del modelo OSI, el protocolo NetBEUI no es por supuesto enrutable. Sin embargo, este protocolo de transporte era *source routable* en Token Ring y podía cruzar las pasarelas de nivel 2 -incluidas en Ethernet.

Relación entre el modelo TCP/IP y las aplicaciones

Por último, la capa de Aplicación es la capa más importante. Esta es la que permite a las aplicaciones de red utilizar los servicios de la pila de protocolos TCP/IP en su totalidad. TCP/IP ofrece dos interfaces que permiten a las aplicaciones de red utilizar sus servicios.

- **La interfaz Windows Sockets**: esta interfaz, también llamada Winsock, desempeña el papel de interfaz estándar entre las aplicaciones basadas en sockets y los protocolos de la suite TCP/IP. El concepto es el siguiente: la aplicación especifica el protocolo, la dirección IP y el puerto a utilizar en la aplicación remota. Los servicios de la interfaz de Windows Sockets permiten realizar esta función, así como la apertura y cierre de las conexiones y el envío y recepción de datos.
- **La interfaz NetBIOS over TCP/IP**: esta interfaz, también llamada NetBT, -desempeña el papel de interfaz estándar entre las aplicaciones NetBIOS. Ofrece servicios de nombres completos, los servicios de entrega de datos en modo conectado y desconectado (es decir TCP y UDP), así como los servicios de gestión de sesiones.



El controlador de transporte NetBIOS over TCPIP (netbt.SYS), está presente en Windows 10 para garantizar la compatibilidad de la interfaz NetBIOS.

2. Plataforma Windows y la interfaz NetBios

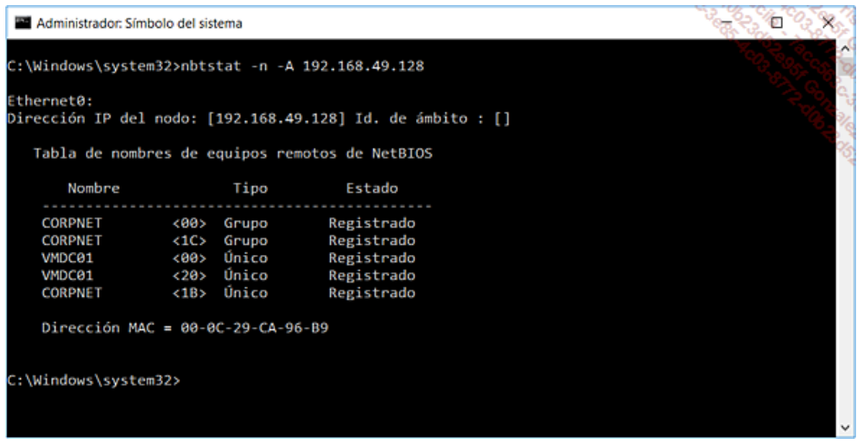
a. Servicios NetBIOS y códigos de servicio Microsoft

En la medida en que muchas aplicaciones siguen utilizando la interfaz NetBIOS, es importante conocer los códigos de servicio utilizados por los componentes de red Microsoft. Estos códigos serán registrados en la red local en forma de mensajes de tipo *limited broadcasts* es decir, los mensajes de difusión de la dirección de destino se limitará a la red o a la subred TCP/IP de origen. Por ejemplo, en la red 10.1.0.0 con un prefijo de 16 bits, es decir, una máscara de subred de clase B, la dirección de destino de estos mensajes de solicitud de registro será 10.1.255.255. Por supuesto, como los routers IP solo encaminan los mensajes dirigidos (unicasts), estos mensajes están limitados a la subred IP local.

Todos los equipos presentes en la red serán notificados y podrían posiblemente contestar o aceptar la solicitud de registro. Eso es lo que sucederá si se inicia de forma fortuita dos equipos con el mismo nombre NetBIOS en la misma red. El último equipo en arrancar quedará excluido de la red NetBIOS hasta que el problema de conflicto se solucione.

Además del registro de nombres NetBIOS a través de mensajes de difusión, la implementación de NetBIOS sobre TCP/IP permite el uso de servidores NBNS (*NetBIOS Name Servers*) como WINS - *Windows Internet Naming Service*. Estos servidores permiten centralizar todos los registros NetBIOS. Por supuesto, estos servidores de registro de nombres NetBIOS funcionan de manera dinámica y permiten disminuir sustancialmente el número de mensajes de difusión. La captura siguiente muestra el uso del comando `nbtstat` que permite ver los códigos de los servicios de un equipo determinado.

En este ejemplo, el equipo de destino funciona con Windows Server 2016 y el comando `nbtstat` lista los nombres NetBIOS inscritos en la interfaz del mismo nombre. La caché local del equipo remoto con la dirección 192.168.49.128 indica que se trata del equipo VMDC01 que actúa como controlador de dominio. Tenga en cuenta que en este ejemplo concreto, y siempre en cuanto a la interfaz NetBIOS, visualizamos un dominio NT y no un dominio Active Directory.



Visualización de nombres NetBIOS registrados en el equipo 192.168.49.128. El código [1B] muestra que el equipo desempeña el rol de controlador de dominio maestro de exploración para el dominio NetBIOS CORPNET

El comando `nbtstat` es un antiguo comando NetBIOS utilizado con mucha frecuencia. Existe desde las primeras implementaciones de Microsoft OS/2 LAN Manager. Además de controlar cada equipo de forma individual, podremos acceder a todos los registros del espacio de nombres NetBIOS consultando la o las bases de datos de los servidores WINS.

Los tipos de nombres NetBIOS presentados a continuación son los más usados en las redes Microsoft.

nombre_equipo[00h]: este nombre se graba por el Servicio puesto de trabajo en el cliente WINS.

nombre_equipo[03h]: este nombre se graba por el servicio de mensajes en el cliente WINS.

nombre_equipo[06h]: este nombre será grabado en el cliente WINS por el Servicio de enrutamiento y acceso remoto, al iniciar este servicio.

nombre_dominio[1BH]: este nombre se registra por cada controlador de dominio Windows NT Server 4.0 que desempeñe el rol de explorador principal de dominio (*Domain Master Browser*). Estos registros de nombre se utilizan para permitir la exploración remota de los dominios.

nombre_equipo[1Fh]: este nombre se registra por los servicios NetDDE (*Network Dynamic Data Exchange*). Solo se registra si los servicios NetDDE se arrancan.

nombre_equipo[20h]: este nombre se graba por el servicio Servidor en el cliente WINS.

nombre_equipo[21h]: este nombre será grabado en el cliente WINS por el Servicio cliente RAS, al arrancar el equipo.

nombre_equipo[BIH]: este nombre se graba por el Agente de vigilancia de la red (Agente Netmon) y solo aparecerá si este servicio se inicia en el cliente WINS.

nombre_equipo[BFh]: este nombre se registra por la herramienta de supervisión de la red (Analizador de tramas que viene con Microsoft Systems Management Server 2.0 o 2003).

nombre_usuario[03h]: este nombre se registra para cada uno de los usuarios conectados. Observe: si varios usuarios se conectan con el mismo nombre, solo el primer equipo registrado en la red, será capaz de registrar dicho nombre.

nombre_dominio[00h]: se trata de un nombre de Grupo NetBIOS registrado por el Servicio Estación de trabajo para poder recibir las transmisiones de exploración procedentes de equipos LAN Manager.

nombre_dominio[1CH]: se trata de un nombre de Grupo NetBIOS utilizado por los controladores de dominio Windows NT en el marco del dominio. Puede contener hasta 25 direcciones IP. Observe que Active Directory no utiliza este registro.

nombre_dominio[1DH]: se trata de un nombre de Grupo NetBIOS utilizado por los exploradores principales de cada subred, sabiendo que solo puede haber un único -explorador principal por subred. Los exploradores de respaldo (Backup Browsers) usan ese nombre para comunicarse con el explorador principal (Master Browser), extrayendo la lista de servidores disponibles para el explorador principal.

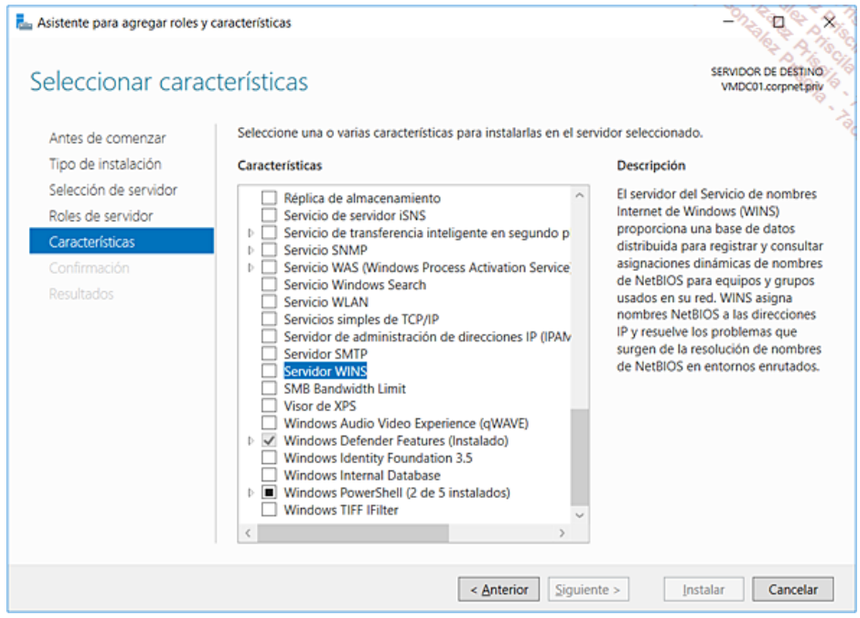
nombre_grupo[1EH]: se trata de un nombre de Grupo NetBIOS ordinario. Cualquier equipo configurado como explorador de red puede emitir hacia ese nombre, y escuchar las transmisiones de ese nombre, para elegir un explorador principal. Un nombre de grupo mapeado de manera estática usa este nombre para inscribirse en la red. Cuando un servidor WINS recibe una solicitud de nombre terminada por [1E], reenvía siempre la dirección de difusión de la red local del cliente que emitió la solicitud.

nombre_grupo[20H]: se trata de un nombre de grupo NetBIOS especial llamado grupo Internet. Está registrado en los servidores WINS para identificar los grupos de equipos para las necesidades de administración.

__MSBROWSE__[01h]: se trata de un nombre de grupo NetBIOS registrado por el explorador principal para cada subred. Cuando un servidor WINS recibe una solicitud acerca de este nombre, reenvía siempre la dirección de difusión de la red local del cliente que emitió la solicitud.

Los códigos de los servicios presentados antes son los códigos relativos a los componentes de red Microsoft. Muchas aplicaciones no-Microsoft siguen utilizando código que requiere de la interfaz de programación NetBIOS. En estos tipos de entornos, el soporte de esta interfaz y también de los servidores WINS es siempre necesario.

Cabe señalar que Windows Server 2016 soporta todavía el servicio WINS. Este servicio se encuentra, al igual que con Windows Server 2012 R2, en el conjunto de las funcionalidades del Administrador de servidores.



Para más información sobre la configuración de servidores WINS, busque WINS en el sitio Technet de Microsoft o haga referencia al kit de recursos técnicos de Windows Server 2003 o Windows Server 2008 que tratan este tema con mucho detalle.

b. Resolución de nombres NetBIOS

La resolución de nombres NetBIOS significa que es posible efectuar una correspondencia entre nombre NetBIOS y la dirección IP asociada a éste. Como se recordará, un nombre NetBIOS es una dirección de 16 bits utilizada para identificar los recursos NetBIOS dentro de la red. De hecho, los primeros 15 bytes están disponibles para el nombre mientras que el último, el 16º, se encuentra reservado para el código de servicio. Por definición, el nombre NetBIOS es un nombre único en el conjunto de la red NetBIOS, siendo un nombre de grupo que será utilizado por todos los miembros de dicho grupo. En este último caso, el nombre NetBIOS es calificado como nombre "NetBIOS no exclusivo".

Por último, cuando un proceso NetBIOS se comunica con otro proceso NetBIOS situado en un equipo de la red, entonces solo se emplea el nombre único. Por contra, en el caso de comunicaciones de una aplicación con varios procesos situados en varios equipos, entonces se utilizará un nombre de grupo NetBIOS.

Registro de los equipos y servicios en la red NetBIOS

El servicio "Compartir impresoras y archivos para redes Microsoft" es un ejemplo de proceso en un equipo cliente Windows. Cuando el equipo arranca, este servicio registra un nombre NetBIOS único basado en el nombre de nuestro equipo. El nombre exacto utilizado por el servicio es el nombre limitado a 15 caracteres. El 16º carácter del nombre (en hexadecimal, valor de 00 a FF) indicará siempre el tipo de recurso. En nuestro ejemplo, el servicio servidor reporta el código 0x20. Este mecanismo de registro se producirá para cada aplicación que pertenezca al espacio de nombres NetBIOS.

c. Orden de las resoluciones NetBIOS

El mecanismo exacto según el cual los nombres NetBIOS se resuelven en direcciones IP depende del tipo de nodo NetBIOS configurado en el equipo. La RFC 1001, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods" define cuatro tipos de nodos NetBIOS.

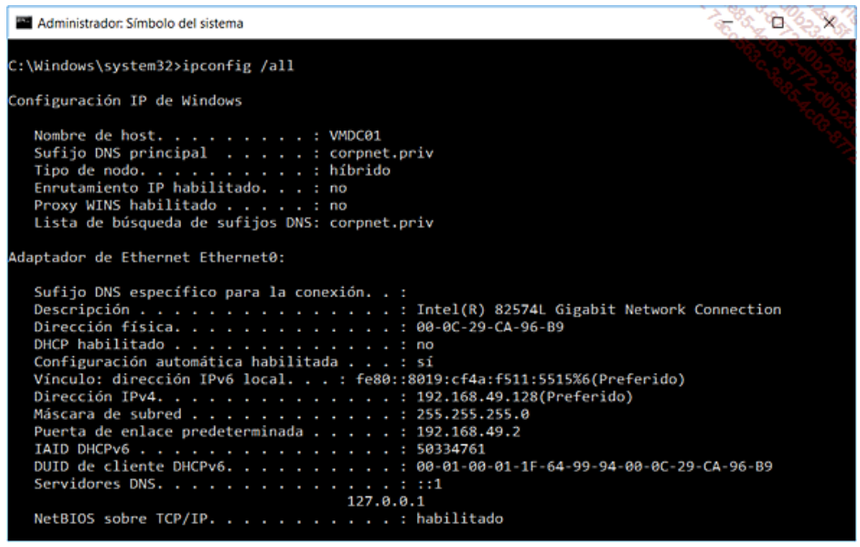
Nodo de tipo B-nodo (difusión): el modo B-nodo (Broadcast node) utiliza las peticiones de nombres NetBIOS de difusión para la inscripción y la resolución de nombres. El B-nodo presenta dos problemas principales:

- Las transmisiones perturban cada nodo de la red local,
- Los routers no transmiten, por defecto, los mensajes de difusión; por lo tanto, sólo los nombres NetBIOS de la red local pueden ser resueltos.

Nodo de tipo P-nodo (punto a punto): El P-nodo (Point to Point node) utiliza un servidor de nombres NetBIOS (NBNS) tal como un servidor WINS para resolver los nombres NetBIOS. El P-nodo no utiliza todas las difusiones. Todas las resoluciones son dirigidas en unicast al servidor de nombres WINS. Este tipo de nodo se utiliza en raras ocasiones.

Nodo de tipo M-nodo (mixto): el M-nodo (Mixed node) es una combinación de B-nodo y P-nodo. Por defecto, un M-nodo funciona primero como un B-nodo. Si un M-nodo no puede ser utilizado para resolver un nombre por difusión, pide un NBNS empleando el P-nodo. Este tipo de nodo se utiliza en raras ocasiones.

Nodo de tipo H-nodo (híbrido): el H-nodo (Hybrid node) es una combinación de P-nodo y B-nodo. Por defecto, un H-nodo funciona como un P-nodo. Si un H-nodo no puede ser utilizado para resolver un nombre empleando NBNS, entonces se utiliza una difusión para resolver el nombre. Como se trata del tipo de Nodo recomendado por Microsoft, es por lo general el usado de forma más común. El hecho de declarar el uso de uno o varios servidores WINS para disponer de mejores resoluciones NetBIOS configura automáticamente el tipo H-node. Podemos determinar el tipo de nodo empleando el comando `ipconfig /all`. El comando siguiente muestra que el tipo de nodo es híbrido y que la interfaz NetBIOS en TCP/IP está habilitada.



d. Orden de resolución de un puesto de trabajo de tipo H-node

La resolución de nombres NetBIOS para los clientes WINS es directamente dependiente del módulo NetBT que implementa la interfaz NetBIOS sobre TCP/IP. El método real de resolución de nombres es por fortuna transparente para las aplicaciones y usuarios.

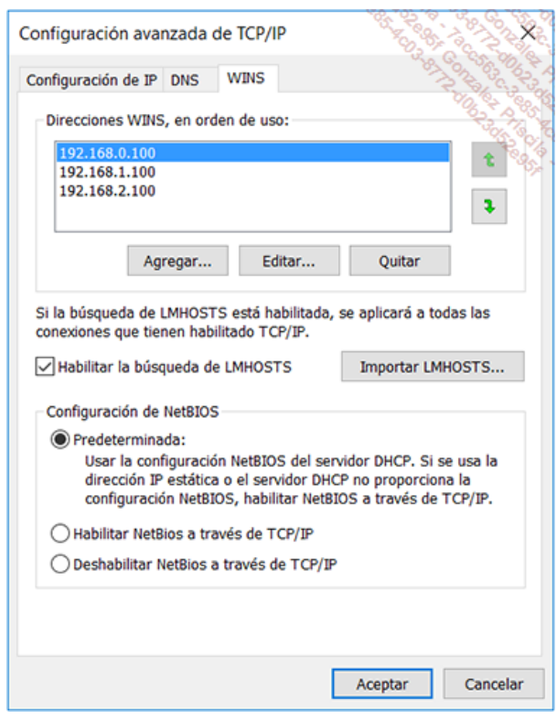
Para todos los sistemas operativos Microsoft Windows desde 2000 hasta Windows 10, los clientes WINS utilizan la siguiente secuencia para resolver un nombre:

- Si el nombre solicitado tiene más de 15 caracteres o si tiene la forma de un nombre totalmente cualificado (FQDN que contienen puntos "."), entonces la solicitud será transmitida de forma directa al sistema de resolución DNS.
- De lo contrario, el equipo controla si el nombre está presente en la caché de nombres remotos del cliente. Podemos consultar empleando el comando `nbtstat -c`.
- De lo contrario, una solicitud de resolución de nombres NetBIOS se envía a los servidores WINS configurados.
- En caso contrario, un mensaje de difusión se envía a la dirección IP de subred.
- Si esto no funciona, se verifica el archivo LMHOSTS siempre que la opción **Habilitar la búsqueda de LMHOSTS** esté habilitada en las propiedades de **Protocolo de Internet (TCP/IP)** de la conexión, pestaña WINS. Esta opción está habilitada por defecto.
- De lo contrario, se verifica el archivo HOSTS.
- Por último, se invocan las resoluciones DNS. En primera instancia, la caché de nombres DNS se consultará, y luego se interrogará a uno o varios servidores DNS.

Para más información sobre las resoluciones de nombres y un organigrama claro de este proceso cuando el ordenador está equipado con varias tarjetas de red configuradas con parámetros TCP/IP específicos, busque en el sitio de Microsoft Technet "Name Resolution Tecnologies".

Declaración de direcciones de los servidores WINS, selección del tipo de nodo NetBIOS y número de servidores WINS declarados

Con las versiones anteriores de Windows (Windows NT y Windows 9x), era posible configurar de forma manual los clientes para que utilizaran solo al menos un servidor WINS primario y, a lo sumo, un servidor secundario adicional. Este último se utilizaba en caso de fallo del primero. La imagen siguiente muestra la pestaña WINS, que agrupa a todos los parámetros relativos a la interfaz y al soporte de NetBIOS.



Configuración de servidores WINS y uso de la búsqueda LMHOSTS

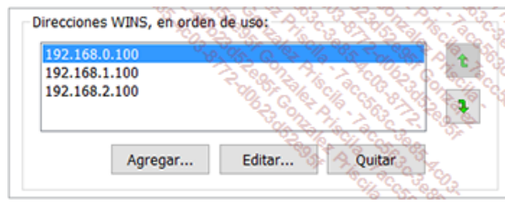
Una vez declaradas, las direcciones de los servidores WINS se solicitarán en el orden en que aparecen en la lista. Observe que contamos con la posibilidad de reorganizar esta lista empleando las flechas situadas a la derecha.

En Windows NT, los servidores WINS declarados eran dos (el servidor WINS principal y el servidor WINS secundario) y estaban en la ventana principal de los parámetros TCP/IP. En los sistemas posteriores a Windows 2000, la interfaz NetBIOS es menos obligatoria. De hecho, los parámetros WINS fueron desplazados hacia esta nueva ubicación.

Aunque los sistemas operativos modernos como Windows 2000 hasta Windows 10 ya no requieren la interfaz NetBIOS para su funcionamiento interno, esta interfaz debe estar siempre presente para garantizar la interoperabilidad con los sistemas y aplicaciones anteriores. Es la razón por la cual, no es recomendable desactivar la interfaz NetBIOS que está siempre presente en todos estos sistemas.

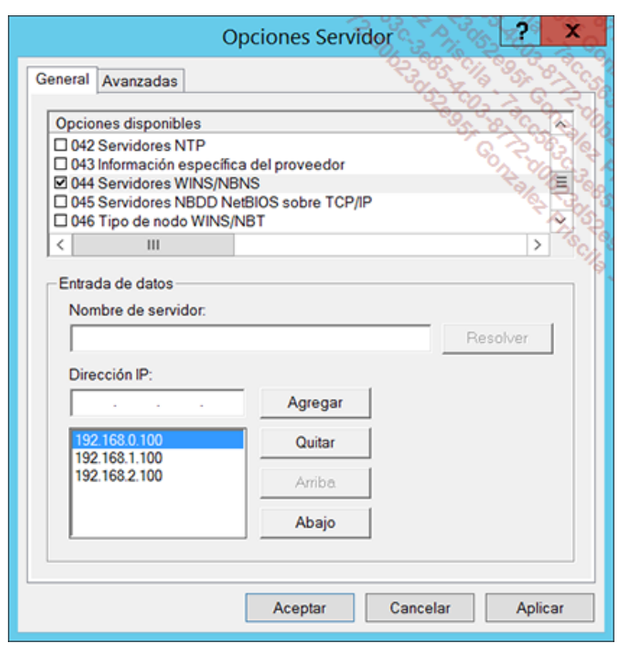
Con Windows Server 2003 y hasta Windows Server 2016 podemos configurar los clientes WINS para que utilicen hasta doce servidores WINS. Podremos gestionar esta lista de dos maneras:

- De manera estática a través de las propiedades del protocolo TCP/IP.



*Declaración de la lista de servidores WINS utilizando los parámetros TCP/IP y la pestaña **WINS***

- De forma dinámica empleando el protocolo DHCP configurando la opción DHCP 44.



Declaración de la lista de servidores WINS utilizando la opción 44 del protocolo DHCP

La declaración de dos servidores WINS es necesaria y suficiente en la mayoría de los casos. Sin embargo, esta limitación fue destacada en varias ocasiones por algunos clientes.

En efecto, no es raro que sea necesario disponer de dos servidores WINS por sitio. En el caso de fallo por parte de los dos servidores WINS del sitio, por ejemplo, la corrupción de los dos servidores WINS locales o de una indisponibilidad de esta parte de la red, sería deseable poder vernos auxiliados por un servidor WINS situado en un sitio remoto. Este tipo de limitación no existe en relación con los parámetros de servidores DNS. Microsoft llevó a cabo esta modificación. Por último, una lista más adaptada de servidores WINS ofrece a los clientes una mejor tolerancia a fallos cuando sus servidores WINS primario y secundario no están disponibles.

Las versiones modernas de Windows -a partir de Windows 2000 hasta Windows Server 2016 soportan ahora hasta doce servidores WINS declarados. Sin embargo, tenga en cuenta que sólo los dos primeros servidores registrados podrán ser utilizados para realizar el registro dinámico de los clientes. Los dos servidores situados en lo más alto de la lista son equivalentes al servidor WINS principal y el servidor WINS secundario en los antiguos equipos Windows NT.

Podremos seguir usando el comando `ipconfig /all`. Éste muestra de forma correcta los parámetros de WINS primario y secundario, así como los otros posibles servidores adicionales.

e. Interfaz y nombres NetBIOS, resoluciones WINS y dominios Active Directory

Hoy en día, no se considera una buena práctica configurar los servicios de resolución NetBIOS basados en WINS.

En términos absolutos, los equipos cliente Windows o Windows Server miembros de un dominio Active Directory no tienen necesidad de recurrir a los servicios de resolución NetBIOS para interactuar con Active Directory. Sin embargo, esto puede ser necesario si todavía se emplean antiguas aplicaciones basadas en la interfaz NetBIOS en la empresa. Con mayor motivo, debemos tener en cuenta que es necesario configurar los equipos cliente miembros de un dominio Active Directory con parámetros WINS si deben comunicarse con otros equipos de tipo NetBIOS.

3. Configuración de un puesto cliente Active Directory

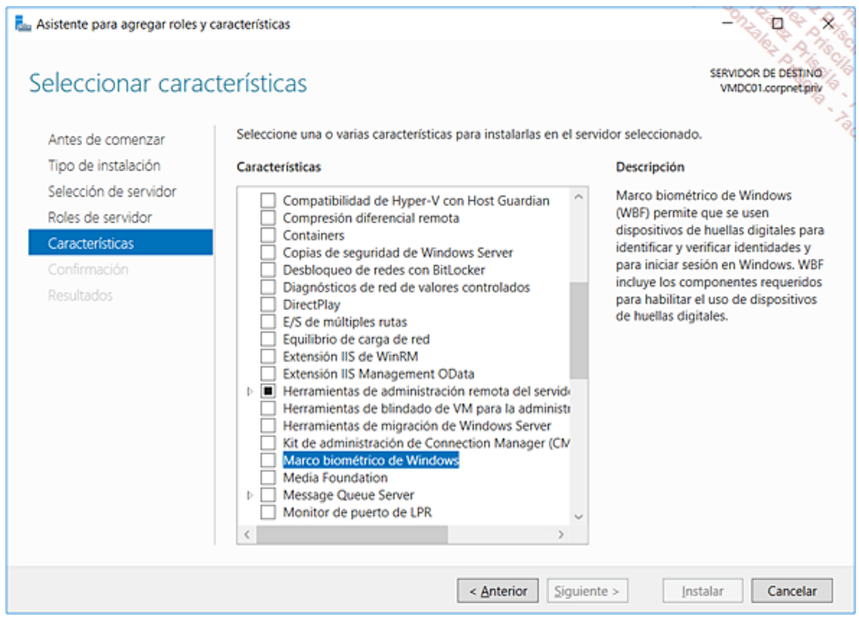
a. Acerca de los servicios de Active Directory

Los únicos y verdaderos clientes Active Directory son los sistemas que funcionan con los sistemas operativos de Microsoft a partir de Windows 2000 y hasta Windows 10 hoy en día. Es evidente que este será también el caso en las próximas versiones de Windows.

Los módulos cliente que soportan los protocolos y mecanismos fundamentales están integrados de forma directa en el sistema operativo. Estos componentes fundamentales son el sistema de ubicación principal basado en el protocolo de resolución de nombres DNS, los protocolos LDAP, NTP y Kerberos, así como los servicios de gestión de configuraciones ofrecidos a través de los objetos de directivas de grupo -en inglés,*Group Policy Objects*. De esta forma, ninguna acción adicional se debe realizar en los equipos cliente "inteligentes" miembros de un dominio Active Directory. Los puestos de trabajo activarán durante el próximo reinicio los módulos necesarios para su funcionamiento con el dominio Active Directory. Como siempre, la condición sine qua non, será que los puestos de trabajo puedan "descubrir" el dominio Active Directory empleando los servidores DNS de la empresa.

La modernización de una antigua infraestructura hacia servicios de directorio Active Directory puede haber sido justificada por la previsión de nuevas necesidades y también nuevas exigencias a corto o mediano plazo. Entre estas nuevas limitaciones, encontraremos nuevas exigencias en materia de seguridad y autenticación. Tenga en cuenta que:

- Los puestos de trabajo y servidores Windows soportan los más altos niveles de autenticación posibles a través del uso del protocolo Kerberos versión 5, los certificados X.509v3 y la información de tipo biométrico soportadas por el WBF (*Windows Biometric Framework*) integrado en todas las versiones de Windows. La utilización de autenticaciones basadas en una tarjeta inteligente, sobre el uso de certificados y claves fuertes asimétricas, de un código PIN y también de un control biométrico (huella dactilar o retiniana) permiten alcanzar los más altos niveles de autenticación.



Observe que los puestos Windows NT soportan mejor las autenticaciones NTLM versión 1 y versión 2.

En los controladores de dominio Windows Server 2003 y hasta Windows Server 2016, las autenticaciones de tipo LAN Manager están desactivadas por defecto. Esta configuración refuerza la seguridad a través del abandono de protocolos hoy obsoletos pero tendrá el efecto de impedir los inicios de sesión de los equipos que requieran el uso de dichos protocolos. Para solucionar este problema causado por los nuevos parámetros de seguridad reforzada, podremos optar por una de las soluciones propuestas a continuación:

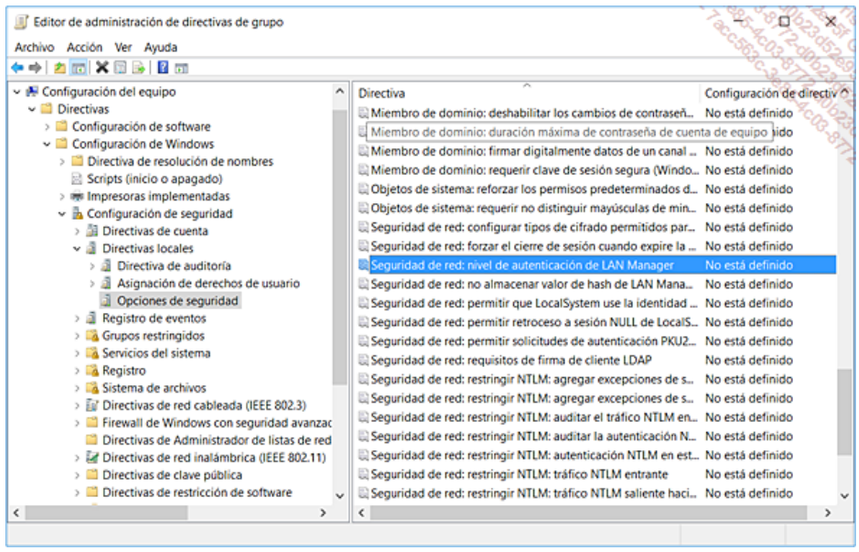
- Actualizar los equipos que no soporten los protocolos Kerberos o NTLM v2 a Windows 7 o una versión más moderna, tal como Windows 10; esta última opción es sin duda la mejor alternativa.

Reactivar el soporte del protocolo de autenticación de LAN Manager

Esta operación no se recomienda. Sin embargo, si el número de puestos que no soportan Kerberos o NTLM V2 sigue siendo muy amplio, podemos decidir reactivar las autenticaciones LAN Manager mientras se planifica una modernización de los equipos.

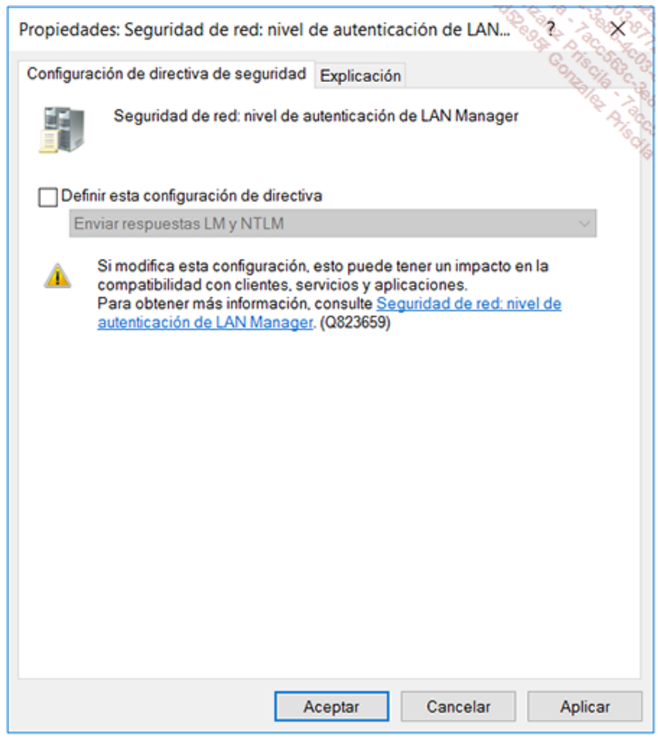
Podemos configurar este parámetro de seguridad abriendo la consola MMC Gestión de directivas de grupo en la ubicación **Panel de control\ Sistema y seguridad\ Herramientas de administración** o también a través del menú **Inicio** de Windows Server 2016.

Una vez cargada la consola, cambiamos la directiva por defecto de los controladores de dominio -en inglés, *Default Domain Controllers Policy*.

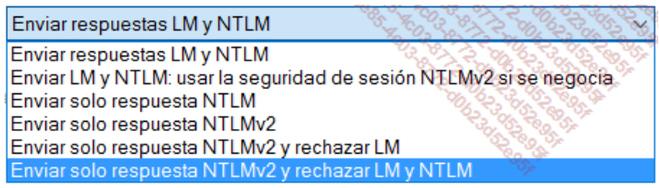


Modificación de las directivas de seguridad de un controlador de dominio

Una vez cargada la directiva de seguridad, desplegamos el árbol de la consola y nos dirigimos a la ubicación **Configuración de seguridad\Directivas locales\Opciones de seguridad**.



Configuración por defecto del nivel de autenticación de LAN Manager



Observe que los valores por defecto del parámetro son:

- Windows 2000 y Windows XP: enviar respuestas LM y NTLM al servidor.
- Windows Server 2003: enviar sólo respuesta NTLM.
- Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 y versiones posteriores: enviar sólo respuesta NTLMv2.

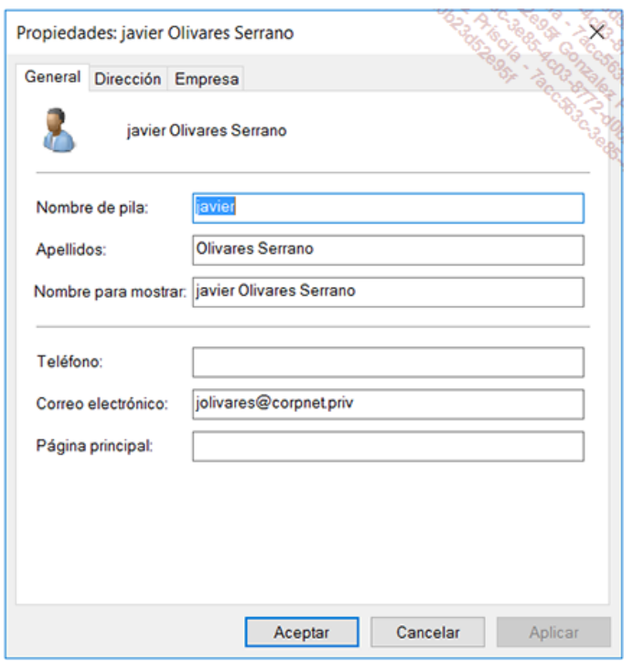
¡Tenga cuidado con la manipulación de las directivas de seguridad de los controladores de dominio Windows Server 2003 y Windows Server 2008 R2 ! Antes de cualquier modificación, por favor, consulte el artículo 823659 titulado "Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments" disponible en la dirección indicada más abajo: http://support.microsoft.com/kb/823659/en-us

Para obtener más información sobre el conjunto de los parámetros de la directiva de seguridad, consulte "Descripción de los parámetros de seguridad" en la ayuda en línea.

Clientes Windows y búsquedas Active Directory en Windows 10

Los usuarios autenticados en Active Directory pueden acceder a sus propiedades personales y también realizar búsquedas en el directorio. Aunque este enfoque sea utilizado de forma excepcional en las empresas, el usuario tiene así la posibilidad de mantener sus datos personales. El botón **Propiedades** permite al usuario la posibilidad de consultar y modificar la información presentada.

De esta manera, cualquier usuario puede acceder y modificar las propiedades que "controle". Este será, por ejemplo el caso de su número de teléfono o su dirección personal.



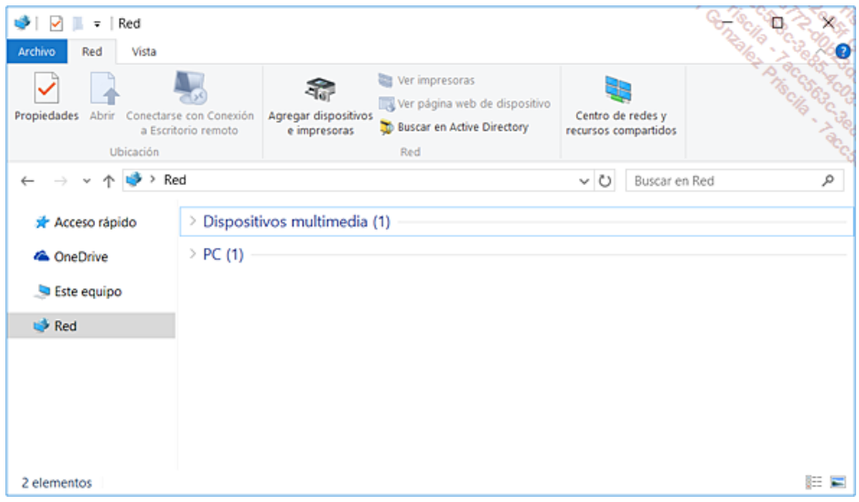
Si desea que un usuario tenga la posibilidad de modificar un atributo de otro objeto usuario, basta con asignar los permisos necesarios en el objeto y el atributo en cuestión. Este principio, llamado "principio de delegación de permisos", es un tema muy importante relativo al uso "general" que las empresas desean hacer de su(s) directorio(s). Los conceptos de delegación y la aplicación de una directiva de delegación se presentan más adelante.

La búsqueda en Active Directory

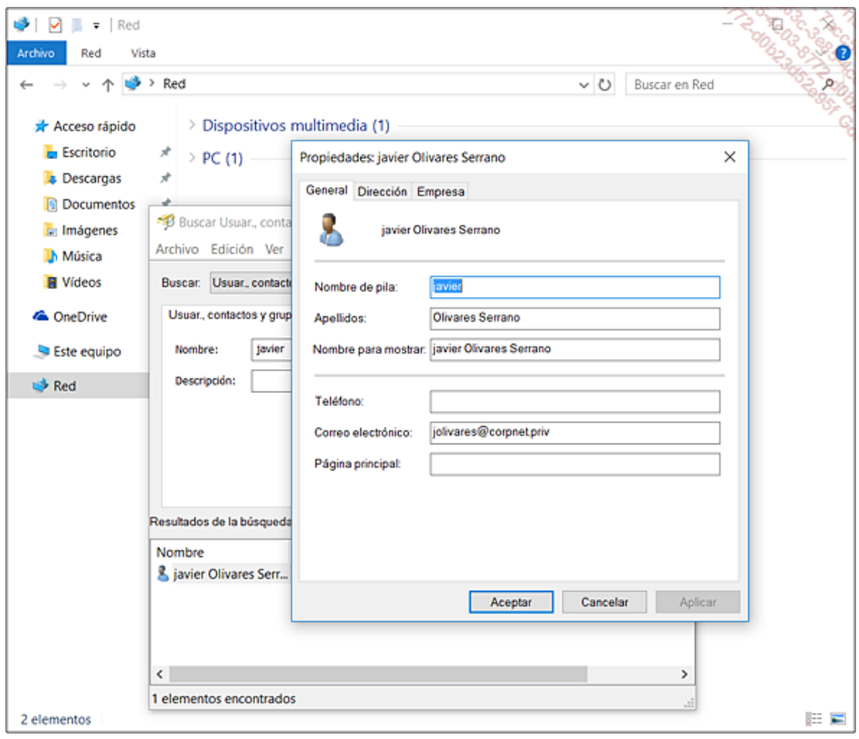
Con respecto a las búsquedas de los objetos de tipo "impresora": para que las impresoras puedan ser localizadas, estas deben estar publicadas. Para más información sobre la publicación de impresoras en Active Directory, busque en el sitio de Microsoft TechNet "Print and Document Services".

Ventana de búsquedas de Active Directory en Windows 10

A lo largo de las versiones de Windows, las funciones de búsqueda han evolucionado. En un puesto de trabajo Windows 10, se puede acceder a las funciones de búsqueda de Active Directory a través del icono de **Red** y luego usando el botón **Buscar en Active Directory**.



Opción de búsqueda "Buscar en Active Directory"



b. Puestos de trabajo Windows y configuración DNS necesaria para los entornos de dominios Active Directory

Los clientes de Active Directory integrados en los sistemas operativos Windows 2000 hasta Windows 10 utilizan los servicios DNS como servicio de localización principal y exclusivo. Las detecciones realizadas mediante las resoluciones DNS permitirán así la resolución de los elementos importantes como son los nombres de dominio, sitios y servicios de Active Directory.

Durante la instalación del directorio Active Directory, la zona DNS relativa al dominio de Active Directory, así como la zona de dominio raíz del bosque se actualiza de forma dinámica con los registros de recursos (SRV, y CNAME) de los nuevos controladores de dominio.

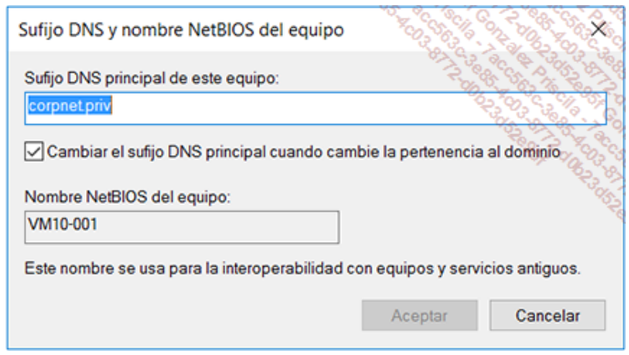
El proceso detallado de búsqueda y selección de los controladores de dominio se explica en el capítulo Servicios de ubicación AD DS y servicios DNS.

Los parámetros relativos a la configuración DNS implican por lo tanto una validación técnica por parte de los equipos de red y Active Directory. Una vez validados, estos parámetros deben aplicarse con rigor para garantizar un funcionamiento normal de los equipos miembro del sector.

A continuación se especifica la lista de temas relacionados con la configuración de Propiedades TCP/IP para cada equipo miembro de un dominio Active Directory.

Definición de un nombre de equipo y host DNS para cada ordenador

Por ejemplo, en el dominio de Active Directory, cuyo nombre completo (FQDN) es corpnet.priv, el nombre de equipo DNS completo podrá ser pc-marketing-1.corpnet.priv. Este nombre de host tendrá como consecuencia que el nombre NetBIOS del equipo, llamado desde hace muchos años "computer name", sea PC-MARKETING-1. Este nombre de 14 caracteres es válido ya que no alcanza el límite de 15 caracteres autorizados por la interfaz NetBIOS.



Herencia del nombre de host TCP/IP con el nombre NetBIOS del equipo

Tales nombres podrían impedir la utilización de nombres como pc-marketing-100. Sería truncado de forma automática e indexado en caso de conflictos. Por lo tanto, en este ejemplo concreto, puede ser aconsejable usar un sistema de nombres más corto como pc-market-xxx.

Para evitar confusiones y errores de resolución, Microsoft recomienda asegurarse de que los nombres de DNS y NetBIOS sean idénticos.

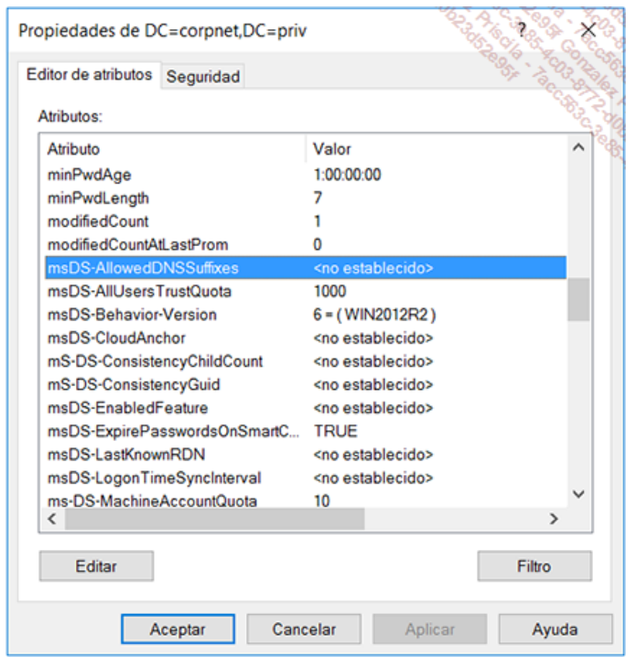
Definición de un sufijo DNS principal para el equipo

Debemos definir y aprobar el nombre de dominio DNS que es colocado antes del nombre de ordenador o equipo, y que proporcionará el nombre completo del equipo (FQDN). En el ejemplo anterior, el sufijo DNS principal es corpnet.priv. La opción **Cambiar el sufijo DNS principal cuando cambie la pertenencia al dominio** permite la actualización automática del sufijo DNS principal en función de la pertenencia al dominio Active Directory.

Aunque este valor no produce ningún efecto sobre la pertenencia real del equipo al dominio, la modificación del sufijo DNS podrán generar los siguientes problemas:

- Los demás usuarios de la red pueden tener dificultades para encontrar el equipo y realizar un control de acceso en su contra.
- El equipo solo podrá funcionar realmente en el dominio de Active Directory si el dominio permite a los equipos miembro del dominio usar un sufijo DNS principal diferente de los nombres de dominio DNS Active Directory.

Por defecto, el sufijo DNS principal del equipo debe hacer coincidir con el nombre del dominio de Active Directory al que pertenece el equipo. Para autorizar uno o varios sufijos DNS principales, el administrador del dominio debe declarar de forma manual una lista de sufijos autorizados estableciendo el atributo **msDS-AllowedDNSSuffixes** en el contenedor de objetos del dominio.

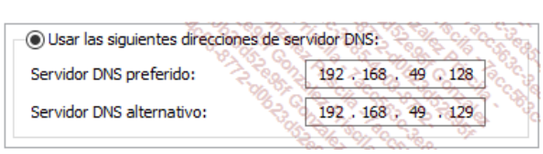


Utilización de ADSIEdit para cambiar el atributo msDS-AllowedDNSSuffixes en el objeto de clase domainDNS

Un nombre de equipo completo está formado por el nombre del equipo y el sufijo DNS principal cuya longitud puede alcanzar 255 caracteres como máximo. Este límite comprenderá los puntos necesarios para delimitar los diferentes dominios, así como el nombre de host. Observe que la longitud del nombre del equipo no podrá exceder los 63 caracteres. Microsoft recomienda que el sufijo DNS principal por defecto sea utilizado.

Definición de una lista de servidores DNS

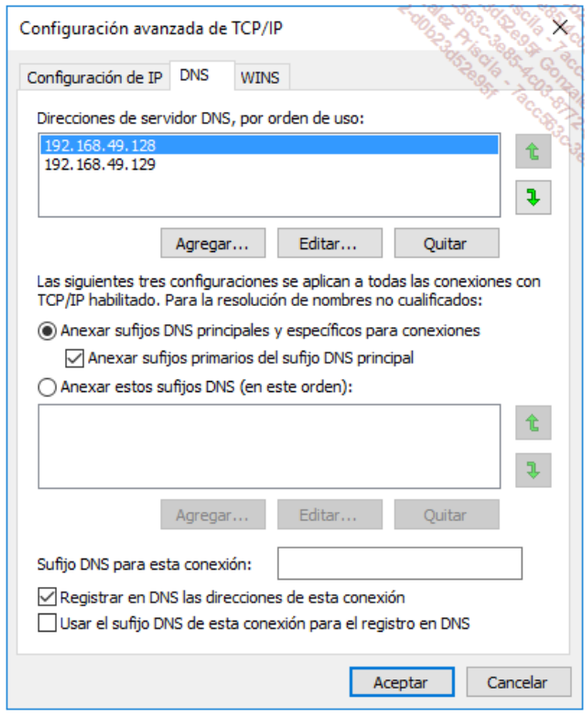
Debemos definir para cada ubicación geográfica cuáles son los servidores DNS para los clientes durante la resolución de nombres DNS, como un servidor DNS preferido, y los servidores DNS secundarios a utilizar cuando el servidor principal no está disponible.



Servidor DNS preferido y secundario de un equipo Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 o Windows Server 2008 R2

La imagen anterior muestra el caso particular de los parámetros DNS de un controlador de dominio Active Directory. En la medida en que se recomienda que cada sitio tenga un controlador de dominio y un servidor DNS, el controlador de dominio será a menudo cliente DNS de sí mismo. También será cliente de un servidor DNS secundario, el cual estará ubicado de preferencia en el mismo sitio. En el caso de que solo exista un controlador de dominio / DNS en el sitio, entonces se podrá seleccionar un servidor DNS situado en un sitio remoto.

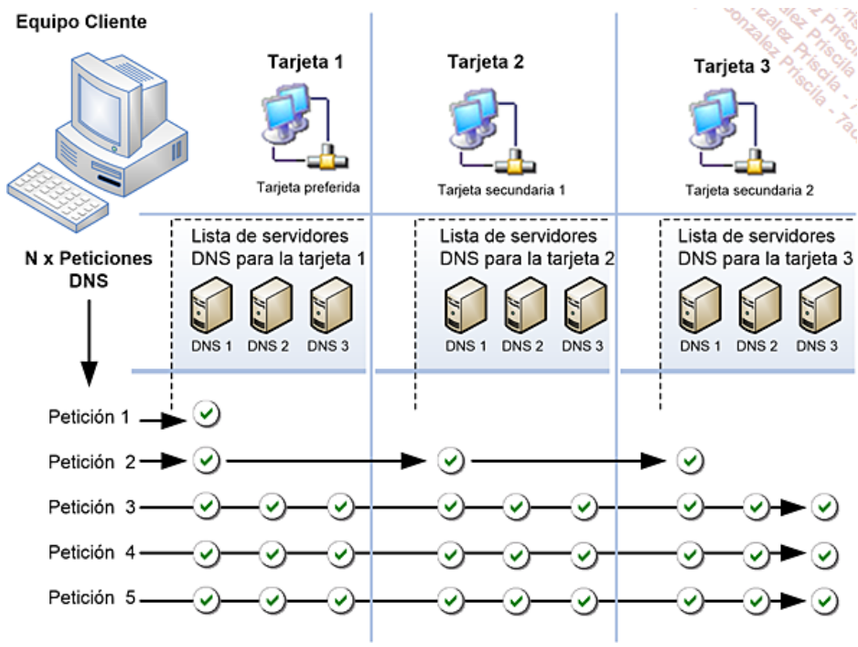
La generación de las solicitudes de resolución DNS es una parte importante del trabajo a realizar por parte del cliente. Es por esta razón que se encuentran en la pestaña **DNS** las configuraciones avanzadas que permiten determinar cómo la parte "cliente DNS" se ocupará de los nombres que no están plenamente cualificados. Los parámetros DNS que debemos definir se presentan a continuación.



Configuración avanzada del cliente DNS (DNR, Domain Name Resolver)

Declaración de múltiples servidores DNS y orden de selección

Si se declaran varios servidores DNS y el cliente DNS no llega a recibir respuesta del servidor DNS actual, entonces el servidor DNS siguiente será seleccionado. Sin embargo, ¿qué podemos decir de una configuración que incluya varias tarjetas de red y varios servidores DNS por tarjeta de red? El esquema siguiente explica cómo el DNR selecciona y distribuye las peticiones de resolución DNS cuando éstas no funcionan.



Distribución de las peticiones DNS en un equipo con varias tarjetas y varios servidores DNS

La secuencia de las solicitudes de resolución de nombres está compuesta por los siguientes pasos:

1. La consulta DNS es enviada al servidor DNS preferido de la primera tarjeta de red. Si la consulta no puede resolverse (de manera positiva o negativa), entonces continuamos al paso 2.

2. La consulta DNS es enviada al servidor DNS preferido de cada una de las tarjetas de red. En nuestro ejemplo, los primeros servidores DNS de cada una de las tarjetas son solicitados de forma simultánea. Si la respuesta a la solicitud vuelve a ser negativa, entonces se continúa al paso 3.

3. La consulta DNS es enviada a todos los servidores DNS de todas las tarjetas.

Resolución de nombres no cualificados

La resolución de nombres no cualificados significa que se trata de una resolución hecha sobre la base de un nombre que no tiene la forma de un FQDN. Para responder a esta problemática, tenemos la posibilidad de configurar los parámetros DNS para que el cliente DNS soporte la aclaración de la solicitud. Se ofrecen las opciones siguientes al administrador:

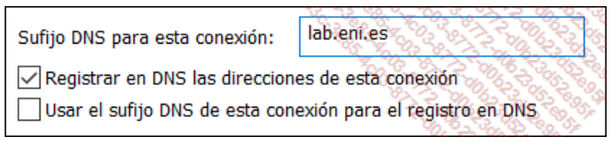
- Añadir los sufijos DNS principales, y específicos de la conexión, al nombre no cualificado para las consultas DNS.
- Añadir una serie de sufijos DNS configurados al nombre no cualificado para las consultas DNS.

- Sufijos DNS específicos de la conexión.

Cada conexión de red puede ser configurada de forma que tenga su propio sufijo DNS y más de un sufijo DNS principal añadido a las propiedades del equipo.

Comportamiento de las actualizaciones dinámicas DNS

Por defecto, cada conexión de red dispone de una gestión totalmente autónoma. De esta manera, es posible tener un gran control del comportamiento del equipo en entornos complejos compuestos de múltiples interfaces de red. Si configuramos un sufijo DNS específico para la conexión, también podemos activar la actualización dinámica DNS del nombre de dominio y las direcciones IP de la conexión.



Control de los registros y del sufijo DNS de cada conexión

La primera opción de **Registrar las direcciones de esta conexión en DNS** significa que la dirección o direcciones IP de la conexión se registran en relación con el nombre completo del equipo, según lo especificado en las propiedades de identificación del -ordenador. En nuestro ejemplo, esto significa que el registro del nombre de host **vm10-001** será registrado en el dominio **corpnet.priv** con las direcciones IP de la conexión concerniente. Por defecto, esta opción está activada y permite registrar el nombre del equipo, considerando el sufijo principal del equipo, es decir el nombre más significativo. La segunda opción **Usar el sufijo DNS de esta conexión en el registro de DNS** significa que el registro del nombre de host **vm10-001** será registrado en el dominio **lab.eni.es**. Observe que esta opción no está activa por defecto. Si no deseamos utilizar la funcionalidad de grabación dinámica DNS, podemos de igual forma desactivar por completo estas actualizaciones. Para esto, desactivamos las opciones **Registrar en DNS las direcciones de esta conexión** y **Usar el sufijo DNS de esta conexión en el registro de DNS**para todas las conexiones de red del equipo.

Para efectuar esta operación, debemos ser miembros del grupo administradores o del grupo de operadores de configuración de red en el equipo local.

Definición de un método de gestión de los sufijos DNS

Acabamos de ver que los sufijos DNS permiten ayudar a obtener una mejor resolución de nombres DNS cuando éstos no están plenamente cualificados. También hemos observado que el orden de estas declaraciones puede tener un efecto significativo sobre la pertinencia de las resoluciones. Por último, es evidente que sería conveniente garantizar una uniformidad de estos parámetros a nivel de toda la empresa o de los diferentes departamentos que la componen. La mejor solución consiste en implementar los parámetros que se hayan configurado empleando una directiva de grupo adaptada.

Es raro que un puesto de trabajo disponga de más de una interfaz de red pero no será el caso con los equipos portátiles todos equipados con una tarjeta de red Ethernet y una conexión integrada Wi-Fi. En los equipos de tipo servidor, las configuraciones multitarjeta son más frecuentes y deberán definirse de forma específica.

Cuando un equipo está equipado con más de una tarjeta de red, se habla de una máquina de tipo "multihomed". Este término significa que el equipo existe varias veces en la misma o en diferentes redes. Este tipo de configuración puede provocar diversos problemas de resolución o de conexiones en función de la topología de red (direcciones IP, cortafuegos, …). De hecho, salvo para las configuraciones donde no se configuran tarjetas en team LACP o independiente del conmutador, no es recomendable usar el modo "multihomed". Tenga en cuenta que cuando las tarjetas de red están conectadas en la misma red local, entonces se hablará de conexiones de tipo "multinets".

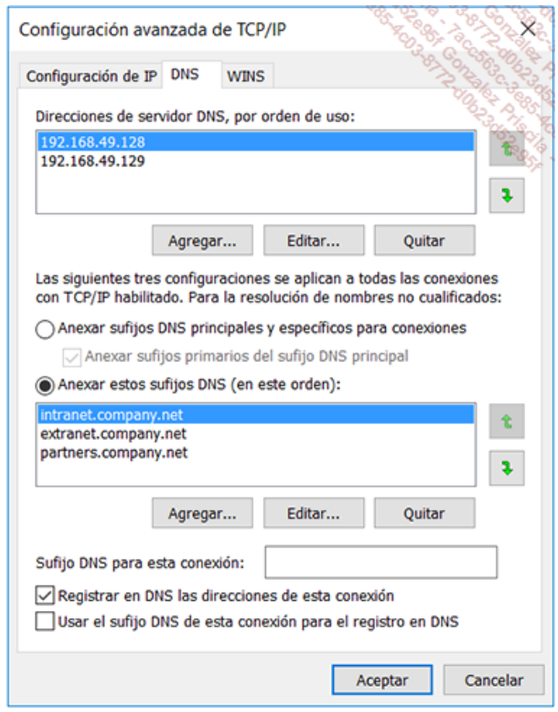
La imagen siguiente ilustra el conjunto de parámetros generales específicos del servicio DNS, que presentamos de forma rápida a continuación:

- Las direcciones de los servidores DNS se listan en función de su orden. En este ejemplo, la dirección 192.168.49.128 es la del servidor DNS preferido, mientras que la dirección 192.168.49.129 corresponde a la dirección del servidor secundario.
- Tal y como se especifica en la interfaz, los tres siguientes parámetros son comunes a todas las conexiones de red del equipo para las que el protocolo TCP/IP está activado. Estos parámetros son **Anexar sufijos DNS principales y específicos para conexiones** ; nos permiten especificar si los sufijos principales del sufijo DNS principal se utilizan. Por último, la última opción concierne a la posibilidad de especificar nuestros propios sufijos mediante la opción **Anexar estos sufijos DNS (en este orden)**.

Estos tres parámetros se refieren a todas las tarjetas relacionadas con el protocolo TCP/IP.

- La declaración del parámetro **Sufijo DNS para esta conexión** permite especificar un nombre de dominio DNS que podrá ser registrado, si es necesario.
- La opción **Registrar en DNS las direcciones de esta conexión** permite asegurar que las direcciones IP de esta conexión se registren para el nombre DNS correspondiente al nombre principal del equipo. Recordemos que el nombre principal del equipo puede verse empleando el comando `ipconfig /ALL` y depende directamente de la pertenencia al dominio Active Directory a través del icono**Puesto de trabajo/Propiedades/Nombre del ordenador**.

El último parámetro **Usar el sufijo DNS de esta conexión para el registro en DNS** nos permitirá registrar dinámicamente el nombre plenamente cualificado del equipo en base al sufijo de la conexión. En este caso, el equipo existe dos veces. Por primera vez en la zona que corresponde al nombre de dominio de pertenencia del equipo y la segunda vez en la zona especificada como sufijo para dicha conexión. Por supuesto, es necesario que esta zona exista y autorizar las actualizaciones dinámicas.



Gestión manual de los sufijos DNS

Configuración de los parámetros de sufijos DNS empleando directivas de grupo

La gestión de los parámetros TCP/IP puede ser larga y pesada, causando inevitables errores humanos. Este hecho tuvo sin duda un impacto en el evidente auge del protocolo DHCP (*Dynamic Host Configuration Protocol*) para ayudar a la correcta configuración de los equipos de red.

Si bien es cierto que el protocolo DHCP soporta los parámetros indispensables para el protocolo IP y también en la parte cliente del servicio de resolución DNS, los objetos de directivas de grupo permiten controlar de forma más fina y distribuir sus "mejores" parámetros en el conjunto de la red. Encontrará los parámetros más interesantes en la ubicación que aparece a continuación: Configuración del Equipo\Plantillas administrativas\Red\cliente DNS.

Los parámetros más importantes se listan a continuación:

Sufijo DNS principal: este parámetro especifica el sufijo DNS principal de todos los equipos afectados por la directiva. El sufijo DNS principal se utiliza para la inscripción de nombres DNS y la resolución de nombres DNS. Este parámetro permite especificar un sufijo DNS principal para un grupo de equipos e impide que los usuarios, incluidos los administradores, lo modifiquen. Si deshabilitamos este parámetro o no lo configuramos, cada equipo usará su sufijo DNS principal local, que es por lo general el nombre DNS del dominio Active Directory al que se une. Sin embargo, los administradores pueden usar el icono Sistema del panel de control para cambiar el sufijo DNS principal de un equipo.

Este parámetro no desactiva el cuadro de diálogo **Sufijo DNS y el nombre de equipo NetBIOS** que los administradores usan para modificar el sufijo DNS principal de un equipo. Sin embargo, si los administradores introducen un sufijo, este sufijo se ignora si el parámetro está activado.

Para que las modificaciones de este parámetro surtan efecto, el sistema deberá ser reiniciado.

Actualización dinámica: este parámetro determina si la actualización automática está activada. Los equipos configurados para permitir la actualización automática graban y actualizan sus registros de recursos DNS en un servidor DNS. Si habilitamos esta opción, los equipos a los que se aplica este parámetro pueden utilizar el registro DNS dinámico para cada una de sus conexiones de red, según la configuración de cada conexión de red individual. Para activar el registro DNS dinámico en una conexión de red específica, es necesario que las configuraciones específicas de la conexión y específicas del equipo permitan el registro DNS dinámico.

Este parámetro controla la propiedad específica del equipo que controla el registro DNS dinámico. Si habilitamos esta opción, permitimos la definición de la actualización automática de forma individual en cada una de las conexiones de red.

Si deshabilitamos esta opción, los equipos a los que se aplica este parámetro no podrán utilizar el registro DNS dinámico para todas sus conexiones de red, sea cual sea la configuración de cada conexión de red individual.

Lista de búsqueda de sufijos DNS: este parámetro determina los sufijos DNS a asignar a un nombre simple no cualificado antes de presentar una solicitud DNS para ese nombre. Un nombre simple no cualificado no contiene puntos, se trata pues de un nombre corto y por lo tanto, diferente de un nombre de dominio totalmente cualificado, tal como "europe.corporate.com".

Si seleccionamos esta opción, podemos especificar los sufijos DNS a añadir antes de presentar una solicitud para un nombre simple no cualificado. Los valores de los sufijos DNS en este parámetro pueden definirse mediante el uso de cadenas separadas por comas, tales como microsoft.com, office.microsoft.com. Un sufijo DNS se añade para cada envío de una solicitud. Si una solicitud no es resuelta, un nuevo sufijo DNS se añadirá en lugar del sufijo erróneo y esta nueva solicitud será enviada. Los valores se utilizan en el orden en que aparecen en la cadena, comenzando por el valor más a la izquierda y continuando hacia la derecha.

Nivel de seguridad de las actualizaciones: este parámetro especifica si equipos a los que este parámetro se aplica utilizan la actualización dinámica segura o la actualización dinámica estándar para la grabación de los registros DNS. Para activar este parámetro, haga clic en**Habilitar** y seleccione uno de los valores siguientes:

- **No seguras seguidas de seguras**: si seleccionamos esta opción, los equipos envían actualizaciones dinámicas seguras solo cuando las actualizaciones dinámicas no seguras son rechazadas.
- **Solo no seguras**: si seleccionamos esta opción, los equipos envían solo actualizaciones dinámicas no seguras.
- **Solo seguras**: si seleccionamos esta opción, los equipos envían solo actualizaciones dinámicas seguras.
- **Intervalo de actualización de registro**: este parámetro especifica el intervalo de actualización de los registros de recursos A y PTR para los equipos a los que se aplica este parámetro. Este parámetro puede aplicarse solo a los equipos que utilizan las actualizaciones dinámicas.

Los equipos Windows basados en Windows 2000 hasta Windows 10 configurados para efectuar los registros DNS dinámicos graban de forma periódica sus registros DNS, aunque sus datos de registro no hayan cambiado. Este regrabación es necesaria para indicar a los servidores DNS configurados para eliminar los registros obsoletos de forma automática que estas grabaciones están siempre al día y deben conservarse dentro de la zona DNS.

Si los registros de recursos DNS son grabados en las zonas donde la limpieza está activada, el valor de este parámetro no debería ser mayor que el intervalo de actualización configurado para estas zonas.

Establecer un intervalo de actualización de registro más largo que el intervalo de actualización de las zonas DNS podría provocar la eliminación no deseada de los registros de recursos A y PTR. Observe que el valor por defecto declarado es de 1800 segundos, lo que corresponde a 30 minutos.

4. Solicitudes de resolución DNS y NetBIOS: Proceso de selección del método

Cuando un ordenador Windows intenta resolver un nombre en una dirección IP, el módulo de resolución transmitirá con mayor prioridad la demanda de resolución al sistema de resolución DNS. Este punto es en especial importante, ya que se trata de un cambio radical en los sistemas Windows 2000 y posteriores en comparación con Windows NT.

En el caso de que la demanda de resolución DNS falle, el módulo de resolución controla la longitud del nombre solicitado. Si la longitud es superior a 15 bytes, es decir 15 caracteres, entonces no puede ser enviada a la interfaz NetBIOS y la resolución falla. Si por contra, el nombre solicitado es de una longitud inferior a 15 caracteres entonces el módulo de resolución verifica que la interfaz de resolución NetBIOS está activa. Si se verifica este punto, entonces el módulo de resolución remitirá la solicitud a la interfaz NetBIOS.

Hemos visto antes que los sistemas operativos Microsoft Windows 2000 y las versiones posteriores soportan varios métodos de resolución de nombres como DNS, WINS, los archivos Hosts y Lmhosts y los mensajes de difusión (broadcasts). En general, un equipo con Windows 10 invoca una combinación de estos diferentes métodos de resolución -con preferencia en los mecanismos de resolución DNS.

5. Prueba de integración en Active Directory

Podemos utilizar DCdiag.exe y Netdiag.exe para resolver los problemas de los equipos cliente que no pueden localizar un controlador de dominio. Estas herramientas pueden ayudarnos a determinar las configuraciones erróneas DNS tanto del lado del cliente como del lado del servidor.

Ya hemos presentado en detalle el comando `Netdiag` en el marco de los comandos de gestión y supervisión de los servicios DNS.

Con respecto a los entornos Active Directory, el comando `DCdiag` nos permitirá avanzar a grandes pasos cuando se trate de diagnosticar posibles problemas de funcionamiento de los equipos específicos que son controladores de dominio Active Directory.

El comando `DCdiag` permite comprobar el funcionamiento de las funciones vitales de Active Directory ofreciendo efectuar una serie de pruebas adaptadas a cada situación crítica. Así tenemos, por ejemplo, la posibilidad de seleccionar los controladores de dominio a probar, así como diferentes categorías de pruebas.

Estas pruebas se clasifican en las tres categorías siguientes y luego detalladas más adelante:

- Las pruebas obligatorias de controladores de dominio que no pueden ser desactivados.
- Las pruebas no obligatorias de controladores de dominio que podemos elegir según nos convenga.
- Las pruebas de equipos que no son controladores de dominio.

Las pruebas obligatorias del comando `DCdiag` incluyen el control de los registros DNS de los controladores, la posibilidad de establecer contacto, así como la verificación del buen funcionamiento de la conectividad LDAP y RPC.

Todas las pruebas especificadas antes solo pueden ser realizados en los controladores de dominio Windows 2000 hasta Windows Server 2016 con la excepción de las pruebas DcPromo RegisterInDNS que solo pueden ser ejecutadas en equipos que no son controladores de dominio.

Para obtener más información sobre la integración de los equipos en los dominios Active Directory, así como sobre la creación de controladores de dominio, consulte el artículo KB 265706 "DCDiag y NetDiag para facilitar la unión a dominios y la creación de controladores de dominio" en la Base de conocimientos de Microsoft.

Novedades de los servicios DNS de Windows Server

1. Servicios DNS de Windows Server 2008 R2

a. Introducción

Windows Server 2008 y Windows Server 2008 R2 implementan los servicios de resolución y gestión de dominios DNS en la forma de un nuevo rol de servidor. Por supuesto, esto es lo mismo con Windows Server 2016 sabiendo que los servicios DNS de Windows Server 2008 y Windows Server 2008 R2 han aportado las nuevas funcionalidades siguientes:

- La carga de zonas en segundo plano: la disponibilidad de los servidores DNS ha mejorado durante el reinicio del servicio DNS cargando los datos de zonas directamente en segundo plano.
- Soporte del protocolo IPv6: los servicios DNS soportan de forma completa la especificación final IPv6 y las direcciones de 128 bits.
- Soporte de los RODC: los servicios DNS asumen un nuevo concepto que permite soportar los servicios DNS dinámicos sobre los RODC. Estas zonas se denominan zonas primarias de sólo lectura - RODC Read-only zones.
- Zonas de tipo GNZ: este nuevo tipo de zona DNS - GNZ (*Global Naming Zone*) proporciona el soporte de nombres globales (Global Single Names). Las zonas GNZ permiten la resolución de nombres de tipo sencillo (single-label name resolution), para las empresas que no desean desplegar los servicios WINS o cuando no es práctico especificar nombres DNS completos.

Los clientes Windows 7 y los servidores Windows Server 2008 R2 soportan las extensiones de seguridad DNS (DNSSEC). DNSSEC permite la firma de una zona DNS y todos sus registros. De esta manera un cliente puede obtener la clave pública del par de claves pública/privada usadas y confirmar que la respuesta remitida por el servidor es auténtica.

El soporte DNSSEC se realiza a través de la implementación de la RFC 4033, 4034 y 4035, y el soporte de cuatro nuevos registros de recursos (DNSKEY, RRSIG NSEC, y DS).

Estas nuevas características se detallan a continuación.

b. Carga de las zonas en segundo plano

Las grandes empresas pueden verse obligadas a gestionar zonas DNS muy voluminosas. Cuando estas zonas están almacenadas en Active Directory y el controlador de dominio debe ser reiniciado, el tiempo de arranque de los servicios Active Directory y luego la carga de datos de las zonas puede hacer que los servicios DNS no están disponibles para los clientes de la red durante un tiempo a veces superior a entre treinta y sesenta minutos.

Los servidores DNS de Windows Server 2008 ahora pueden cargar los datos DNS en segundo plano. Durante el inicio del servicio las siguientes operaciones se realizan en este orden:

- Análisis del conjunto de las zonas a cargar.
- Carga de los indicadores de raíz a partir del archivo Cache.dns o el almacenamiento de Active Directory.
- Carga de los datos de las zonas almacenadas en los archivos de zona.
- Arranque de las funciones de respuestas DNS y del soporte RPC.
- Inicio de las funciones de carga de las zonas almacenadas en las particiones de Active Directory.

En este momento las zonas DNS Active Directory se cargan en paralelo empleando varios threads. De esta forma, el servicio DNS puede responder a las peticiones de resolución de los clientes durante la carga.

Cuando las solicitudes de resolución no pueden ser satisfechas al no estar presentes en la memoria, el servicio DNS busca de forma directa los datos a partir de la base de datos Active Directory, mientras que la carga continúa. Esta funcionalidad acelera aún más la carga.

c. Soporte de las direcciones IPv6

Las direcciones IPv6, a diferencia de las direcciones IPv4 que están organizadas en 32 bits, se formatean en 128 bits. En adelante, los servicios DNS de Windows Server 2008 soportan por completo la especificación final del protocolo IPv6 y las direcciones de 128 bits. Esto es lo mismo para el comando dnscmd que acepta direcciones IP en ambos formatos. El servidor DNS puede utilizar reenviadores cuyas direcciones estén en los dos formatos.

Por último, las zonas de búsqueda inversa específicas a las direcciones IPv6 serán soportadas a través de la zona inversa ip6.arpa.

El soporte del protocolo IPv6 por los servicios DNS de Windows Server 2008 y las versiones posteriores no es, hasta la fecha, de una gran importancia. Pero está claro que esto podrá ser el caso en los próximos años como consecuencia del desarrollo de la red Internet y su adhesión a IPv6.

En relación con el soporte de IPv6: como los servidores DNS pueden hoy responder a las solicitudes de resolución de los clientes utilizando las direcciones IPv4 (A) y también las direcciones IPv6 (AAAA), es necesario asegurarse de que la parte cliente DNS de los puestos de trabajo soporta estas respuestas.

d. Soporte de DNS de los controladores de dominio en solo lectura

El objetivo principal de los controladores de dominio en solo lectura es reforzar la seguridad de los controladores de dominio en las que se autoriza a recibir datos solo desde otro Controlador de dominio, y en modo alguno de forma directa. De esta manera, las fuentes de escritura son conocidas y controladas, y el contralor es mucho menos vulnerable a ataques.

Para garantizar un buen funcionamiento de los servicios DNS en esos servidores disponibles sólo en modo lectura, Windows Server 2008 R2 y versiones posteriores introducen un nuevo tipo de zonas denominadas zonas primarias de sólo lectura.

Estas zonas son también llamadas "Branch Office Zones".

Durante la instalación de un controlador de dominio en modo sólo lectura, el nuevo controlador recibe una replicación completa de sólo lectura (RO) de las particiones de dominio, de esquema, de configuración, y por supuesto, de todas las particiones ForestDNSZones/DomainDNSZones utilizadas por los servicios DNS. Luego, las inscripciones y otras actualizaciones dinámicas serán implementadas de la siguiente manera:

- El servidor DNS no acepta la actualización de los clientes de forma directa.
- Las solicitudes de escritura DNS de los clientes serán remitidas a un servidor DNS con autoridad.
- Los datos actualizados son por último recibidos mediante la replicación desde un servidor DNS con autoridad.

El soporte "desviado" de las inscripciones y actualizaciones dinámicas en los controladores de tipo RODC es una característica importante porque permite desplegar este tipo de controladores sin debilitar la seguridad, ni introducir limitaciones funcionales en la infraestructura DNS

dinámica.

e. Soporte de las zonas de tipo GlobalNames

La mayoría de las redes Windows utilizan hoy en día los sistemas de nombres DNS, los sistemas de resolución de nombres DNS, y también los mecanismos de resolución WINS.

Hoy en día, los nombres IP-DNS son utilizados de manera amplia, aunque algunas aplicaciones utilizan todavía la interfaz NetBIOS y los mecanismos de resolución DNS y/o WINS.

¡Observe! No hay que confundir la interfaz NetBIOS, en el sentido de programación del término, y un sistema de registro y de resolución de nombres NetBIOS, tal como el servicio WINS.

Por razones históricas totalmente aceptables, y también razones técnicas inherentes a las plataformas Windows NT o compatibles con NT, es frecuente que las empresas sigan implementando WINS en sus redes. En tales casos, WINS es considerado como un sistema de resolución secundario, detrás de los servicios DNS.

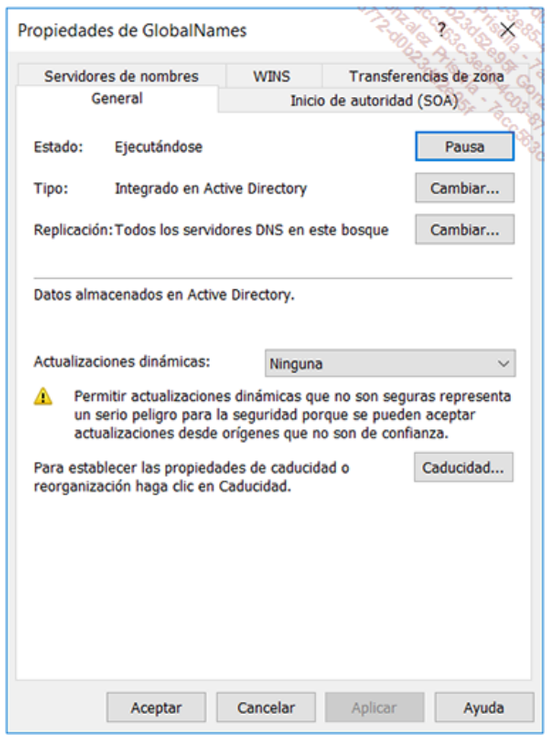
Además el hecho de que la interfaz NetBIOS, los nombres NetBIOS y los mecanismos propios del sistema de resolución WINS están cerca de la obsolescencia, no es menos cierto que algunos principios son todavía muy apreciados por los administradores de Windows, en particular la facilidad de declaración de nombres estáticos sencillos y el poder hacerlos disponibles de forma global a escala empresarial.

Para responder a estas problemáticas, los servicios DNS de Windows Server 2008 R2 y versiones posteriores permiten a las empresas considerar una transición total del entorno WINS existente hacia un entorno completamente DNS sin dejar de soportar un espacio de nombres plano de tipo etiqueta simple dentro de la nueva zona DNS Global Names.

Un nombre de tipo etiqueta simple frente a los nombres compuestos de múltiples etiquetas. Por ejemplo, portal01 es un nombre de etiqueta simple (simple label), mientras que portal01.corpnet.priv es un nombre de etiquetas múltiples (multilabels).

Contenido de la zona (GlobalNames)

En general, los nombres simples contenidos en una zona de tipo GlobalNames deberían estar contenidos en una zona de Active Directory replicada a escala del bosque. De esta manera, un ámbito de resolución único puede ser ofrecido de forma global. Tenga en cuenta que es posible publicar un registro DNS de tipo SRV para declarar la existencia de varias zonas GlobalNames contenidas en varios bosques Active Directory.



Características de una zona de tipo GNZ (Global Names Zone).

A diferencia de los servicios WINS, las zonas DNS GlobalNames deben utilizarse solo para que el DNS pueda resolver un conjunto limitado de nombres de tipo etiqueta simple. Puede tratarse de algunos servidores cuyos nombres serán gestionados de manera muy centralizada.

¡Observe! Microsoft recomienda no utilizar la zona GlobalNames en lugar de las resoluciones habituales. Observe también que las actualizaciones dinámicas no están soportadas en la zona GlobalNames. En comparación con las operaciones de administración de WINS, la zona GlobalNames debería contener el equivalente de los registros estáticos WINS.

Cuando desplegamos una zona de tipo GlobalNames, una resolución de tipo etiqueta simple se realiza del modo siguiente:

- Una solicitud de resolución basada en un nombre corto, es decir, de tipo etiqueta simple, se inicia.

- El sufijo principal del puesto de trabajo se añade al nombre corto y se transmite la petición al servidor DNS.
- Si la demanda basada en un FQDN fracasa, entonces el cliente genera otras peticiones basadas en los sufijos DNS adicionales, declarados de forma local o a través de GPO.
- Si estas peticiones fallan entonces el cliente realiza una petición basada en el nombre corto.
- Si el nombre corto solicitado aparece en la zona GlobalNames, el nombre es resuelto.
- Si el nombre corto solicitado no aparece en la zona GlobalNames, entonces la demanda de resolución se transmite a WINS.

Ninguna actualización específica se requiere en los puestos cliente para que puedan resolver nombres de la zona GlobalNames. El sufijo DNS principal, los sufijos DNS específicos a las conexiones y la lista de búsqueda de sufijo DNS siguen funcionando de forma normal.

Las actualizaciones dinámicas no están soportadas en la zona GlobalNames. Sin embargo, cabe señalar que las actualizaciones dinámicas enviadas a un servidor DNS en primer lugar se comparan con los datos de la zona GlobalNames antes de ser comparados con los datos de zona local. Este control permite garantizar la unicidad de los nombres presentes en la zona GlobalNames.

f. Evolución de la parte Cliente DNS

Acabamos de ver que los servicios DNS de Windows Server 2008 R2 y versiones posteriores, tales como Windows Server 2016 soportan nuevas funcionalidades para satisfacer las nuevas demandas. Aunque no haya consecuencias directas en términos de infraestructura, conviene señalar que a partir de Windows Vista y hasta las versiones más modernas como Windows 10, los cambios en la parte cliente DNS se han introducido a su vez.

Windows Vista, Windows Server 2008 y las versiones posteriores soportan LLMNR (*Link-Local Primary Name Resolution*): ahora es posible mediante esta nueva evolución del cliente DNS resolver nombres DNS utilizando un mensaje de red de tipo multicast local. Este método, también llamado mDNS, para Multicast DNS, permite a los clientes que soportan esta característica resolver nombres DNS de una red local cuando el o los servidores DNS habituales no están disponibles. Una vez que los servicios DNS se encuentren otra vez disponibles, los mecanismos de resolución habituales se reanudan de forma normal.

El soporte del protocolo LLMNR ofrece un nuevo método para minimizar los efectos de los fallos en los servicios DNS. Tenga en cuenta que también puede tratarse de un método de resolución para las redes ad hoc tales como las salas de conferencia, zonas de libre acceso, etc..

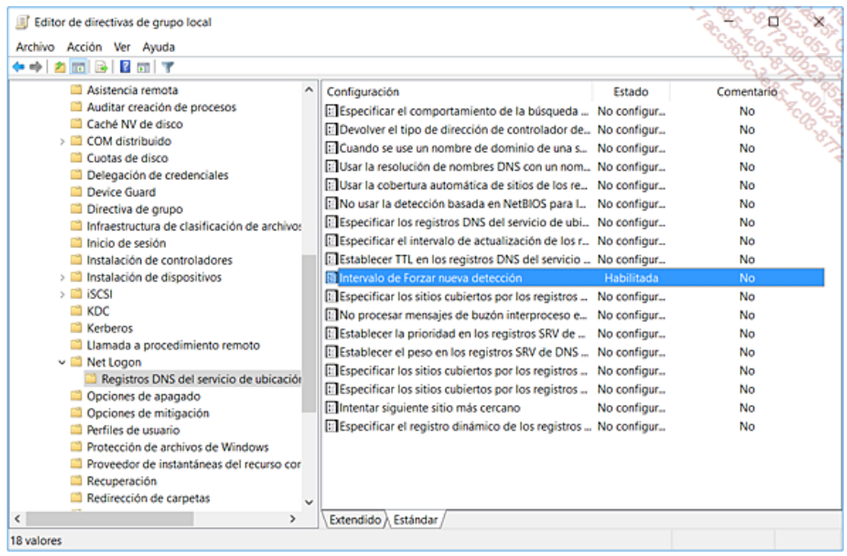
g. Selección de los controladores de dominio

Windows Vista, Windows Server 2008 y las versiones posteriores, tales como Windows 10 y Windows Server 2016, incorporan modificaciones relativas a la selección de los controladores de dominio para reducir su impacto en el rendimiento de la red.

En los sistemas más antiguos como Windows XP o Windows Server 2003, el sistema local conserva el nombre del controlador de dominio seleccionado hasta que un evento fuerza a descubrir otro controlador de dominio.

Las versiones posteriores de estos sistemas refrescan de forma periódica los datos relativos a los controladores de su dominio de pertenencia. Este nuevo método permite hacer frente a los problemas que pueden surgir cuando un puesto cliente intenta localizar a su controlador de dominio favorito cuando la red o algunas circunstancias no lo permiten. El hecho de renovar periódicamente la asociación permite que el puesto cliente minimice la probabilidad de estar asociado a un controlador de dominio inadecuado disponiendo del contralor que mejor se adapte a la situación.

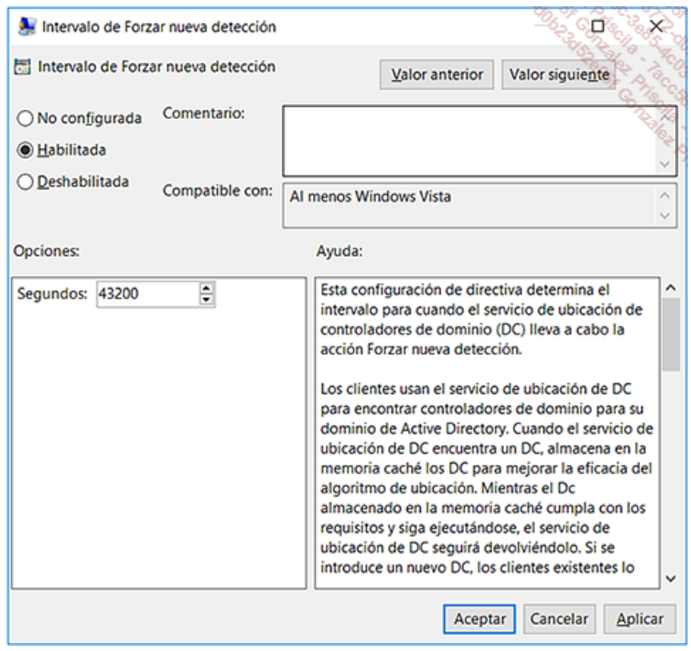
La imagen siguiente muestra la configuración del período de refresco empleando objetos directiva de grupo con el parámetro **Intervalo de Forzar nueva detección** disponible para sistemas Windows Vista, Windows Server 2008 y las versiones posteriores, tales como Windows 10 y Windows Server 2016.



Nuevo parámetro "Intervalo de Forzar nueva detección".

Para adaptarse al cambio de condiciones de la red, el localizador de controladores de dominio ejecuta por defecto una búsqueda forzada en función de un intervalo especificado. Asegura también el equilibrio de carga de los clientes en todos los controladores disponibles en los dominios o bosques. El intervalo por defecto de la detección forzada por el localizador es de 12 horas. La detección forzada también puede activarse si se llama al localizador de controladores de dominio utilizando el indicador DS_FORCE_REDISCOVERY.

Si se activa este parámetro de directiva, el localizador de controladores de dominio para el equipo ejecuta una detección forzada de forma periódica en función del intervalo configurado.



El intervalo mínimo es de 3.600 segundos (1 hora) para evitar un tráfico de red excesivo debido a la búsqueda. El intervalo máximo autorizado es de 4.294.967.200 segundos, y cualquier valor superior a 4.294.967 segundos (~49 días) es tratado como un número infinito. Si este parámetro de directiva está inhabilitado, la opción **Forzar intervalo de nueva detección** se utiliza por defecto para el equipo cada doce horas. Si este parámetro de directiva no está configurado, la opción **Forzar la detección** se utiliza por defecto para el equipo cada doce horas, salvo si el valor del parámetro del equipo local en el Registro es diferente.

2. Novedades de Windows Server 2012 R2

Windows Server 2012 R2 incorpora cambios en términos de rendimiento y seguridad. Encontraremos a continuación el conjunto de nuevas funcionalidades del servicio servidor DNS para Windows Server 2012 R2:

- Soporte mejorado del Protocolo DNSSEC para el soporte de las extensiones de seguridad DNS. Windows Server 2012 R2 soporta la gestión de claves automatizadas.
- Soporte de escenarios de DNS integrados en Active Directory con el soporte de -actualizaciones dinámicas en las zonas firmadas DNSSEC.
- Adición del soporte de protocolos NSEC3 y RSA/SHA-256 con DNSSEC.
- Distribución automatizada de los anclajes de seguridad a través de Active Directory.
- Renovación automática de los anclajes de seguridad según la RFC 5011.
- Soporte de reenviadores DNS dinámicos: esta nueva funcionalidad reorganiza la lista de reenviadores declarados en función del tiempo de respuesta de cada servidor. Las operaciones de reorganización están activadas por defecto, pero pueden ser desactivadas empleando la clave de registro HKLM \ System \ CurrentControlSet \ Servicios \ DNS \ Parameters \EnableForwarderReordering.

Además de estas mejoras en torno al soporte del protocolo DNSSEC, se ha ampliado la configuración y gestión DNS a través de Windows PowerShell.

Para más detalles sobre las mejoras en los servicios DNS de Windows Server 2012 R2, busque en el sitio de Microsoft Technet "Novedades de DNS".

3. Novedades de Windows Server 2016

El servicio DNS de Windows Server 2016 introduce una nueva funcionalidad llamada directivas DNS. Esta característica permite a los administradores resolver algunos problemas relacionados con la gestión del tráfico, el equilibrio de carga o condicionar las respuestas DNS en función de determinados parámetros del entorno.

Estas directivas, declaradas mediante Windows PowerShell, permiten al administrador especificar cómo un servidor DNS responde a las peticiones de resolución DNS de los clientes. A través de estas nuevas directivas, las respuestas pueden variar en función de los siguientes parámetros:

- Alta Disponibilidad: con este tipo de directiva, los clientes DNS son redirigidos al mejor equipo para una determinada aplicación.
- Gestión del tráfico: los clientes DNS son redirigidos al centro de datos más cercano.
- Zonas DNS divididas: los registros DNS se dividen en diferentes zonas. Los clientes DNS reciben una respuesta en función de su ubicación interna o externa.
- Filtrado: las consultas DNS pueden ser bloqueadas a partir de una lista con direcciones IP o nombres DNS considerados maliciosos.
- Aspectos legales: los clientes DNS que fueron identificados como maliciosos son redirigidos hacia un señuelo en lugar del equipo que tratan de alcanzar.
- Redirección en función de horarios: los clientes DNS pueden redirigirse hacia determinadas regiones o Datacenter a determinadas horas.

Los dos ejemplos siguientes ilustran toda la potencia de estas nuevas directivas DNS:

- Ejemplo 1 - Bloqueo de las solicitudes de resolución DNS de un dominio DNS particular: este ejemplo permite denegar las respuestas a las solicitudes de resolución en el dominio research.corpnet.priv.

```
Add-DnsServerQueryResolutionPolicy -Name "Block-DNS-Research-Policy"
-Action IGNORE -FQDN "EQ,*.research.corpnet.priv"
```

- Ejemplo 2 - Bloqueo de las solicitudes de resolución DNS para una subred IP específica considerada ilícita: este ejemplo bloquea las solicitudes de resolución procedentes de la red IP 10.1.0.0/16.

```
Add-DnsServerClientSubnet -Name "Blocked-IP-Subnet-10-1" -IPv4Subnet
10.1.0.0/16
Add-DnsServerQueryResolutionPolicy -Name "Block-IP-Subnet-10-1-Policy"
```

```
-Action IGNORE -ClientSubnet "EQ,Blocked-IP-Subnet-10-1"
```

Recomendación: las nuevas directivas DNS permiten gestionar las problemáticas específicas en entornos que pueden ser muy distintos unos de otros. Por esta razón, es necesario definir con precisión los objetivos de filtrado a alcanzar y probar el comportamiento de las resoluciones DNS. Una vez que el comportamiento alcance las expectativas, será posible realizar un despliegue en el entorno de producción.

Para más detalles sobre las mejoras en los servicios DNS de Windows Server 2016, busque en el sitio de Microsoft Technet "What's New in DNS Server in Windows Server 2016" o "DNS Policies Overview" a través del enlace siguiente: https://technet.microsoft.com/en-us/library/mt169379(v=ws.11).aspx

Introducción

Acabamos de ver que las zonas DNS estándar existen en forma de archivos que son por lo general almacenados en \system32\dns. La idea consiste ahora en abandonar este almacenamiento para usar el ofrecido por los servicios de directorio Active Directory. Antes de entrar en los detalles de esta integración, conviene señalar que Active Directory y DNS manipulan los nombres que parecen idénticos, pero que en realidad estos nombres pertenecen a espacios muy diferentes.

La tabla siguiente ilustra el paralelismo que existe entre los elementos que pertenecen a DNS y los que pertenecen a Active Directory.

Elementos de DNS	Elementos y objetos del directorio Active Directory
Almacenamiento de tipo archivo	Almacenamiento de tipo base de datos
Archivos de zona en \System32\dns	Objetos contenedores de tipo **dnsZone**
Registros de recursos (RR - *Resource Record*)	Objeto de tipo **dnsNode**

Así, podemos decir que el espacio DNS está compuesto por zonas, y registros de recursos en las zonas, mientras que el espacio Active Directory, llamado "bosque" en su -totalidad, está compuesto por dominios y objetos dentro de estos dominios.

A continuación listamos los objetos y atributos de Active Directory utilizados en el marco del servicio DNS:

DnsZone: se trata de un objeto contenedor creado en el momento en que se crea una zona en Active Directory.

DnsNode: se trata de un objeto utilizado para asignar un nombre a un registro que contendrá varios datos.

DnsRecord: se trata de un atributo de tipo multivalor asociado a la clase de objeto dnsNode. Se utiliza para almacenar los registros de recursos en el objeto dnsNode.

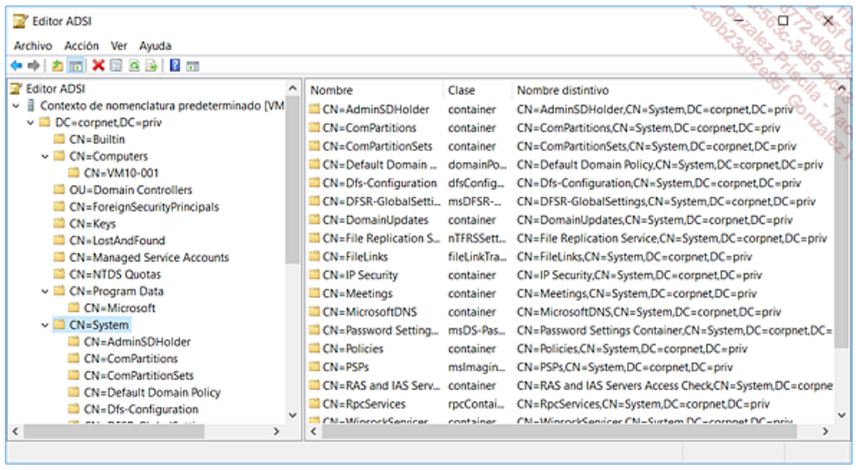
DnsProperty: se trata de un atributo de tipo multivalor asociado a la clase de objeto dnsNode. Se utiliza para almacenar la información de configuración de la zona.

Por último, cada zona integrada en el directorio se almacena en un objeto contenedor de tipo dnsZone, el cual se identifica con el nombre asignado a la zona en el momento de su creación.

Objetos equipo Active Directory y nombres

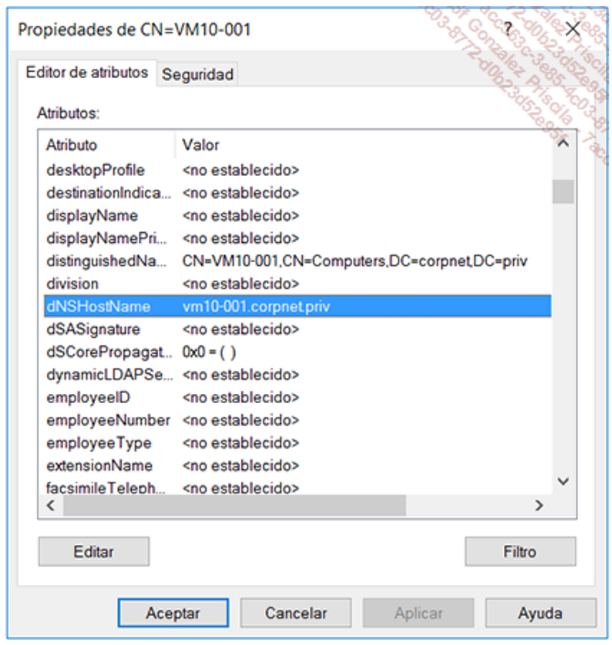
Cada equipo miembro de un dominio Windows Active Directory existe en forma de un objeto de tipo Computer. La figura siguiente muestra un equipo perteneciente a un dominio empleando la herramienta ADSI Edit.

El complemento ADSI Edit se encuentra integrado por defecto en Windows Server 2016 Podemos acceder a este ejecutando Adsiedit.msc o también a través del Administrador del servidor. Observe que esta herramienta de edición y modificación de los objetos contenidos en las particiones del directorio Active Directory existe desde hace muchos años y forma parte de las herramientas de soporte contenidas en el CD-ROM de Windows Server 2003 y Windows 2000 Server.



El equipo VM10-001 en el contenedor Computers del dominio Corpnet.priv.

Como objeto existente en el directorio Active Directory, sus propiedades existen en forma de atributos. Así, estos atributos son manipulados por el mismo directorio, por las aplicaciones o también por cualquier entidad habilitada para hacerlo. La siguiente imagen muestra la ventana para ver o modificar los atributos de un objeto, siempre con ADSI Edit.



Propiedades del objeto VM10-001 y valor del atributo dNSHostName

La tabla siguiente presenta los diferentes atributos de un objeto perteneciente a la clase computer y relacionado con la gestión de nombres.

Atributos del objeto	Designación y valor del atributo
canonicalName	Representa el nombre canónico Active Directory del objeto corpnet.priv/computers/vm10-001.
cn	Representa el nombre común LDAP del objeto vm10-001.
displayName	Representa el nombre de visualización LDAP del objeto vm10-001$.
distinguishedName	Representa el nombre distinto completo CN=vm10-001,CN=Computers,DC=corpnet,DC=priv.
dNSHostName	Representa el nombre DNS en la forma de un FQDN vm10-001.corpnet.priv.
name	Representa el nombre vm10-001.
sAMAccountName	Representa el nombre SAM (*Security Account Manager*) del equipo vm10-001$.
servicePrincipalName	Representa los nombres de las identidades (SPN, *Security Principal Names*) HOST/vm10-001 HOST/vm10-001.corpnet.priv.

Según explicado antes, esta tabla muestra que un equipo dentro de un dominio Windows existe en varios espacios de nombre distintos. Los atributos más importantes en términos de seguridad son **sAMAccountName** y **servicePrincipalName**, que pueden ser controlados mediante el comando de sistema **SetSPN.exe**.

Por supuesto, otros atributos mejorarán el directorio con información cuyo uso será más perceptible.

A continuación presentamos algunos ejemplos de atributos:

Atributos del objeto computer win10-001	Denominación y valor del atributo
objectCategory	CN=Computer,CN=Schema,CN=Configuration, DC=corpnet, DC=priv.
operatingSystem	Windows 10.

Ventajas de la integración de las zonas DNS en Active Directory

Los controladores de dominio Windows Server permiten al servicio DNS beneficiarse de los múltiples avances tecnológicos aportados por Active Directory. Estos avances se presentan a continuación.

1. Actualización a modo multimaestro (o maestros múltiples)

En el modelo habitual de almacenamiento de las zonas DNS, las actualizaciones son posibles solo hacia el servidor primario para la zona. De hecho, solo un servidor DNS que sirve de referencia para la zona se encuentra en modo lectura y escritura. Se trata de una gran limitación cuando se desea aprovechar actualizaciones DNS en forma dinámica.

Otro inconveniente del modelo DNS tradicional es que toda la disponibilidad de escritura de la zona se basa en este único servidor principal. Si el servidor no está disponible, entonces las peticiones de actualización formuladas por los clientes DNS no son tratadas para toda la zona. Además, cuando la zona expira en función del valor fijado en el registro SOA, ésta pasa al estado de expirado y no se trata ninguna solicitud de resolución DNS adicional.

Por contrario, cuando una zona DNS se integra en Active Directory y la zona está configurada para soportar actualizaciones dinámicas, entonces estas actualizaciones pueden a su vez ser soportadas en modo multimaestro. De hecho, todos los servidores DNS de tipo NS y controlador se convierten en una fuente principal para la zona. Por lo tanto, la zona puede ser actualizada por los servidores DNS que funcionan en cualquier controlador de dominio. Este concepto permite ofrecer una disponibilidad total, siempre que se disponga de varios controladores de dominio que funcionen como servidores DNS. Cabe señalar que sólo los controladores de dominio disponibles sólo en modo lectura, llamados en inglés RODC para *Read Only Domain Controllers*, constituyen la excepción a la regla.

2. Seguridad avanzada de los controles de acceso a las zonas y los registros

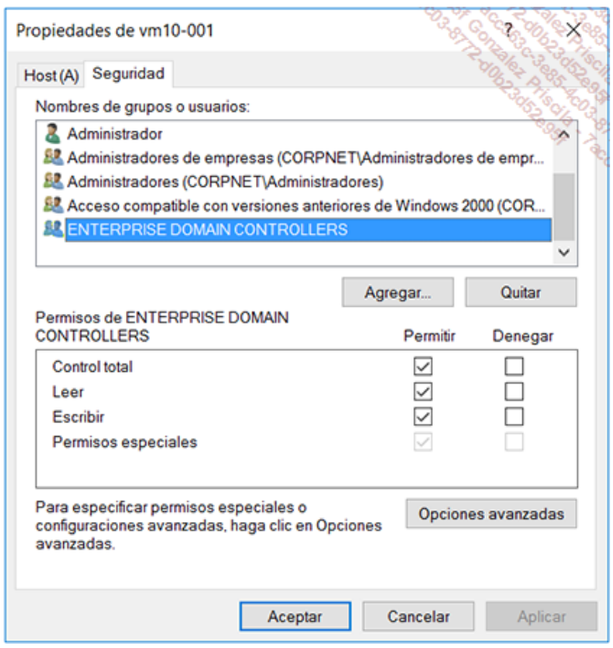
Cada registro de recurso DNS es un objeto Active Directory de tipo dnsNode. En este sentido existe y se aprovecha, como todos los otros tipos de objetos del directorio, de los servicios de seguridad de Active Directory. En nuestro caso, se tratará de autenticaciones mutuas utilizando el protocolo Kerberos v5 y el uso de los SPN. El soporte de las listas de control de acceso permite controlar quién puede hacer que sobre cada objeto, es decir, sobre cada registro DNS.

Por supuesto, todos estos objetos tienen permisos por defecto que securizan en entorno DNS, pero podemos por ejemplo acceder a las funciones de las ACL (*Access Control List*) para securizar de manera especial un contenedor dnsZone en el árbol de Active Directory. La granularidad de administración es muy fina, ya que, en función de las necesidades de seguridad, necesitaremos siempre la posibilidad de gestionar cada zona y cada registro dentro de una zona.

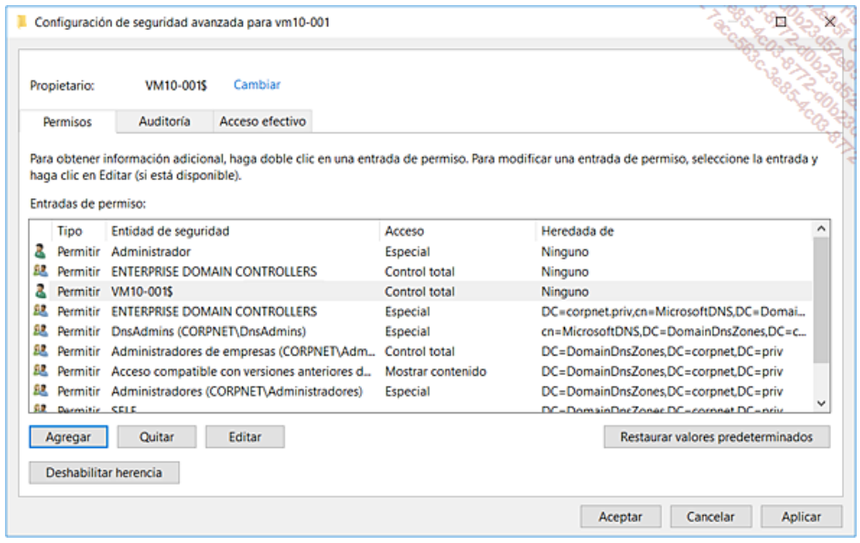
El grupo Integrado **Usuarios autentificados** dispone de una autorización de tipo **crear todos los objetos secundarios**. Esta ACL permite autenticar a todos los equipos Windows que soporte la autenticación Kerberos.

El grupo de seguridad **Usuarios autentificados** considera todas las entidades que puedan ser controladas ya se trate de objetos usuario, grupos u objetos de tipo equipo miembros del dominio Active Directory o de cualquier dominio aprobado.

Una lista de control de acceso por defecto securiza cada nuevo registro. La imagen siguiente muestra los permisos del registro que se refiere al equipo llamado VM10-001, miembro del dominio corpnet.priv.

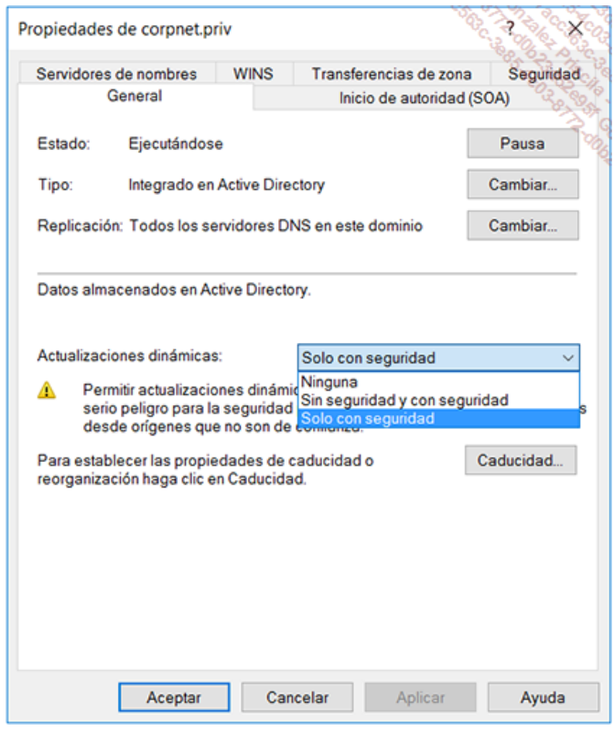


El Grupo ENTERPRISE DOMAIN CONTROLLERS posee la autorización de escritura en el objeto vm10-001



Se aprecia por lo tanto, que al principio, todos los equipos autenticados mediante el protocolo Kerberos podrán crear de forma dinámica su propio registro. Una vez creado, los controladores de dominio de la empresa podrán modificar el registro, siempre por cuenta del cliente. En el caso de un entorno de red en particular seguro, podemos especificar nuestros propios permisos para que las actualizaciones dinámicas no estén autorizadas para un equipo cliente específico. Este podría ser el caso para un grupo de seguridad concreto, el cual podrá contener usuarios y/o equipos. Observe también que las listas de control de acceso que especifiquemos en los objetos Active Directory a través de la Consola MMC de gestión del DNS se limitarán al servicio cliente DNS.

Las funcionalidades de control de acceso no están disponibles con las zonas principales estándar sino solo para zonas DNS integradas en Active Directory.



Selección de las actualizaciones dinámicas seguras para la zona corpnet.priv.

Cuando una zona está integrada en el directorio, el parámetro por defecto de actualización de la zona queda modificado para autorizar sólo las actualizaciones seguras.

La tolerancia a errores es máxima. Las zonas serán replicadas de forma automática y sincronizadas en los nuevos controladores de dominio cuando se añadan a un dominio Active Directory.

Las zonas integradas en el directorio se almacenan por defecto en cada controlador de dominio. El almacenamiento y la gestión de la zona no constituyen recursos adicionales. Además, los métodos utilizados para sincronizar la información almacenada en el directorio ofrecen mejores resultados en relación con los métodos estándar de actualización de las zonas que requieren una configuración manual y a veces la transferencia completa de la zona (caso de los antiguos servidores DNS no-Windows que no soportan las transferencias de zona incrementales tipo IXFR basadas en el estándar RFC 1995).

Los rendimientos de las replicaciones de las zonas integradas en Active Directory están de forma directa relacionados con el hecho de que el motor de replicación del directorio replica con una granularidad muy fina. En efecto, las replicaciones se realizan de forma independiente para cada objeto, para cada atributo del objeto y también para cada valor de atributo del objeto (funcionalidad LVR - *Listed Value Replication*, del modelo de replicación de Active Directory).

En cuanto a las replicaciones, éstas son comprimidas en los vínculos intersite. Integrando el almacenamiento de sus bases de datos de zonas DNS en Active Directory, podemos simplificar la replicación de las zonas DNS a escala de toda la red de la empresa sea cual sea su tamaño.

La eliminación del servicio DNS de un controlador de dominio no borra los datos contenidos en la base de datos Active Directory, pero sólo las particiones que figuran en el controlador de dominio que ha sido rebajado.

Si está usando las zonas DNS en modo estándar y también en modo integrado Active Directory, estos dos tipos de zonas se almacenarán y replicarán por fuerza de forma separada. En este caso, deberemos por supuesto administrarlas por separado. Habrá que implementar y administrar dos topologías de replicación separadas. Una topología de replicación será necesaria para los datos almacenados en el directorio y otra para replicar los archivos de zona entre los servidores DNS estándar. Tal configuración será compleja de mantener y evolucionar, incluso si no hay ninguna dificultad técnica específica.

Con la integración de las zonas DNS en el directorio, todos los problemas de replicación y de gestión de almacenamiento que se presentan para DNS y para Active Directory se reúnen en una única entidad administrativa.

La replicación del directorio es más rápida y eficaz que la replicación DNS estándar y beneficia a las zonas DNS muy voluminosas.

En la medida en que la replicación de Active Directory no afecta a los elementos añadidos, eliminados o modificados (objetos, atributos o valores de atributos) sólo las modificaciones esenciales son propagadas. Estas mejoras permiten minimizar las operaciones LDAP así como los flujos de replicación entre los controladores de dominio.

Las zonas secundarias no pueden almacenarse en el directorio, sólo las zonas principales de Active Directory. A partir del momento en que los servidores DNS son servidores Windows que utilicen el modelo de replicación multimaestro Active Directory, no hay ningún interés en conservar las antiguas zonas de tipo secundario.

Particiones del directorio por defecto

Los servicios de directorio Active Directory aparecieron con Windows 2000 Server. Es en este momento cuando Microsoft puso los cimientos de los servicios de infraestructura que se siguen utilizando hoy en día tanto en los entornos locales con Active Directory en Windows Server 2012 R2 y Windows Server 2016, como en el cloud Microsoft Azure con Azure Active Directory.

Los párrafos siguientes ilustran estos fundamentos siempre de actualidad, acompañados de las observaciones que caracterizan a cada versión del sistema operativo -Windows 2000 Server en Windows Server 2016.

Los controladores de dominio disponen de varios espacios de almacenamiento denominados **particiones**. Obtenido de la terminología LDAP (*Lightweight Directory Access Protocol*), una partición, también conocida como **contexto de nombres** (en inglés, *naming context*), es una estructura de almacenamiento de datos situada en el interior del directorio Active Directory. Esta permite al directorio distinguir varias topologías de replicación. De manera más simple, podemos imaginar que el directorio Active Directory existe en forma de una base de datos, que está compuesta por varias partes que pertenecen a las diferentes topologías de replicación.

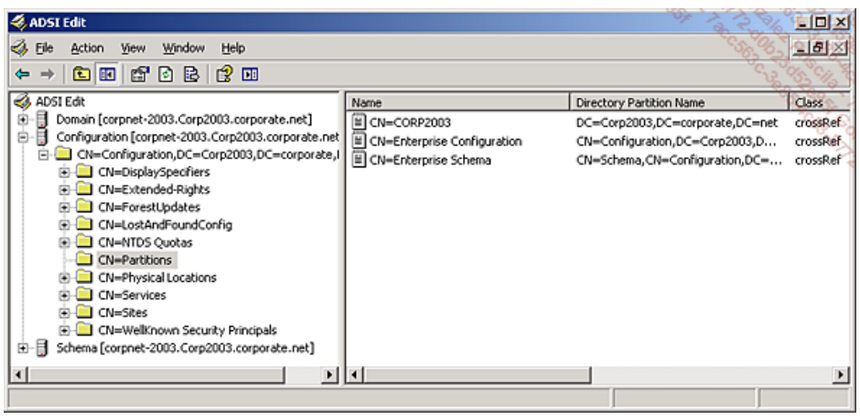
Tratándose de los controladores de dominio Windows 2000 Server, la base de datos Active Directory contiene solo, para el dominio de prueba Corp2003.Corporate.net, las tres particiones presentadas a continuación:

- La partición de dominio cuyo nombre completo es: DC=Corp2003,DC=Corporate,DC=net

  Esta partición contiene todos los objetos de tipo de usuarios, grupos de usuarios, equipos, directivas de grupo, etc.
- La partición de la configuración de la empresa cuyo nombre completo es: CN=Configuration,DC=Corp2003,DC=Corporate,DC=net

  Esta partición contiene todos los objetos de configuración del directorio Active Directory al igual que algunas aplicaciones integradas en Active Directory.
- La partición del esquema de la empresa cuyo nombre completo es: CN=Schema,CN=Configuration,DC=Corp2003,DC=Corporate,DC=net

  Esta partición contiene todas las clases y atributos que formalizan los objetos gestionables por el directorio.



La configuración de Active Directory muestra las tres particiones comunes a los entornos Windows 2000, Windows Server 2003, Windows Server 2008 y Windows Server 2008 R2

La imagen anterior muestra claramente las tres particiones por defecto creadas de forma automática en el momento de la instalación de Active Directory al emplear el asistente de instalación dcpromo. El árbol mostrado por ADSI Edit despliega los contextos de nombres de dominio, de la configuración y del esquema.

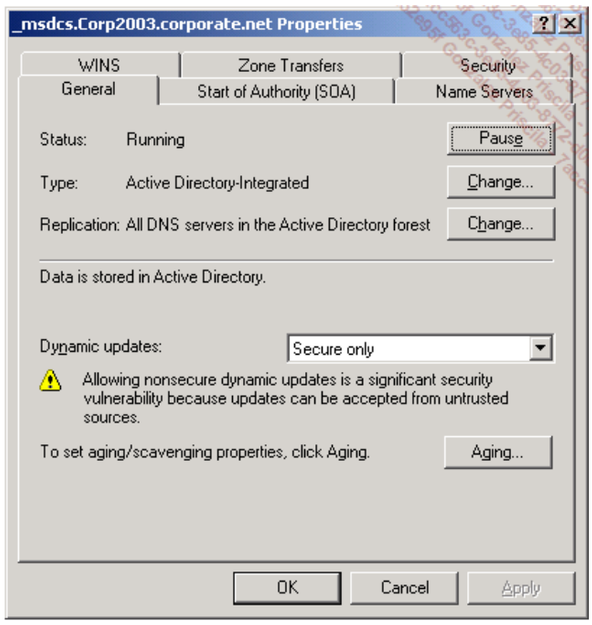
Podemos de esta forma comprobar que la partición de configuración cuyo nombre LDAP es CN=Configuration,DC=Corp2003,DC=Corporate,DC=net contiene, al nivel de objeto CN=Partitions, la declaración de las tres particiones presentadas.

Veremos más adelante que cuando un controlador de dominio desempeña el papel de catálogo global, en inglés GC para *Global Catalog*, y que la infraestructura de bosque de Active Directory contiene más de un dominio Active Directory, entonces el controlador de dominio catálogo global incluye también las particiones de dominio del otro u otros dominios miembros del bosque. Este tipo de partición es particular en el sentido de que contiene solo un conjunto muy limitado pero suficiente de atributos. Las particiones de tipo Catálogo Global son también llamadas particiones de tipo PAS de Partial Attribute Set.

También tenemos la posibilidad de manipular las particiones Active Directory utilizando el comando de sistema `NTDSutil`. Integrado en el sistema desde la primera versión de Windows 2000 Server, este comando es la herramienta que nos permitirá efectuar la mayor parte de las tareas de mantenimiento y/o configuración de los servicios de dominio Active Directory.

Integración de Active Directory y los servidores DNS Windows 2000 Server

En lo que refiere a los controladores de dominio Windows 2000 Server, la integración de las zonas dentro del directorio Active Directory consiste en incluir dichas zonas dentro de la partición del dominio. Observe que en este caso, solo puede utilizarse esta partición. La imagen siguiente muestra que esta opción se ofrece para un controlador Windows Server 2003, cuando el dominio contiene tanto controladores Windows 2000 y Windows Server 2003.

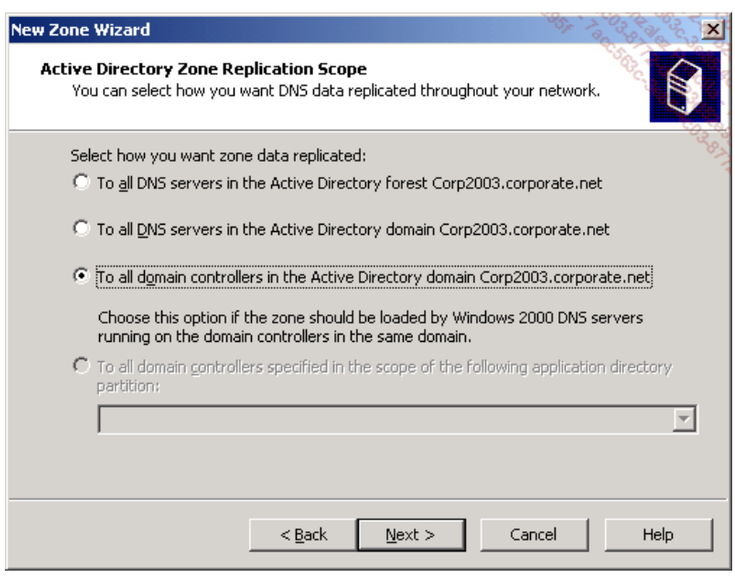


Parámetros de tipo y de replicación para la zona en curso

Según nuestras necesidades, tendremos toda la libertad de elegir el tipo de cada zona, así como los detalles sobre el almacenamiento de las zonas replicadas en el directorio Active Directory.

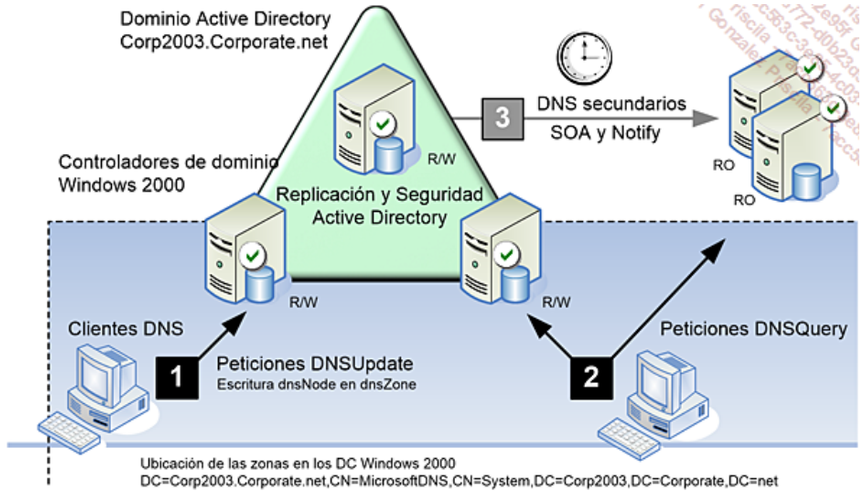
La imagen siguiente muestra que en nuestro ejemplo la zona será almacenada y, por lo tanto replicada para todos los controladores de dominio del dominio Active Directory (**To all domain controllers in the Active Directory domain Corp2003.corporate.net**).

Como se indica, esta opción será elegida si la zona debe ser responsable de los servidores DNS de Windows 2000 que se ejecuten en los controladores de dominio presentes dentro del mismo dominio.



Los cuatro ámbitos de replicación ofrecidos por Windows Server 2003

El diagrama siguiente ilustra este caso. El campo se compone de controladores de dominio Windows 2000 Server y posibles controladores de dominio más recientes, por ejemplo controladores de dominio Windows Server 2003 y/o Windows Server 2008 R2. Estos controladores de dominio ejecutan a su vez el servicio servidor DNS de Windows que alberga la zona DNS del dominio Active Directory Corp2003.Corporate.net -o cualquier otra zona necesaria para el entorno de producción.



Integración de tipo Windows 2000 de las zonas DNS en Active Directory

Con respecto a la compatibilidad de los controladores de dominio dentro del mismo entorno de Active Directory: si bien hoy en día los controladores de dominio Windows 2000 Server están obsoletos, muchos entornos aún utilizan controladores Windows Server 2003. Esta versión es totalmente compatible dentro de un entorno que incluya otros controladores de dominio más modernos, hasta Windows Server 2012 R2. Debemos, no obstante, garantizar que utiliza el SP2 de Windows Server 2003 y que dispone de las últimas actualizaciones publicadas por Microsoft. Por último, en comparación con una integración más moderna, Microsoft define que los controladores de dominio Windows Server 2016 requieren que los niveles funcionales de bosque y de dominio utilizados sean al menos Windows Server 2008. De esta forma, el entorno ya no puede contener controladores más antiguos y la replicación del volumen SYSVOL podrá realizarse a través DFSR y no a través NTFRS. Observe a su vez que si durante la definición del dominio se ha empleado un nivel funcional inferior como el nivel funcional de Windows Server 2003, se requerirá realizar de forma previa la migración del volumen de SYSVOL NTFRS a DFSR.

La integración de las zonas DNS representadas en este esquema destacan los siguientes puntos:

- Los tres controladores de dominio Windows son a su vez servidores DNS. Se encuentran todos disponibles en lectura y escritura para cualquier zona donde las actualizaciones sean dinámicas.
- Los registros de recursos DNS existen como objetos Active Directory y, por lo tanto son replicados y seguros como tales.

Con respecto a la seguridad de los registros en las zonas DNS Active Directory, Microsoft recomienda de forma expresa que las actualizaciones dinámicas funcionen en modo "solo con seguridad". En este caso, sólo las máquinas Windows pertenecientes al dominio Active Directory y autenticadas empleando el protocolo Kerberos V5 tendrán la posibilidad de realizar actualizaciones dinámicas.

- Los clientes DNS dinámicos que funcionan con todas las versiones que van desde Windows 2000 hasta Windows 10 tienen la posibilidad de registrarse en cualquier servidor DNS dinámico.
- En el caso de que algunos controladores de dominio que desempeñen a su vez el rol de servidor DNS encuentren problemas de compatibilidad, estos servidores podrán participar siempre como servidores DNS con zonas DNS secundarias durante todo el período de transición. Por supuesto, como las zonas secundarias estándar están disponibles solo en modo lectura, estos servidores no podrán soportar actualizaciones dinámicas durante este período de transición.

La implementación de una red Windows Active Directory se efectúa con frecuencia de forma progresiva. En este caso, conviene emparejar los mejores puestos de trabajo más modernos con los nuevos servidores que actúen como controladores de dominio y servidores DNS. El objetivo es garantizar que los puestos de trabajo más modernos puedan aprovechar con la mayor rapidez los servicios de Active Directory más modernas y a su vez: localización de los controladores, autenticación Kerberos, directivas de grupo, servicios de certificados, etc.

Integración de Active Directory y servidores DNS Windows Server 2016

Los controladores de dominio que utilicen versiones posteriores a Windows 2000 Server y hasta Windows Server 2016 disponen, para desempeñar su papel de controladores de dominio, de las mismas particiones de directorio que los servidores Windows 2000. Recordemos, que nos referimos a las particiones del esquema de configuración del dominio actual, y las particiones de los otros dominios del bosque cuando el controlador desempeña a su vez el rol de catálogo global.

Una novedad importante surgida a partir de Windows Server 2003 y todavía importante con Windows Server 2016 atañe a las particiones del directorio de aplicaciones. Una partición del directorio de aplicaciones es una partición de Active Directory de un nuevo tipo que se replica solo hacia uno o varios controladores declarados de forma específica y que soporten este nuevo tipo de particiones. De esta forma, un controlador que participe en la replicación de una partición especificada mantendrá una réplica de esta misma partición. Las aplicaciones y servicios podrán entonces utilizar este nuevo tipo de partición como una zona específica de almacenamiento de datos.

Para ilustrar este principio, los servicios TAPI (*Telephony Application Programming Interface*) pueden ser configurados para almacenar datos específicos para las aplicaciones TAPI 3.1 en una partición del directorio de aplicaciones creada a tal efecto.

Con respecto a las particiones MS-TAPI del directorio de aplicaciones con Windows Server 2003: en estos servidores, el asistente para**Configurar el servidor** proporciona una ubicación central a partir de la cual podemos instalar y configurar la mayoría de los servicios incluidos en el sistema. Si instalamos los servicios de directorio Active Directory empleando este asistente, se aprovechará para crear de forma automática una partición llamada por defecto MsTapi.nombrededominio. En el caso de que el controlador de dominio se instale sin emplear este asistente, es decir, usando directamente el comando `dcpromo.exe`, podemos instalar la partición del directorio de aplicaciones MSTAPI utilizando el comando `tapicfg.exe`. Este comando permite realizar las operaciones de gestión específicas para los servicios TAPI. Los dos mandos siguientes nos permiten, de forma respectiva, mostrar la configuración TAPI y crear la partición del directorio de aplicaciones:`tapicfg show` y `tapicfg install /directory: mstapi31.Corp2003.Corporate.net`. Tengamos en cuenta que estos comandos no se han incluido en Windows Server 2012 R2, ni Windows Server 2016

La herramienta de línea de comando `Ntdsutil` también nos permite manipular las particiones gestionadas por Active Directory. Sin embargo, a diferencia de una herramienta como el comando `tapicfg` diseñada para realizar una serie de operaciones de configuración específicas de TAPI, el comando `ntdsutil` nos permitirá solo efectuar operaciones concretas en el directorio Active Directory.

Siempre acerca de las particiones del directorio de aplicaciones, cabe señalar que una partición puede contener cualquier tipo de objeto a excepción de objetos con identificadores de seguridad (SID). La idea es que la seguridad sea siempre almacenada en las particiones "habituales" de Active Directory y no en otras. No es posible crear los principios de seguridad tales como objetos de tipo usuario, grupos de seguridad o equipos. Desde un punto de vista de la gestión de las particiones, conviene especificar que, de forma independiente del tipo de partición, sólo los miembros del grupo Administradores de la empresa pueden crear o gestionar de forma manual las particiones del directorio de aplicaciones. Desde el punto de vista del almacenamiento, la ventaja de almacenar datos de aplicaciones -tales como las que se refieren a las zonas DNS- en una partición del directorio de aplicaciones y no en una partición de directorio de dominio es que nos beneficiamos de un mayor control del tráfico de replicación y un elevado nivel de seguridad. En efecto, los datos correspondientes se replicarán solo a los controladores de dominio seleccionados y los datos disponen de ACL donde los accesos se controlan a través del uso del protocolo Kerberos v5.

La tabla siguiente describe las extensiones de replicación de zona disponibles para los datos de la zona DNS integradas en Active Directory.

Ámbito de replicación	Implementación Windows
Todos los servidores DNS en el bosque de Active Directory: una partición del directorio de aplicaciones será creada en el nivel del bosque.	Réplica de los datos de la zona hacia todos los servidores DNS ejecutados en los controladores de dominio dentro del bosque Active Directory. Se trata del ámbito de replicación más importante.
Todos los servidores DNS en el dominio Active Directory: una partición del directorio de aplicaciones será creada en el nivel del dominio Active Directory.	Réplica de los datos de la zona hacia todos los servidores DNS ejecutados en los controladores de dominio del dominio Active Directory. Esta opción es el parámetro por defecto de la replicación de zona DNS integrada en Active Directory para los controladores de dominio que funcionen en Windows Server 2003 y hasta Windows Server 2016.
Todos los servidores DNS en el dominio de Active Directory: en este caso, no es necesario crear una partición del directorio de aplicaciones. La zona se creará dentro de la partición existente en el dominio.	Replica los datos de la zona a todos los controladores de dominio del dominio Active Directory. Esta opción es necesaria para soportar la carga de una zona Active Directory para los servidores DNS que funcionen bajo Windows 2000 Server.
Todos los controladores de dominio en una partición de directorio de aplicaciones especificada: una partición del directorio de aplicaciones debe ser creada de forma expresa y replicada a los servidores designados de forma específica.	Réplica de los datos de la zona en función del ámbito de replicación de la partición de directorio de aplicaciones especificada. Para que una zona esté almacenada en la partición del directorio de aplicaciones especificado, es necesario que el servidor DNS que mantiene la zona se registre en la partición del directorio de aplicaciones específico.

Así, cuando un nuevo dominio de Active Directory es aplicado en base a desde un controlador de Dominio Windows Server 2003 hasta un Windows Server 2016, el asistente de instalación de Active Directory tomará la iniciativa para crear zonas relativas al dominio de Active Directory en los sitios definidos a continuación.

1. ForestDnsZones.NomBosqueDns

Esta partición se crea por defecto y permite un almacenamiento a nivel de todo el bosque. Está disponible en todos los servidores DNS que funcionan con los controladores de dominio del bosque. Por lo tanto, cualquier zona DNS que se almacene en esta partición del directorio de aplicaciones será replicada a todos los servidores DNS ejecutados en los controladores de dominio del bosque.

Por supuesto, esta opción es especialmente importante para garantizar una amplia disponibilidad de registros críticos que afecten a la misma infraestructura del bosque. Por defecto, el Asistente de instalación de Active Directory almacenará aquí la zona que contenga todos los controladores de dominio del bosque.

Esta zona, de gran importancia para el conjunto del bosque, se almacena en el lugar designado a continuación:**_msdcs.NombredeDominioDnsRaizdelBosque**.

2. DomainDnsZones.NomdeDominioDns

Esta partición del directorio de aplicaciones se crea por defecto para incluir cada dominio del bosque. Las zonas DNS almacenadas en esta partición del directorio de aplicaciones se replicarán a todos los servidores DNS que funcionen en los controladores de dominio del mencionado dominio.

Esta opción se asemeja a lo que también se efectuaba por defecto en los antiguos controladores de dominio Windows 2000 Server. Sin embargo existe un matiz importante. En los controladores de dominio Windows 2000 Server, las zonas almacenadas en el dominio Active Directory utilizan la partición del dominio misma. En un servidor DNS controlador de Dominio Windows Server 2003 hasta Windows Server 2016, una zona almacenada dentro del dominio podrá disponer de su propia partición independiente.

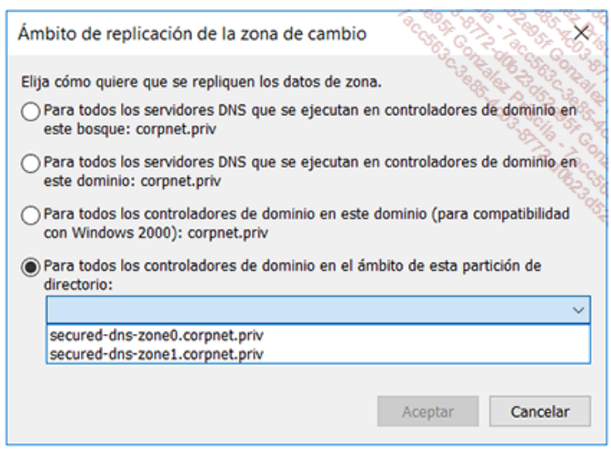
Además de la creación de las zonas, si seleccionamos el Asistente de instalación de -Active Directory para instalar y configurar de forma automática un servidor DNS en el controlador de dominio local, el servidor DNS se instalará en el equipo en el que se ejecute el asistente. Durante esta operación, el parámetro del servidor DNS preferido del equipo se configura a su vez para utilizar el nuevo servidor DNS local a través de la dirección de bucle de TCP/IP 127.0.0.1. De esta forma, el primer controlador de dominio es cliente de su propio servidor DNS.

El segundo controlador a ser instalado en el dominio deberá utilizar luego al primero como servidor DNS preferido -al menos durante la fase de instalación. Al final, varios controladores de dominio de Active Directory asumiendo el rol de servidores DNS contendrán las zonas de dominio Active Directory. Los otros equipos (clientes y servidores) que se añadirán al dominio deberán utilizar al menos dos de estos servidores DNS -preferido y auxiliar de forma respectiva. El hecho de que un cliente DNS pueda disponer de dos servidores DNS proporcionará la tolerancia a fallos necesaria para abordar cualquier problema en uno de los servidores DNS.

Los puestos de trabajo que trabajen con Windows 7 hasta Windows 10 pueden utilizar el protocolo LLMNR - *Link-Local Multicast Name Resolution*, como servicio de resolución de nombres cuando todos los demás métodos no están operativos. Este protocolo de resolución basado en mensajes de tipo multicast permite a estos equipos localizar otros equipos LLMNR situados en la misma red, incluso cuando los servicios DNS u otros servicios de resolución de nombres no están disponibles. Con el fin de mejorar la experiencia del usuario en caso de fallo en los servicios de resolución DNS, los puestos de trabajo Windows 10 utilizan solicitudes de resolución LLMNR y NetBIOS en paralelo.

3. Utilización de otras particiones del directorio de aplicaciones

También tenemos la posibilidad de usar nuestras propias particiones de directorio de aplicaciones de Active Directory. La imagen siguiente muestra la consola MMC de gestión de DNS ofreciendo la posibilidad de seleccionar la partición a utilizar. De esta forma, las particiones **secure-DNS-zone0.corpnet.priv** y **secure-DNS-zone1.- corpnet.priv** podrán ser utilizadas como espacio de almacenamiento para las zonas DNS.



Selección de el ámbito de la partición del directorio de aplicaciones

Al seleccionar una opción de replicación, no olvide que cuanto mayor sea el alcance de una replicación, mayor será el tráfico causado por la replicación en la red. Por ejemplo, si escogemos replicar los datos de una zona DNS a todos los servidores DNS del bosque, el tráfico de la red producto será más denso que si replicamos los datos de la zona DNS a todos los servidores DNS de un único dominio Active Directory de este bosque.

Con independencia de la opción inicial, siempre podemos modificar a posteriori la manera en que los datos de las zonas serán replicados. Sin embargo, no se debe olvidar que el cambio de ubicación requiere una replicación completa del contenido hacia el o los nuevos emplazamientos.

4. Creación de una partición en el directorio de aplicaciones de Active Directory

Para crear una partición capaz de incluir una zona DNS, tendremos que usar el -comando **ntdsutil** de la siguiente forma:

1. En el intérprete de comandos, ejecutamos `ntdsutil`. Se muestra el comando `ntdsutil`.

2. Escriba: `partition management`

3. Escriba: `connections`

4. Escriba: `connect to server FQDN-de-su-controlador`

5. Escriba: `quit`

6. Para crear una partición de directorio de aplicaciones, escriba el comando siguiente: `create nc DN-PartitiondirectorioApp FQDN-ControladorDominio`.

De esta forma, para nuestro dominio de prueba, deberemos introducir el comando siguiente: `create nc dc=secure-dns-zone0,dc=corpnet,dc=priv vmdc01.corpnet.priv`.

El comando `ntdsutil` dispone de una ayuda sencilla pero bastante clara. Como ocurre con frecuencia, los nombres de objeto de Active Directory deberán estar denominados especificando el DN LDAP, mientras que los nombres de servidores tendrán que utilizar el FQDN o el hostname.

Una vez creada la partición del directorio de aplicaciones, debemos declarar los diferentes controladores de dominio como réplica de la nueva partición empleando el comando: `add nc replica DN- AppPartitionDirectory FQDN` del controlador de dominio contemplado para la operación.

Automatización de los comandos Ntdsutil

Aunque las funciones ofrecidas por Ntdsutil sean para la mayoría de las operaciones críticas, es posible que deseemos automatizar ciertas tareas creando scripts que contengan una serie de comandos Ntdsutil. Muchas funciones Ntdsutil que realizan modificaciones abren un mensaje que consulta al usuario si realmente desea realizar la operación en particular. Por supuesto, cuando estos mensajes aparecen Ntdsutil espera una entrada de teclado por parte del usuario.

Los comandos `popups off` y `popups` nos permiten, de forma respectiva, desactivar y activar estos mensajes cuando se ejecuta Ntdsutil a partir de un archivo de comandos o un script.

Las operaciones soportadas por el comando Ntdsutil pueden ser peligrosas para el buen funcionamiento del directorio Active Directory. Se recomienda no desactivar los mensajes de confirmación cuando se ejecutan ciertos tipos de scripts. Una vez realizada una operación empleando un script en modo `popups off` se recomienda reactivar las confirmaciones empleando el comando `popups on`.

La eliminación de una partición de directorio de aplicaciones es tan simple como su creación. Siempre empleando Ntdsutil, puodemos utilizar la misma lógica especificando el comando: `Delete nc replica DN- AppPartitionDirectory FQDN` del controlador de dominio contemplado para la operación.

La supresión de la última réplica de una partición del directorio de aplicaciones, ocasiona la pérdida definitiva de todos los datos almacenados en esta partición.

Para efectuar estas operaciones, debemos ser miembro del Grupo Admins del dominio o del grupo Administradores de empresa en Active Directory, o haber recibido por delegación las autorizaciones necesarias.

5. Replicación de las particiones del directorio de aplicaciones y casos de los catálogos globales

Los datos de una zona DNS integrada en Active Directory, almacenados en una partición de directorio de aplicaciones no son replicados en el o los catálogos generales del bosque. Si bien es cierto que un controlador de dominio que contiene el catálogo global también puede albergar particiones de directorio de aplicaciones, tenga en cuenta que no replicará esos datos en el catálogo global.

Sin embargo, cuando los datos de una zona DNS integrada en Active Directory se almacenan en una partición de dominio, una parte de estos datos se almacena en el catálogo global. Estos datos mínimos son necesarias para garantizar el soporte de los servidores DNS que funcionen bajo Windows 2000 Server.

6. Almacenamiento de zonas, particiones de aplicaciones y replicaciones

El ámbito de replicación de una partición de directorio de aplicaciones respeta la infraestructura de sitios Active Directory. De esta forma, al igual que ocurre en Windows 2000 Server, los parámetros de replicación se aplican a todas las particiones conocidas. Por lo tanto, la replicación de estas particiones se producirá con el mismo calendario de replicación intersite ya definido en el nivel de la infraestructura de los sitios Active Directory.

7. Zonas DNS integradas en Active Directory y particiones del directorio AD LDS

Los servidores Windows Server 2003 hasta Windows Server 2016 pueden desempeñar el rol de servidores de directorio LDAP v2 y v3 estándar sin requerir la instalación de la función de controlador de dominio de Active Directory.

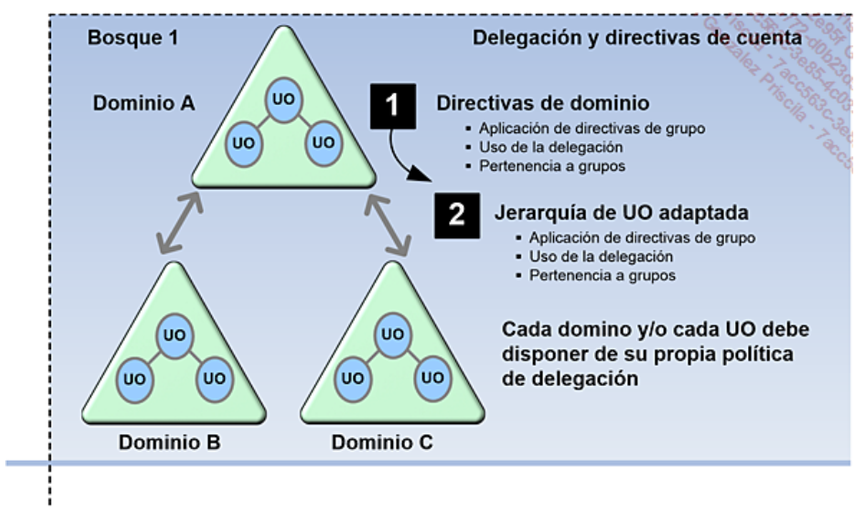
Este componente adicional se conocía como ADAM de *Active Directory/Application Mode* para los servidores Windows Server 2003. Disponible como descarga en el sitio de Microsoft en la categoría "Features Packs" para Windows Server 2003, desde entonces fue integrado en todas las versiones de Windows Server 2008 hasta Windows Server 2016 en forma de un nuevo rol conocido como Servicios AD LDS (*Active Directory Lightweight Directory Services*).

Las diferencias propias de cada versión de los servicios ADAM y AD LDS son mínimas o incluso inexistentes, así que solo hablaremos de los servicios AD LDS.

Los servicios AD LDS permiten al administrador aplicar varias particiones de guía, así como el soporte de varias instancias AD LDS en el mismo servidor. Esta funcionalidad permite incluir en el mismo servidor varios esquemas, ya que cada instancia deberá disponer de su propio esquema. Los servicios de directorio AD LDS son en particular interesantes para las aplicaciones que deban basarse en LDAP, pero que no requieran una relación directa con un directorio empresarial como Active Directory.

De esta forma, la siguiente imagen muestra que los servicios y los datos globales son almacenados en Active Directory, mientras que los datos locales específicos de las aplicaciones son almacenados en las particiones soportadas por los servicios AD LDS, es decir, por las equipos que no son controladores de dominio.

En los servidores Windows Server 2008 hasta Windows Server 2016, los servicios AD LDS (*Active Directory Lightweight Directory Services*) sustituyen a los servicios ADAM de las versiones anteriores. Observe que los servicios AD LDS son simplemente una evolución menor de los servicios ADAM.



Directorio de Active Directory y las particiones de directorio de tipo ADAM

Las principales características ofrecidas por AD LDS se presentan a continuación:

- Las particiones soportadas por los servicios AD LDS son similares a las particiones del directorio de aplicaciones disponibles a partir de Windows Server 2003. Sin embargo, estas particiones no requieren el uso del rol de controlador de dominio.
- Los servicios AD LDS se presentan a través del Administrador de servidores con las versiones de Windows Server 2008 hasta Windows Server 2016.
- Una instancia AD LDS puede incluir varias particiones.
- Las instancias AD LDS soportan los espacios de nombres X500 y DNS.
- La replicación de las particiones AD LDS respeta el mismo modelo utilizado por Active Directory. Cada instancia AD LDS dispone de su

propia directiva de replicación.

- Las instancias AD LDS pueden funcionar en servidores Windows Server miembros de un dominio Active Directory, y también en servidores autónomos.
- Cada instancia dispone de sus propios ejecutables y de sus propios parámetros TCP/IP (direcciones, puertos). Es así posible que un servidor incluya varias instancias AD LDS de diferentes niveles.
- Como ocurre con los controladores de dominio de Active Directory, la copia de seguridad y la restauración de las instancias AD LDS están de forma directa soportadas por las herramientas integradas en el sistema Windows Server.
- Podemos administrar y soportar las instancias AD LDS utilizando las mismas herramientas que ya empleamos con los servicios de directorio Active Directory. Podemos a su vez usar de la misma manera las herramientas LDP, ADSI Edit, Replmon, NTDSUtil y el analizador de rendimiento para el seguimiento de cada instancia.
- Los servicios AD LDS utilizan los servicios de seguridad ofrecidos por la infraestructura Windows disponible. De esta forma, podemos implementar controles de acceso en la base a los principios de seguridad implementados en el bosque Active Directory, dominios aprobados, y las cuentas del equipo local. También contamos con la posibilidad de crear objetos de usuario en el sentido LDAP directamente en AD LDS. En este caso, solo los autenticaciones LDAP de tipo Simple Bind serán utilizables para dichas cuentas.
- Las cuentas establecidas dentro del directorio AD LDS no son entidades de seguridad de Windows. Por lo tanto, carecen de SID.
- El servidor AD LDS no es un servidor de autenticación Windows que soporte el protocolo Kerberos v5. Sin embargo, AD LDS podrá utilizar las cuentas situadas en un dominio Active Directory y en este caso, utilizar autenticaciones basadas en el protocolo Kerberos v5.
- Los servicios AD LDS no pueden ser utilizados de forma directa por las aplicaciones Active Directory de Microsoft como Exchange Server, SharePoint Server o SQL Server. Estas aplicaciones requieren el uso de controles de seguridad basados en SID, lo que no es el caso de los entornos con los servicios AD LDS.

Microsoft remarca que los conceptos utilizados por AD LDS, incluidos los relativos al aislamiento, son interesantes en más de un sentido. Por ejemplo, el rol "Server EDGE Transport" disponible con Microsoft Exchange Server utiliza una instancia AD LDS que actúa como servidor LDAP para los servicios Exchange en un equipo que no forme parte del dominio Active Directory. El servidor "aislado" de esta forma evita la exposición de un controlador de dominio de Active Directory dentro de una DMZ. Observe que esta aplicación es todavía funcional con Exchange Server 2016.

- El componente principal AD LDS se implementa a través de DSAMain.exe. En un controlador de dominio Active Directory, el servidor LDAP, el motor de replicación DRS (*Directory replication System*), el centro de distribución de claves Kerberos, así como el soporte de SAM están integrados en el módulo LSASS (*Local Security Authority SubSystem*).
- Las instancias virtuales AD LDS se implementan en forma de servicios de Windows.
- El motor LDAP AD LDS incluye la totalidad del código de Active Directory.
- Los servicios AD LDS no requieren de manera específica el uso del DNS para localizar los servidores AD LDS. Las aplicaciones pueden ser configuradas para consultar a cualquier servidor utilizando las instancias de AD LDS.
- Los servicios AD LDS ya no soportan las antiguas interfaces de Microsoft como SAM.
- Los servicios AD LDS no soportan ninguna integración con el servicio de replicación de archivos FRS (*File Replication Service*).
- Los servicios AD LDS pueden ser útiles cuando es necesario disponer de un servidor LDAP estándar. Esta solución también es muy interesante si deseamos implementar una aplicación LDAP "en paralelo a un directorio ya existente".

Una partición AD LDS no puede almacenar ninguna entidad de seguridad. La utilización del directorio AD LDS en un entorno Microsoft significa que los servicios de directorio Active Directory siguen aglutinando todo lo que se refiere a las autenticaciones Kerberos y otros servicios globales de infraestructura.

Las instancias AD LDS utilizan la seguridad de Active Directory.

Las particiones gestionadas por los servicios AD LDS no permiten almacenar zonas DNS. Como veremos más adelante, sólo los controladores de dominio Windows Server pueden albergar particiones capaces de contener zonas DNS.

En resumen, los servicios AD LDS desempeñan un papel complementario a los servicios ya ofrecidos por los servicios de directorio de Active Directory. Esta solución responderá a las necesidades expresadas por desarrolladores Windows y no-Windows. Sin embargo, observe que los servicios AD LDS no sustituyen en ningún caso a los servicios de dominio Active Directory. Para más información sobre los servicios AD LDS, conéctese a la dirección http://www.microsoft.com/adlds o busque "Active Directory Lightweight Directory Services" en el sitio Microsoft Technet.

8. Condiciones necesarias para lograr un cambio de almacenamiento

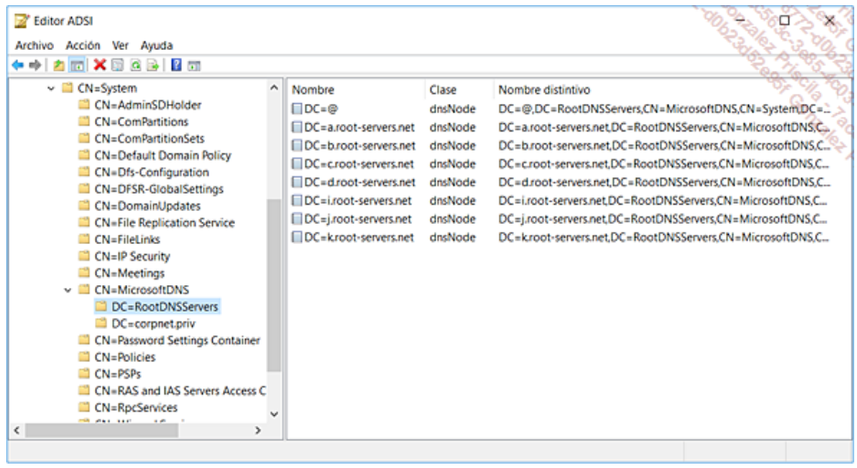
Para poder cambiar el almacenamiento de una zona a partir de la partición de dominio a una partición del directorio de aplicaciones, debemos poder unirnos al controlador de dominio que tiene el rol de maestro de asignación de nombres de dominio (en inglés, el *Domain Naming Master FSMO*) en la red. Si no es el caso, no podremos crear particiones del directorio de aplicaciones para incluir la zona DNS.

Transferencia del rol de "Maestro de asignación de nombres de dominio": en caso de problema de disponibilidad del maestro de asignación de nombres de dominio, basta con trasladar el rol de maestro de asignación de nombres de dominio a un controlador de dominio que funcione con Windows Server 2008 R2 o una versión posterior, tal como Windows Server 2012 R2 o Windows Server 2016. En el caso de que la transferencia de rol no pueda realizarse, se podrá forzar el rol empleando el comando ntdsutil.

9. Indicaciones de raíces

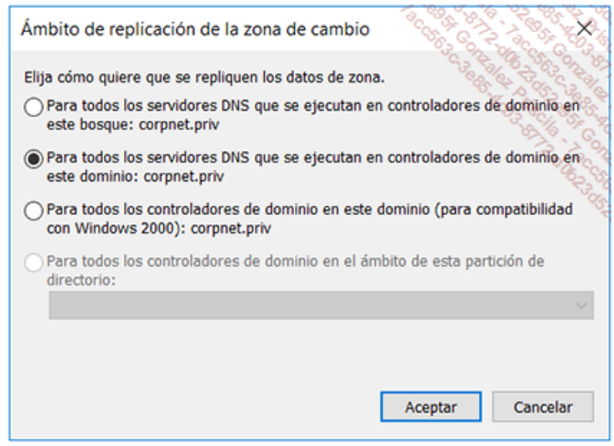
Cuando el nivel funcional de dominio utilizado es Windows Server 2003 o Windows Server 2008, entonces las indicaciones de raíz que permiten al servidor DNS de referirnos a los servidores DNS del dominio raíz del espacio de DNS se almacenan en la partición de directorio de aplicaciones dentro del dominio.

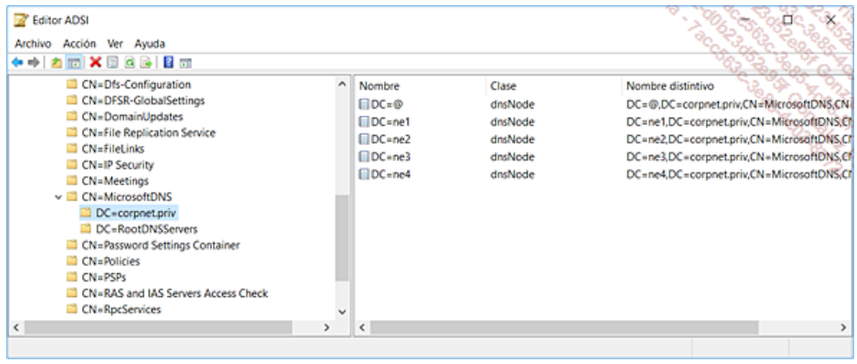
La imagen siguiente muestra las indicaciones de raíces por defecto del dominio corpnet.priv dentro de la partición de dominio.



Indicaciones de raíces almacenadas en el contenedor System de la partición del dominio con Windows 2000

El contenedor **CN=MicrosoftDNS,CN=System,dc=Corpnet,dc=priv** incluye los diferentes contenedores, cada uno mantiene el contenido de una zona determinada. Los registros A de los servidores raíz existen luego bajo la forma de objetos de tipo dnsNode dentro del contenedor RootDNSServers. Las imágenes siguientes ilustran la configuración de la zona DNS integrada en Active Directory del dominio corpnet.priv así como su contenido dentro de la partición del dominio empleando la herramienta ADSI Edit.





10. Almacenamiento de las zonas en Active Directory y registros dinámicos de los controladores de dominio

Por defecto, el servicio Inicio de sesión Red en inglés Net Logon, graba de forma automática los registros de recursos DNS necesarios para el buen funcionamiento del localizador del controlador de dominio.

En la medida en que estos registros de recursos son fundamentales para las replicaciones Active Directory, así como para la localización de los controladores de dominio por los equipos cliente, el servicio Inicio de sesión Red de un controlador de dominio graba cada 24 horas los registros DNS necesarios. En caso de ausencia o incoherencias de estas grabaciones, también podemos forzar su regrabación reiniciando el servicio Inicio de sesión Red.

Esta operación puede realizarse empleando los siguientes comandos: `net stop netlogon & net start netlogon`

Seguridad de las actualizaciones dinámicas

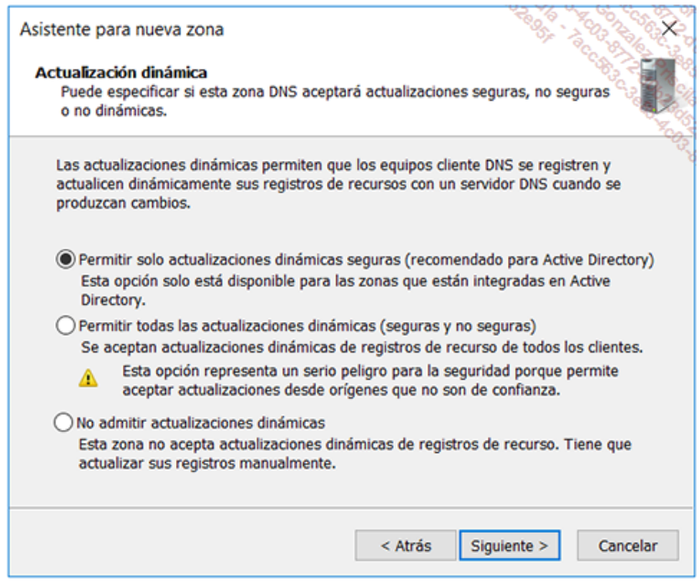
La protección de las zonas DNS es un punto en particular importante para garantizar la integridad de los registros. Esto se aplica, por supuesto para todos los tipos de registros, sabiendo que prestaremos una atención específica a los datos DNS necesarios para garantizar el buen funcionamiento del directorio de Active Directory.

Los servidores DNS que funcionen con Windows Server 2003 hasta Windows Server 2016 nos permiten declarar de forma independiente en cada zona la forma en que su seguridad está gestionada. Estos parámetros tendrán por necesidad implicaciones en el nivel de la seguridad de las zonas DNS estándar o directamente integrados en Active Directory.

1. Configurar las actualizaciones dinámicas seguras

Con los controladores de dominio Windows Server 2008 y hasta Windows Server 2016, el parámetro definido por defecto en la creación de una nueva zona DNS solo permite las actualizaciones dinámicas seguras. Se trata del parámetro más seguro dentro de un entorno donde el soporte de los registros dinámicos es necesario.

La imagen siguiente muestra el valor por defecto presentado al Administrador a través del Asistente de creación de una nueva zona DNS integrada en Active Directory.

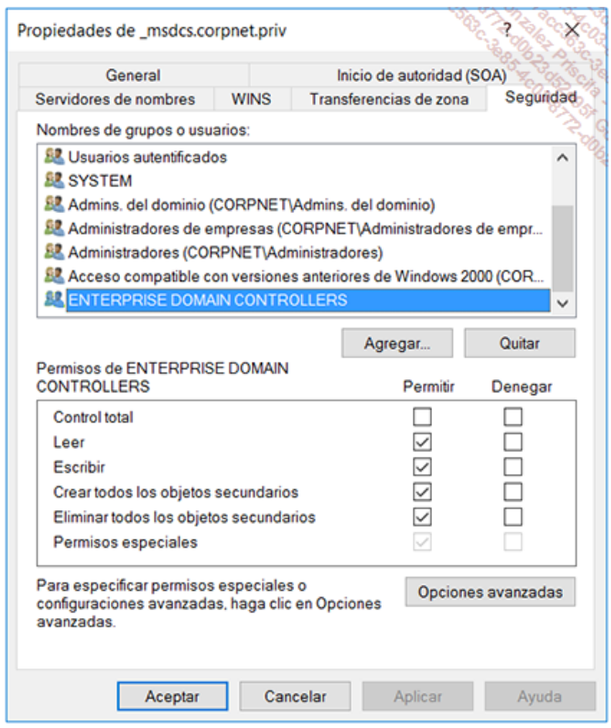


Datos almacenados en Active Directory y actualizaciones dinámicas seguras

Con esta opción, recomendada por defecto, la carga de gestión de los registros DNS se minimiza, permitiendo a la empresa disponer de un entorno DNS actualizado en todas las circunstancias.

Esta opción permite a los sistemas informáticos autenticados y pertenecientes al mismo dominio Active Directory que el servidor DNS realice las actualizaciones en la zona.

La integración de Active Directory permite también gestionar de forma muy específica la lista de control de acceso a las zonas DNS almacenadas en Active Directory. Estos permisos nos permitirán controlar qué usuarios y grupos de Active Directory están facultados para manipular las zonas DNS.



Grupos especiales y permisos por defecto de la zona segura _msdcs.corpnet.priv integrada en Active Directory

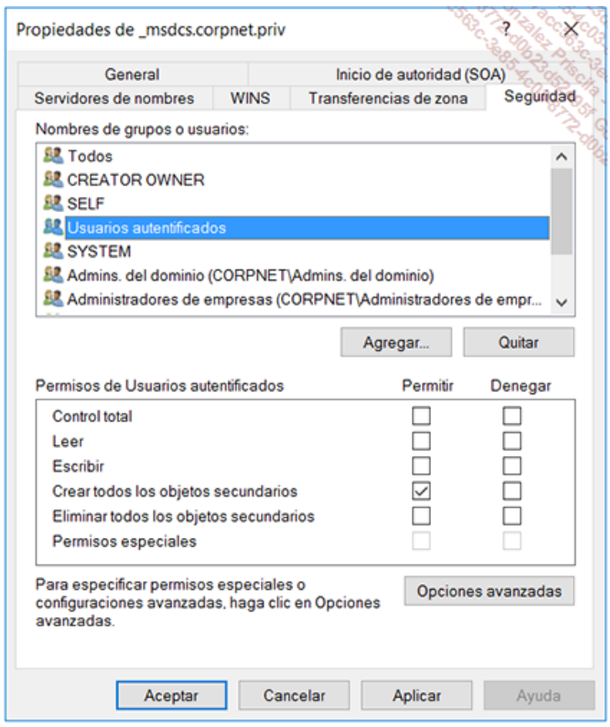
Por defecto, sólo las entidades certificadas pueden crear registros y actualizar a posteriori en caso de cambio. La tabla siguiente enumera las autorizaciones establecidas por defecto para las zonas DNS seguras almacenadas en el directorio Active Directory.

Permisos de las zonas	Implementación Windows
Administradores	Autorizar: Leer, escribir, Crear todos los objetos secundarios, Permisos especiales.

Usuarios autentificados	Autorizar: Crear todos los objetos secundarios.
Propietario creador (OWNER)	Permisos especiales.
DNSAdmins	Autorizar: Control total, Leer, Escribir, Crear todos los objetos secundarios, Eliminar todos los objetos secundarios, Permisos especiales.
Admins. del dominio	Autorizar: Control total, Leer, Escribir, Crear todos los objetos secundarios, Eliminar todos los objetos secundarios, Permisos especiales.
Administradores de empresas	Autorizar: Control total, Leer, Escribir, Crear todos los objetos secundarios, Eliminar todos los objetos secundarios, Permisos especiales.
ENTERPRISE DOMAIN CONTROLLERS	Autorizar: Control total, Leer, Escribir, Crear todos los objetos secundarios, Eliminar todos los objetos secundarios, Permisos especiales.
Todos	Autorizar: Leer, Permisos especiales
Acceso compatible con versiones anteriores de Windows 2000	Autorizar: Permisos especiales.
SYSTEM	Autorizar: Control total, Leer, Escribir, Crear todos los objetos secundarios, Eliminar todos los objetos secundarios, Permisos especiales.

Algunos grupos cuentan con permisos especiales directamente heredados del objeto servidor DNS mismo. Estos permisos son necesarios para garantizar el correcto funcionamiento, en las mejores condiciones de seguridad de la zona. En resumen, los permisos sobre las zonas seguras DNS pueden clasificarse de la siguiente manera:

- El grupo **Todos** dispone solo de un permiso de lectura que permite solo obtener acceso de lectura al contenido de la zona.
- Los grupos de carácter administrativo permiten administrar las diferentes funciones disponibles en un objeto de tipo zona DNS.
- El grupo **Usuarios autentificados** permite realizar los controles de acceso que permitan o no la actualización dinámica de los registros de recursos DNS.



Permiso "Crear todos los objetos secundarios" para el grupo Usuarios autentificados

Estas listas de control de acceso permiten disfrutar de un alto nivel de seguridad al instalar un controlador de dominio que ejecute a su vez el rol de servidor DNS. Microsoft recomienda manipular estos permisos con precaución.

2. Actualizaciones seguras y grabaciones DNS realizadas a través de DHCP

Los servidores DHCP que ejecuten en Windows Server 2003 hasta Windows Server 2016 pueden participar en las actualizaciones dinámicas en el espacio de nombres DNS para cada uno de los clientes que soportan las operaciones de actualización dinámica.

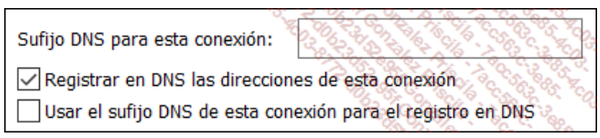
Se plantean preguntas de los controles de acceso a las zonas DNS así como la propiedad de los registros de estas zonas.

El funcionamiento del proceso de actualización de las zonas DNS por el servicio Servidor DHCP se describe a continuación. El primer problema es que es el servidor DHCP debe tener conocimiento del nombre completo del equipo cliente DHCP. Por lo tanto, para que pueda tener éxito al incluir y actualizar los registros de recursos de tipo puntero (PTR) y host (A) por cuenta de sus clientes DHCP, es necesario enviar esta información de los clientes DNS al servidor DHCP.

La opción de nombre de dominio completo del cliente, llamada Opción 81, permite al cliente proporcionar esta al servidor DHCP (FQDN, *Fully Qualified Domain Name*). De forma opcional, el cliente puede especificar al servidor DHCP cómo desea que el servidor trate la operación.

Así, cuando la opción 81 es emitida por un cliente DHCP Windows 2000 hasta Windows 10, el servidor DHCP reacciona y determina la operación que será necesario o no realizar procediendo como se muestra a continuación:

- El servidor DHCP actualiza los registros A y PTR DNS si los clientes solicitan la asistencia empleando la opción 81.



La imagen anterior muestra que el puesto de trabajo efectuará su registro de recurso de tipo A en el DNS utilizando su sufijo principal. Recordemos que el sufijo principal está directamente derivado de pertenencia del dominio y también puede complementarse con un sufijo DNS adicional a nivel de cada conexión de red.

- El servidor DHCP actualiza los registros A y PTR DNS aunque los clientes no realicen la solititud.

En este caso, el servidor DHCP tomará la iniciativa de realizar las grabaciones por cuenta de los clientes teniendo en cuenta que las operaciones necesarias dependerán de la naturaleza de los clientes DHCP.

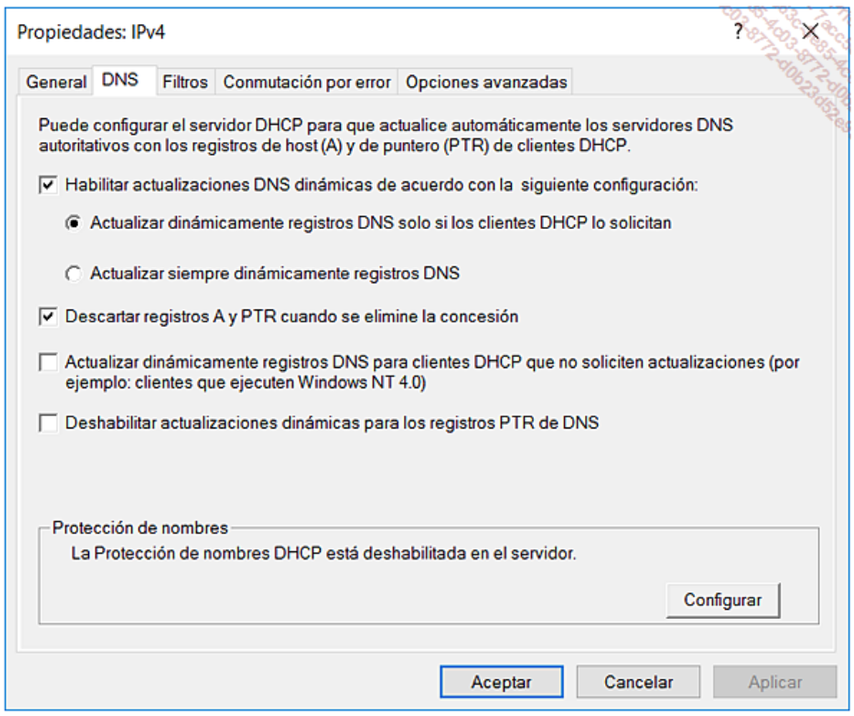
El primer caso se refiere al principio de las actualizaciones/DHCP DNS para los clientes DHCP modernos Windows XP hasta Windows 10. En este caso, se realizarán las operaciones siguientes:

- El cliente envía una petición DHCP (DHCPREQUEST) al servidor, incluyendo la opción DHCP 81. Por defecto, el cliente solicita que el servidor DHCP incluya el registro DNS de tipo PTR, mientras que el cliente registra él mismo su propio registro DNS de tipo A.
- El servidor devuelve al cliente un acuse de recibo DHCP (DHCPACK) atribuyendo un contrato de arrendamiento de la dirección IP incluyendo la opción DHCP 81. Los parámetros por defecto del servidor DHCP (**Actualizar los registros PTR y A DNS solo si los clientes DHCP lo solicitan**), utilizan la opción 81 indicando al cliente que el servidor DHCP se hará cargo de la operación de registro DNS de tipo PTR y que el cliente incluirá el registro DNS de tipo A.

Las operaciones de registro realizadas por el cliente y por el servidor DHCP se realizan por completo de forma asíncrona. Así, el cliente grabará su registro de tipo A de manera separada del servidor DHCP que soporta el registro de tipo PTR.

El segundo caso se refiere al principio de las actualizaciones/DHCP DNS para los clientes DHCP mas antiguos de tipo Windows NT o Linux. Estas versiones de cliente DHCP/DNS no soportan de forma directa el proceso de actualización dinámica del DNS. No podemos imaginar ningún nivel de comunicación entre los clientes y el servidor DNS. Para estos clientes "no compatibles", se efectúan las siguientes operaciones:

- El cliente DHCP envía una petición DHCP (DHCPREQUEST) al servidor. La petición no incluye la opción DHCP 81 ya que ésta no está soportada por este tipo de clientes.
- El servidor DHCP devuelve al cliente un acuse de recibo DHCP (DHCPACK), asignando un contrato de arrendamiento de la dirección IP, sin la opción DHCP 81.
- El servidor DHCP envía a continuación al servidor DNS las actualizaciones del registro de recurso host de tipo A. El servidor envía también las actualizaciones del registro de recurso de tipo puntero (PTR).



Valores por defecto de la configuración de las actualizaciones automáticas de los registros de tipo A y PTR a zonas DNS dinámicas para un ámbito DHCP

Los parámetros de la imagen anterior están disponibles en general en el objeto Servidor DHCP para los protocolos IPv4 e IPv6 y también, de manera independiente, a nivel de cada dominio DHCP. El comportamiento de los registros dinámicos puede configurarse de forma muy fina, de forma global y también para cada ámbito DHCP.

Ahora que sabemos cuáles son las operaciones realizadas por los clientes DNS y servidores DHCP para actualizar los registros de recursos DNS, debemos considerar la problemática de estas actualizaciones hechas por poder a través de los servidores DHCP Windows Server 2003 hasta Windows Server 2016.

De hecho, si un servidor DHCP realiza la primera operación de actualización dinámica para un registro de recursos dado, entonces el servidor DHCP pasa a ser el propietario del registro. Será el único capaz de mantener este registro.

Por supuesto, esto puede plantear un problema en un cierto número de casos. El caso más tradicional concierne a la posibilidad de que hubiera un servidor DHCP de respaldo y poder mantener los registros en el caso de fallo del servidor DHCP de producción. Como acabamos de ver, si el primer servidor DHCP es el único propietario de los registros, es por supuesto el único capaz de modificarlos.

Otro efecto secundario concierne a la actualización de los clientes anteriores a las versiones más modernas como Windows 7 o Windows 10. Sabemos que para garantizar el soporte de los equipos que no soportan las inscripciones DNS dinámicas, es necesario que el servidor DHCP realice la actualización por cuenta del cliente. Por lo tanto, también es el único que dispone de los permisos necesarios en los registros DNS lo que hace cualquier actualización posterior imposible. Esto es particularmente cierto después de que estos equipos hayan sido actualizados a una versión más moderna como, por ejemplo, Windows 10.

3. Utilización del grupo especial DNSUpdateProxy para realizar las actualizaciones dinámicas de las zonas DNS seguras

Para que uno o varios servidores DHCP sean autorizados a actualizar los registros DNS contenidos en una zona segura para la cual carecen de los permisos necesarios, podemos añadir estos servidores DHCP al grupo DNSUpdateProxy.

En este caso, el próximo objeto que incluirá el mismo registro de nombres en la zona DNS se convertirá automáticamente en el nuevo propietario del registro.

Observe que los objetos creados por los miembros del Grupo DnsUpdate Proxy no son seguros por defecto. Este punto es muy importante porque de esta forma el primer usuario no miembro del grupo DnsUpdateProxy que realiza una operación de modificación de uno de esos registros, se convierte en el nuevo propietario.

Securización de los registros durante la utilización del grupo DnsUpdateProxy

El hecho de que los registros DNS creados por los miembros del Grupo DnsUpdateProxy no sean seguros expone de forma potencial esos registros a todo tipo de usurpación de identidad, y por lo tanto, de ataques. Además, este grupo es difícilmente utilizable de forma efectiva cuando las operaciones de registro se refieren a áreas integradas en Active Directory, que funcionan para solo actualizaciones dinámicas seguras.

De hecho, habrá que por necesidad añadir los permisos adecuados para autorizar los registros creados por los miembros del grupo para estar seguros.

Para proteger los registros no seguros o autorizar a los miembros del grupo DnsUpdate Proxy para incluir los registros en las zonas que no solo permiten actualizaciones dinámicas seguras, podemos crear una cuenta de usuario dedicada y configurar servidores DHCP para que efectúen las actualizaciones dinámicas DNS en base a esta identificación.

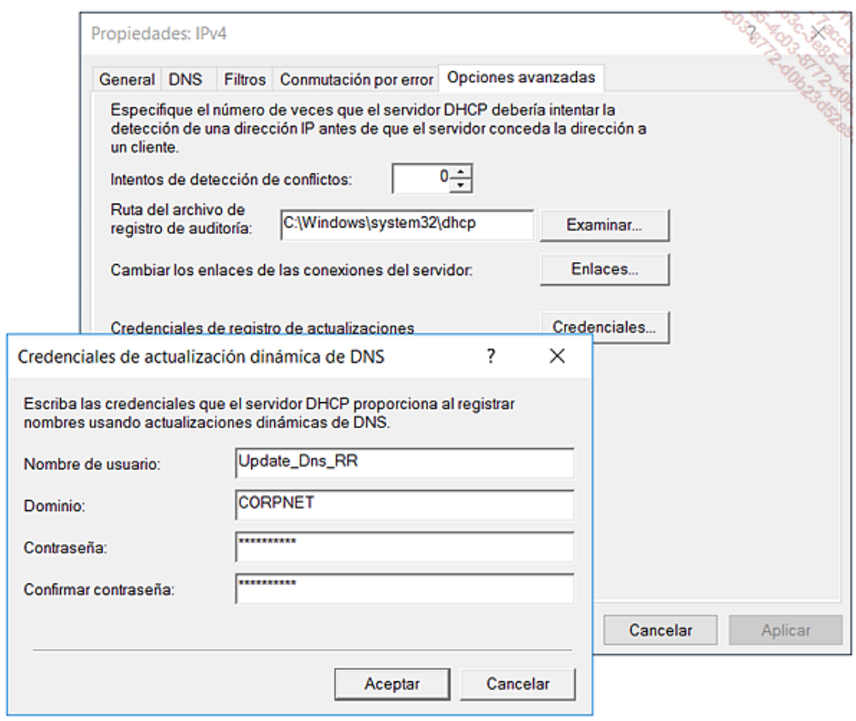
En función de las restricciones de seguridad impuestas, podemos también utilizar una o varias cuentas de usuario para controlar los accesos a uno o varios servidores DHCP.

Esta cuenta de usuario específica es una cuenta de usuario cuyo único objetivo es proporcionar a los servidores DHCP la información de autenticación mínima para realizar con éxito las actualizaciones DNS en modo dinámico. Cuando creamos una cuenta especial para este uso y configuramos los servidores DHCP con dicho usuario, cada servidor DHCP proporcionará esta información en el registro de nombres para la cuenta de cliente DHCP. Una vez efectuada la operación, el próximo objeto que incluya el mismo registro de nombres en la zona DNS se convertirá de forma automática en el nuevo propietario del registro.

Con respecto a la ubicación de la cuenta de identificación DHCP: la cuenta de usuario utilizado para la autenticación del servidor DHCP deberá establecerse en el bosque donde reside el servidor DNS principal de la zona a actualizar. Esta cuenta también puede residir en otro bosque, siempre que ésta tenga una aprobación de bosque establecida con el bosque que contiene el servidor DNS principal de la zona a actualizar. Observe que no puede tratarse de un dominio aprobado situado en otro bosque, pero sólo de un dominio en un bosque aprobado. Para este último punto es necesario que los dos bosques funcionen como mínimo en el nivel funcional de bosque Windows Server 2003 o posterior.

4. Seguridad de las zonas DNS y poder del servicio Servidor DHCP en los controladores de dominio Active Directory

Cuando el servicio Servidor DHCP se instala en un controlador de dominio, este servicio posee y utiliza la autoridad del controlador de dominio para actualizar o eliminar cualquier registro DNS inscrito en una zona integrada en Active Directory. Para impedir el servidor DHCP hacer una utilización incorrecta o ilegal de los poderes del controlador de dominio, puede configurar el servidor DHCP para que se autentique de forma específica.



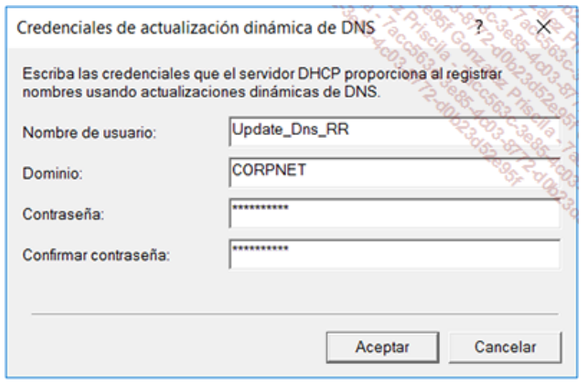
Información de identificación del servidor DHCP Windows Server 2003

Observe que esta opción solo está disponible en los servidores DHCP Windows Server 2008 hasta Windows Server 2016, a nivel de los objetos IPv4 y IPv6 del servidor DHCP. Esta importante problemática abarca todos los registros incluyendo los registros escritos de manera segura por los equipos que actúan como controladores de dominio de Active Directory, y cualquiera que sea su versión de sistema operativo Windows Server. La posibilidad de que exista un servidor DHCP que opere sobre datos en los que no debería tener permiso para manipular es un tema en particular preocupante, que puede solucionarse de dos maneras:

- La recomendación de Microsoft es evitar instalar el servicio Servidor DHCP en un controlador de dominio.

El artículo Q255134 de la base de conocimientos Microsoft Technet titulado "Installing Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) on a Domain Controller" describe esta problemática. También podemos buscar en el sitio de Microsoft Technet "DHCP Security" o utilizar el vínculo https://technet.microsoft.com/es-es/library/dd296625(v=ws.10).aspx.

- En el caso de que no sea posible aplicar esta primera recomendación, siempre podemos implementar la autenticación del servidor DHCP antes presentada y disponible en los servidores Windows Server 2003 hasta Windows Server 2016.



Declaración de la información de identificación en el servidor DHCP Windows Server

Por supuesto, la solución ideal consiste en acelerar el proceso de migración de los antiguos equipos a puestos modernos que funcionen con Windows 7, o preferible, -Windows 10. Esta última alternativa es la mejor recomendación que podemos hacer.

En efecto, en este caso cada equipo es autenticado empleando el protocolo Kerberos V5 para poder crear y mantener posteriormente su propio registro con total seguridad. Los servidores DHCP no son implicados por cuenta de los clientes.

5. Comando Netsh y declaración de la autenticación del servidor DHCP

Podemos configurar los servidores DHCP con la información de la cuenta de identificación empleando la consola MMC de gestión del servicio DHCP. En el caso de que deseemos automatizar esta operación, podemos usar el comando de contexto `Netsh`. Este comando puede ser operado en línea de comandos, como se especifica a continuación:

1. Abra una línea de comandos como administrador y ejecute el comando `netsh`.

2. Para entrar en el contexto DHCP, escriba: `dhcp`.

3. Para acceder a su servidor local, escriba: `server`.

4. Para declarar los parámetros de autenticación del servidor DHCP, escriba el comando: `set dnscredentials NombreUsuario NombreDominio Contraseña`

- En el caso que sea necesario modificar esta declaración en muchos servidores, podemos también utilizarlo pasando todos los parámetros necesarios en la misma línea de comandos o empleando un archivo de script.
- El carácter * permite declarar la contraseña durante la ejecución del comando. En el caso de un script que contenga la contraseña, verifique que el script esté contenido en un directorio encriptado.

Para más información sobre la configuración de la información de identificación empleando la Consola DHCP, busque en el sitio de Microsoft Technet "Introducción al protocolo dhcp".

6. Conflictos de gestión de las autorizaciones en las zonas DNS

El servicio Servidor DNS que se ejecuta en un controlador de dominio que posee zonas almacenadas en Active Directory almacena los datos de la zona en la base de objetos proporcionados por el mismo directorio, es decir, los objetos y atributos de Active Directory contenidos en diferentes particiones del directorio.

Configurar la lista de permisos de acceso a los objetos de Active Directory de tipo DNS corresponde a configurar la lista de permisos de las zonas DNS usando la consola de gestión del DNS.

En la medida en que estos datos específicos al DNS no son más que los datos de Active Directory, será prudente asegurarse de que los administradores de la seguridad de los objetos de Active Directory y los administradores de la seguridad de los objetos de tipo DNS colaborarán estrechamente con el fin de evitar cualquier error de configuración o el establecimiento de parámetros de seguridad contradictorios.

Los objetos y atributos de Active Directory utilizados por los datos de las zonas DNS almacenadas en Active Directory se describen a continuación:

- El elemento **DnsZone** es un objeto de tipo contenedor creado cuando una zona se almacena en Active Directory.
- El elemento **DnsNode** es un objeto de tipo nodo utilizado para relacionar y asociar un nombre en la zona a los datos de recursos.
- El elemento **DnsRecord** es un atributo de valores múltiples de un objeto de tipo dnsNode. Se utiliza para almacenar los registros de recursos asociados al objeto de nodo seleccionado.
- El elemento **DnsProperty** es un atributo de valores múltiples de un objeto dnsZone utilizado para almacenar la información de configuración de una zona.

Para más información sobre el conjunto de clases y atributos de objetos de Active Directory, visite el sitio Microsoft MSDN en la direcciónhttp://msdn.microsoft.com y busque la información que describe el contenido del esquema del directorio Active Directory.

Integración de los servidores DNS Windows con los existentes

Las familias de sistemas operativos de red Windows Server disponen de un servicio de servidor DNS totalmente interoperable con otros servidores DNS de tipo BIND, a menudo disponibles en las diferentes distribuciones de Linux. Los servidores DNS que ejecuta Windows Server 2003 hasta Windows Server 2016 respetan la implementación de la casi totalidad de las especificaciones de los servicios DNS que aparecen en las RFC (*Request for Comments*). En el marco de su adhesión a los estándares de Internet, Microsoft participa activamente en la mejora de los protocolos proponiendo muchas contribuciones (publicaciones de RFC en modo *draft*), las cuales pasan a ser con frecuencia los estándares.

El conjunto de las RFC Internet DNS implementadas en los servicios DNS de Windows Server está disponible a través de los enlaces siguientes:

- https://msdn.microsoft.com/es-es/library/windows/desktop/ms682099(v=vs.85).aspx
- http://www.ietf.org/

1. Acerca de las RFC soportadas por el servicio DNS de Windows Server 2003 y Windows Server 2008 R2

Los documentos RFC son una serie de informes, propuestas de protocolos y normas de protocolos en curso de evolución, utilizados por la comunidad Internet. Las especificaciones de los servicios DNS se basan en las RFC aprobadas y publicadas por la IETF en las que participan también otros grupos de trabajo.

Las RFC siguientes contienen las especificaciones utilizadas por Microsoft para diseñar e implementar los servicios de servidor y cliente DNS en un entorno Windows Server:

RFC	Título
1034	Domain Names Concepts and Facilities
1035	Domain Names Implementation and Specification
1122	Requirements for Internet Hosts - Communication Layers
1123	Requirements for Internet Hosts Application and Support
1876	A Means for Expressing Location Information in the Domain Name System
1886	DNS Extensions to Support IP Version 6
1995	Incremental Zone Transfer in DNS
1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
2181	Clarifications to the DNS specification
2308	Negative Caching of DNS Queries (DNS NCACHE)
2535	Domain Name System Security Extensions (DNSSEC)
2671	Extension Mechanisms for DNS (EDNS0)
2782	A DNS RR for specifying the location of services (DNS SRV)
2845	Secret Key Transaction Authentication for DNS (TSIG)
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2930	Secret Key Establishment for DNS (TKEY RR)
2931	DNS Request and Transaction Signatures (SIG(0)s)
3110	RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
3445	Limiting the Scope of the KEY Resource Record (RR)
3596	DNS Extensions to Support IP Version 6
3645	Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)

2. Acerca de las RFC 1034 y 1035

Estas dos RFC describen el protocolo estándar original de DNS para la aceptación de los servicios de nombres de dominio en un entorno TCP/IP. Estos datos explican los protocolos de forma detallada, poniendo de relieve las ideas y técnicas subyacentes utilizadas en la mayoría de las implementaciones de DNS. Podemos buscar en Internet los documentos señalados a continuación. Estos documentos contienen las especificaciones utilizadas para diseñar e implementar los servicios DNS en los sistemas operativos Windows y Windows Server de Microsoft:

Nombre del archivo (en inglés)	Título
Draft-skwan-utf8-dns-02.txt	Using the UTF-8 Character Set in the Domain Name System
Draft-ietf-dhc-dhcp-dns-08.txt	Interaction between DHCP and DNS
Draft-ietf-dnsind-tsig-11.txt	Secret Key Transaction Signatures for DNS (TSIG)
Draft-ietf-dnsind-tkey-00.txt	Secret Key Establishment for DNS (TKEY RR)
Draft-skwan-gss-tsig-04.txt	GSS Algorithm for TSIG (GSS-TSIG)
af-saa-0069.000.doc	ATM Name System Specification version 1.0

3. Consulta de las RFC en la Web

Podemos obtener el conjunto de las RFC a partir del sitio Web RFC Editor (en inglés). Las RFC se clasifican en función de los siguientes criterios: estándares de Internet aprobadas, normas Internet propuestas (propuestas para su evaluación), los métodos recomendados para Internet o documentos de tipo FYI (*For your information*). Aquí encontraremos también otros documentos llamados documentos de asistencia en línea. Estos documentos proponen nuevas especificaciones que solo se encuentran en la fase de propuesta. Por esta razón estos documentos no tienen todavía un número RFC. http://www.rfc-editor.org/

4. Interoperabilidad de los servicios DNS de Windows Server

En la medida en que Internet se basa de forma integral en el sistema de nombres y resolución de nombres DNS, y donde el directorio Active Directory lo utiliza de forma natural y sofisticada, es evidente que no puede haber para una empresa determinada ninguna incompatibilidad fundamental entre el espacio privado de los dominios Active Directory y el espacio público de Internet. Los principales beneficios de dicha interoperabilidad son los siguientes:

- Interoperabilidad completa con otros servidores DNS que respeten las RFC en cuanto al servicio de nombres DNS, y viceversa.

- Utilización de servidores DNS de Windows Server en Internet y en particular dentro del Cloud Microsoft Azure.

Para probar la interoperabilidad de los diferentes servidores DNS entre sí, Microsoft ha puesto a prueba los servicios de servidor y cliente DNS con las siguientes implementaciones de BIND.

- BIND 4.9.7;
- BIND 8.1.2 et BIND 8.2;
- BIND 9.1.0.

Las últimas versiones del servidor DNS BIND 9.9.9 y 9.10.4 no han sido objeto de validaciones especiales por los equipos de pruebas de Microsoft, pero funcionan normalmente en entornos heterogéneos con las versiones anteriores de servidores BIND o de servidores DNS Windows Server 2008 R2 hasta Windows Server 2012 R2. Los posibles problemas de compatibilidad y/o de configuración relacionados con el uso del servicio DNS de Windows Server en entornos particulares, o con los servidores DNS en Internet, se presentan a continuación.

5. Problema de compatibilidad y búsqueda directa e inversa WINS

Desde las primeras versiones de servidores DNS Windows Server, el servicio servidor DNS puede ser configurado para transmitir las peticiones de resolución no satisfechas a un servidor WINS. Esta operación de búsqueda adicional denominada WINS *Forwarding* esta soportada para las zonas de búsqueda directa e inversa, y puede ser activada o no a nivel de cada zona.

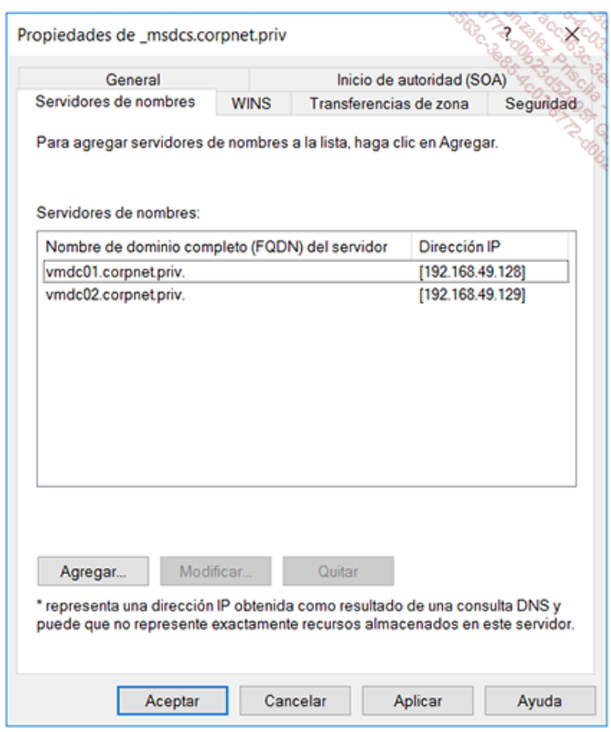
Es importante señalar que la activación de las búsquedas WINS en una zona DNS creará un registro de recurso de tipo WINS en la zona DNS. Esta opción no deberá utilizarse si la zona debe ser replicada a otros servidores dotados de otras implementaciones DNS que no reconozcan los registros de recursos de tipo WINS.

6. Especificación del servicio DNS de Windows Server e integración dinámica a través de los servidores DHCP

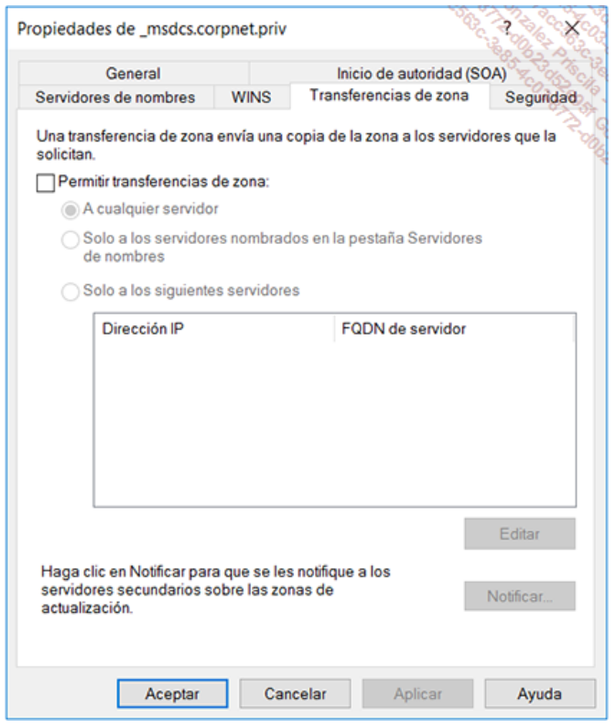
Con los servidores que operan con Windows Server 2003 hasta Windows Server 2016, el servicio Servidor DHCP ofrece soporte por defecto de la grabación y la actualización de información para los clientes DHCP heredados en las zonas DNS. Los clientes heredados por lo general incluyen sistemas operativos Microsoft anteriores a Windows 2000 y también los sistemas no Microsoft tales como versiones antiguas de Linux o Unix. La integración entre los servicios DNS y los servicios DHCP proporcionada por Windows Server permite al cliente DHCP incapaz de actualizar de forma dinámica los registros de recursos DNS contar con información actualizada en las zonas de búsqueda directa y las zonas de búsqueda inversas DNS a través del servidor DHCP.

Autorizaciónes de las transferencias de zonas

Por defecto, los accesos a las zonas están securizados. Así, un servidor DNS de Windows Server solo autoriza las transferencias de zonas a los servidores DNS especificados como servidores de nombres. La imagen siguiente ilustra los registros NS declarados en la pestaña **Servidores de nombres**.



Una vez efectuada esta operación, las transferencias de zona deberán ser autorizadas a través de la pestaña **Transferencias de zona**.



La opción **Permitir transferencias de zona** no se refiere a las zonas integradas en Active Directory que se replican empleando el motor de replicación de los controladores de dominio de Active Directory. Esta opción solo se utiliza para autorizar las transferencias de zonas de tipo AXFR (transferencias completas) e IXFR (transferencias incrementales) solo entre las zonas DNS primarias y secundarias.

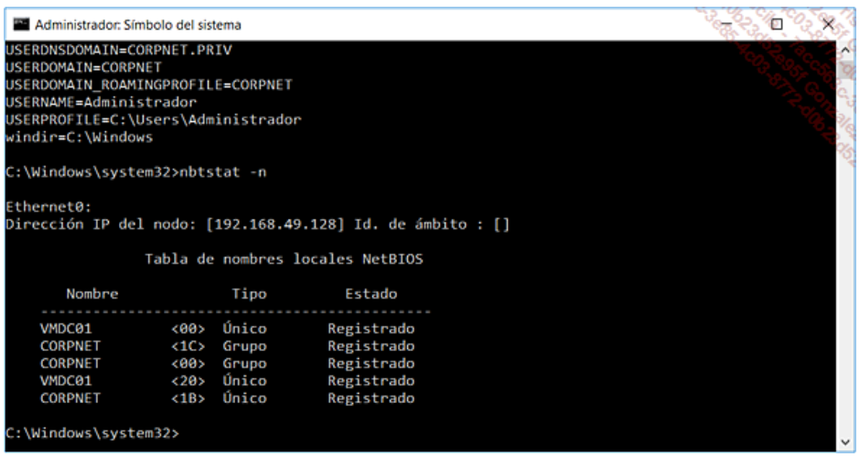
Introducción

Los principales elementos implicados en una infraestructura de servicios distribuidos y servicios de seguridad Active Directory requieren una configuración apropiada de los servicios DNS. Así, con una configuración realizada siguiendo las reglas, los equipos Windows 7 hasta Windows 10, serán capaces de interrogar al sistema de resolución DNS para localizar los equipos que desempeñen el rol de controlador de dominio dentro de la infraestructura de servicios de dominio de Active Directory. ¡Este hecho significa también a la inversa, que el directorio Active Directory no puede funcionar de forma normal ni ofrecer sus servicios de una manera adecuada si no dispone de una configuración DNS adaptada y plenamente operativa!

Vuelta al pasado -con respecto a la interfaz NetBIOS: Con Active Directory, ¡los métodos cambian en su fundamento! En efecto, en los entornos de dominios basados en la interfaz NetBIOS, el dominio registra su nombre en el código de servicio NetBIOS [1C]. Este registro de grupo - empleado por los antiguos clientes NetBIOS tales como Windows NT, se anuncia siempre en la red TCP/IP a través de la interfaz NetBT - NetBIOS over TCP/IP, incluso con Windows Server 2016. Desde un punto de vista NetBIOS, esta entrada puede contener hasta 25 controladores de dominio con sus direcciones IP respectivas, sea cual sea la versión del sistema operativo. Desde un punto de vista técnico, en comparación con un entorno de controladores de dominio Windows Server 2016, las normas de compatibilidad harán que el registro de grupo [1C] pueda contener controladores de dominio que funcionen desde Windows Server 2008 hasta Windows Server 2016.

La imagen siguiente muestra el conjunto de nombres soportados por el controlador de dominio vmdc01.corpnet.priv Windows Server 2016:

- El nombre DNS del dominio de Active Directory utilizando la variable USERDNSDOMAIN = CORPNET.PRIV
- El nombre NetBIOS del dominio de Active Directory utilizando la variable USERDOMAIN = CORPNET
- La inscripción del controlador de dominio VMDC01 con el nombre de Grupo NetBIOS CORPNET y el código de servicio [1C]



Espacios de nombres Active Directory, DNS y NetBIOS

Servicio de ubicación DNS y selección de controladores de dominio

Los procesos de inicio de sesión integrados en los equipos Windows 2000 hasta Windows 10 se utilizan para localizar el controlador de dominio más cercano al equipo.

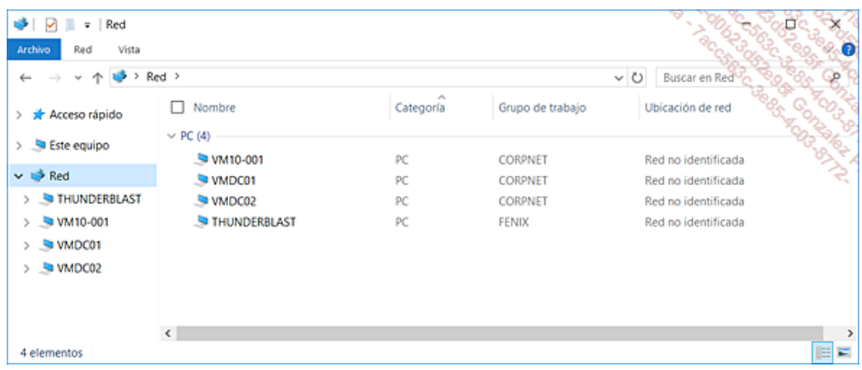
Este servicio llamado Inicio de sesión de Red, en inglés Net Logon funciona de forma idéntica en todas las versiones de Windows Client y Windows Server. Observe que los antiguos puestos de trabajo o servidores que no soportan Active Directory no podrán utilizar los mecanismos de localización basados en los servicios de resolución de nombres DNS y tendrán que utilizar el antiguo sistema de selección basado en la interfaz NetBIOS, el Código de servicio [1C] y el servicio de resolución WINS para garantizar buen funcionamiento de las resoluciones NetBIOS en entornos IP compuestos por múltiples redes y subredes encaminadas.

Con respecto a la interfaz NetBIOS y registros de campo [1C] y [1D]: no debemos confundir el registro de nombres de dominio NetBIOS [1C] con el registro de nombres de dominio [1D]. En efecto, el código [1D] se destina al buen funcionamiento de las funciones de exploración de la red. Se registra para los exploradores principales. Recordemos que existe un explorador principal, Master Browser, por cada subred TCP/IP. Los exploradores de respaldo, Backup Browsers, utilizan este nombre para comunicarse con el explorador principal obteniendo la lista de servidores disponibles mantenida por este explorador principal. Además, tenga en cuenta que los servidores WINS están diseñados para devolver una respuesta de registro positivo para el nombre de tipo nombre_de_dominio[1D] aunque el servidor WINS no registra este nombre en su base de datos. Esto tiene el efecto de forzar una consulta de tipo difusión por parte del cliente. En efecto, como el nombre [1D] no está registrado en la base WINS, si el nombre_de_dominio[1D] se solicita al servidor WINS, este último devolverá una respuesta negativa. Esta respuesta negativa obligará al cliente a enviar un mensaje de difusión en la subred local.

Con respecto al servicio Explorador de equipos en los servidores Windows Server 2008 y hasta Windows Server 2016: el registro NetBIOS es un registro utilizado por los clientes para acceder al Master Browser, sabiendo que no existe un solo Master Browser por subred IP. El registro NetBIOS <1E> es un registro de tipo Normal Group que los exploradores de equipos pueden resolver a través de difusión o en el cual podrán ponerse a la escucha para participar en la selección del equipo Master Browser. En los servidores Windows Server 2008 y hasta Windows Server 2016, el servicio Explorador de equipos se encuentra desactivado. Este servicio no se requiere en la medida de que las versiones de Windows más recientes pueden utilizar un método de descubrimiento mucho más moderno llamado WSD - Web Service Discovery protocol. El hecho de que el servicio Explorador de equipos esté desactivado no requiere la declaración de los registros de NetBIOS y <1E>.

Con respecto a los métodos de descubrimiento: los sistemas operativos cliente Windows 7 hasta Windows 10 y servidores Windows Server 2008 hasta Windows Server 2016 disponen de una pila de red reescrita por completo. Ésta incorpora muchas mejoras en el ámbito del descubrimiento de red, la detección de ubicaciones y tipos de dispositivos. El descubrimiento de la red ha sido mejorado mediante la adición de los protocolos LLTD (*Link Layer Topology Discovery*), FD (*Function Discovery*) y WSD (*Web Services for Devices*).

La imagen ilustra el uso de los distintos protocolos de descubrimiento redes disponibles en los sistemas desde Windows 7 hasta Windows 10:



Protocolos de descubrimiento integrados en Windows

En cuanto a la selección de los controladores de dominio de Active Directory, no es necesario declarar un controlador de dominio preferido para que un equipo cliente como Windows 2000 hasta Windows 10 sea capaz de elegir de forma correcta un controlador de dominio. Si disponemos de una red extendida y deseamos que los equipos cliente seleccionen un controlador de dominio cercano, entonces deberemos estructurar nuestra infraestructura física Active Directory en base a varias zonas geográficas, empleando objetos "Sitios de Active Directory".

El concepto de **Sitio de Active Directory** permite a los clientes Active Directory localizar la ubicación de los servicios deseados, y a los controladores de dominio de replicar mejor la información contenida en las particiones que estén a su cargo. Por lo general, los Sitios de Active Directory se pondrán en marcha cuando sea necesario, es decir, cuando varias zonas geográficas están vinculadas por enlaces de comunicación de red lentas o también cuando la selección de los controladores por los clientes debe ser, por otros motivos, controlada de forma especial.

Observe que si se quiere, a pesar de contar con una conexión rápida, disponer de una buena selección de controladores de dominio, se deberán crear sitios de Active Directory.

Al igual que en el pasado donde un controlador de dominio Windows NT registraba su rol empleando los códigos de servicio NetBIOS, los controladores de dominio de Active Directory graban también sus registros de servicios de tipo SRV basándose en la infraestructura de Active Directory y su sitio de pertenencia respectivo.

Los servicios DNS, disponibles en los controladores de dominio, desempeñan un papel importante, devolviendo a los clientes las referencias que les permiten seleccionar un controlador de dominio local o cercano a ellos. Éste será utilizado para muchas operaciones tales como la autenticación Kerberos del equipo y la sesión del usuario, las búsquedas LDAP en el directorio y también la aplicación de las directivas de grupo a nivel de los sitios, los dominios y unidades organizativas. Cada sitio Active Directory se asocia a una o más redes o subredes IP, los controladores de dominio pueden de forma sencilla usar la dirección IP de origen de los equipos clientes para determinar el mejor sitio que se utilizará para dirigir sus búsquedas DNS. El escenario siguiente toma como ejemplo el caso de un equipo portátil que se utilizará en un lugar diferente de su sitio habitual:

1. El cliente obtiene una configuración TCP/IP válida a partir de un servidor DHCP. En ese momento, el equipo cliente utiliza su antiguo sitio de pertenencia y envía las peticiones DNS para buscar un controlador de dominio en este sitio.

El hecho de que el equipo emplee el protocolo DHCP para obtener la configuración IP no es una condición necesaria. Hoy en día, el protocolo DHCP se utiliza en la mayoría de las redes -ya sea en modo dinámico, o a veces en modo estático empleando reservas de direcciones IP. Por supuesto, el uso de la asignación de direcciones IP a través de DHCP es necesario en el caso de los equipos portátiles que se desplazan de una red a otra.

2. El servidor DNS responde con los registros de recursos de tipo SRV. El equipo cliente utiliza entonces estas respuestas para dirigir una serie de "ping LDAP" hacia los controladores de su anterior sitio de pertenencia.

Observe que los mensajes de tipo "ping LDAP" utilizan el protocolo LDAP sobre UDP, es decir, el puerto UDP 389. Este punto es importante porque a veces, los cortafuegos se configuran para gestionar el tráfico LDAP en el puerto TCP 389, con lo que no es suficiente para soportar todos los servicios LDAP. En este caso concreto, una configuración que bloquee mensajes UDP 389 tendrá por efecto el no permitir la

correcta selección de los controladores de dominio en un entorno multisitio.

3. El primer controlador de dominio situado en el anterior sitio de pertenencia del cliente compara la dirección IP de origen del cliente con la suya y constata que el cliente se encuentra en un sitio Active Directory diferente. Esta operación es muy fácil de lograr para el contralor solicitado, ya que todos los sitios son conocidos, todas las redes y subredes IP están declaradas y asociadas al sitio de Active Directory adecuado.

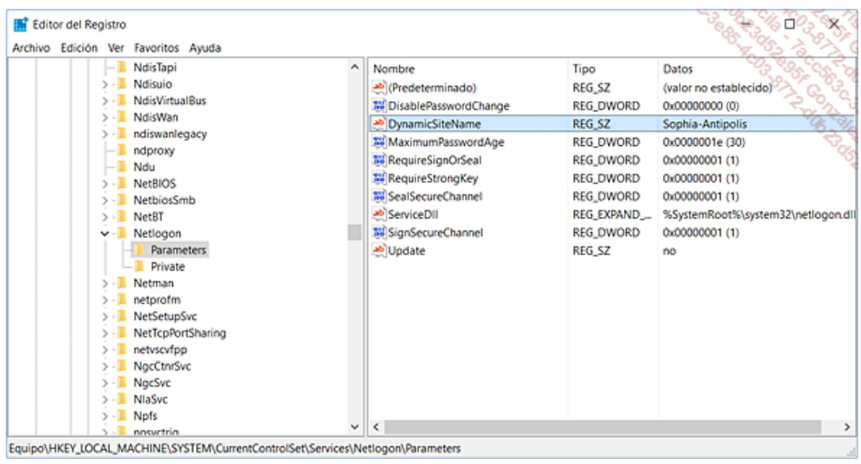
4. El Contralor informará entonces el cliente que no se encuentra en el antiguo sitio, y le enviará el nombre de su nuevo sitio de pertenencia.

5. El cliente dirige entonces sus peticiones DNS en los registros SRV para buscar un controlador de dominio que pertenezca a su nuevo sitio conocido inscrito en la partición de configuración Active Directory y en las zonas DNS.

6. Un controlador de dominio del nuevo sitio de pertenencia Active Directory se selecciona y responde al cliente Windows. A partir de ese momento, el cliente ajusta sus datos de localización y considera el nuevo sitio como su sitio de pertenencia.

Cuando el usuario vuelva a su lugar de origen o por qué no a otro sitio, este proceso se realizará de nuevo para actualizar de forma dinámica la información de localización del equipo cliente.

Los clientes de Active Directory que utilizan los sistemas operativos Windows 2000 hasta Windows 10 o Windows Server 2016 guardan el nombre del sitio Active Directory en la clave del registro de siguiente: HKLM \ System \ CurrentControlSet \ Services \ Netlogon \ Parameters \ DynamicSiteName —.



El método de búsqueda de los controladores de dominio por los equipos cliente parte del principio de que cada lugar geográfico es conocido, así como sus redes IP asociadas. Luego, el sitio debe incluir uno o varios controladores de dominio.

Uso de los registros SRV y proceso de selección vinculado a la búsqueda de los servidores de directorio LDAP

Cuando un usuario inicia una acción que requiere una búsqueda de Active Directory, el cliente Active Directory envía una consulta DNS con un registro de tipo SRV correspondiente a los servidores activos en el puerto LDAP TCP 389. La primera petición se dirige siempre al sitio Active Directory local del cliente en la medida en que el cliente ha logrado determinar su lugar de pertenencia con el método antes explicado. Este principio tiene, por supuesto, su principal ventaja al evitar el tráfico a través de redes extendidas. Por contra, si no hay un controlador de dominio disponible en el sitio del cliente, entonces el cliente enviará una solicitud de resolución sobre todos los registros SRV con independencia del lugar de pertenencia, lo que corresponde en potencia a interrogar a cualquier controlador de dominio en el dominio de pertenencia, al menos hasta que la configuración de los sitios Active Directory se adapte de forma automática para resolver este problema.

Cobertura de los sitios Active Directory que ya no disponen o no cuentan con un controlador de dominio Active Directory

El sitio que no contenga un contralor o donde un controlador ha dejado de responder quedará de forma automática incluido por la infraestructura de Active Directory a través de los componentes KCC (*Knowledge Consistency Checker*) y ISTG (*Inter Site Topology Generator*). De hecho, el primer controlador de dominio instalado en un sitio desempeña el papel de ISTG y se hace cargo de la creación de objetos de conexión a otros sitios. Visto su importante papel, ISTG también revisa la construcción de la topología de replicación y, por lo tanto las comunicaciones intersitio.

Cada 30 minutos, ISTG prueba su existencia actualizando el atributo **InterSiteTopologyGenerator** del objeto NTDS Settings. Este atributo y su valor se replican luego y los controladores podrán verificar cada 60 minutos la presencia correcta del ISTG de cada uno de los sitios. Esta operación consistirá en ayudar al sitio huérfano actualizando las zonas DNS del sitio a través de la declaración de controladores de dominio plenamente operativos procedentes del sitio "más cercano".

De esta forma, los controladores de dominio del sitio A, pueden hacerse cargo de todas las peticiones de autenticación del sitio B cuando el sitio B no dispone de al menos un controlador de dominio operativo.

Este comportamiento se explica más adelante en detalle.

Compatibilidad entre los equipos cliente y los dominios Active Directory

Los dominios Active Directory que utilizan controladores de dominio Windows Server 2003 hasta Windows Server 2016 son compatibles al 100% con todos los tipos de clientes Windows. Esta compatibilidad también se proporciona con los sistemas que usan clientes no-Windows mediante el soporte del cliente Samba versión 3.0 y posterior, con frecuencia utilizado en las plataformas UNIX, Linux y Apple OS/X.

Samba es un conjunto de servicios y herramientas que permite a los equipos con Linux, UNIX, Apple u otros sistemas conectarse y compartir o utilizar los recursos de tipo archivos e impresoras a través de protocolos como NTLM, Kerberos y SMB/CIFS. Mientras que las versiones 3.x pueden desempeñar el papel de un controlador de dominio compatible NT4, las últimas implementaciones de SAMBA a partir de la versión 4.x también pueden desempeñar el papel de controlador de dominio Active Directory. Aunque la aplicación de este tipo de solución no sea fácil y requiere una atención especial en términos de soporte, mantenimiento y administración, múltiples configuraciones Microsoft / SAMBA permiten soportar diferentes escenarios para permitir a los usuarios de Windows acceder con toda transparencia a los recursos compartidos por los equipos no-Windows, como los equipos que funcionan con Linux. Por supuesto, también puede lograrse en sentido contrario .

La versión de Samba 4.4 publicada en marzo de 2016 es una versión muy similar a un verdadero controlador de dominio Active Directory. Sin embargo, muchas diferencias dificultan la aplicación operativa de este tipo de controladores de dominio no-Windows. En efecto, la documentación de SAMBA especifica que para preservar la compatibilidad con los controladores de dominio Windows Server, es recomendable utilizar los niveles funcionales de dominio y bosque de Windows Server 2003. Cabe señalar que si este requisito previo permite una compatibilidad con los controladores de dominio que funcionen desde Windows Server 2003 hasta Windows Server 2012 R2, lamentablemente, se limita de manera importante las funcionalidades ofrecidas en el dominio Active Directory y excluye también a Windows

Server 2016. Otras restricciones importantes son notables con la replicación del volumen SYSVOL no soportada a través NTFRS o DFSR que requiere la aplicación de mecanismos para rodear la limitación basados en Robocopy bajo Windows o rsync bajo Linux. Cabe destacar también la pérdida de funcionalidad como la papelera de Active Directory o la recuperación granular de los objetos borrados a través de las instantáneas (snapshots) de Active Directory. En resumen, los controladores Active Directory que funcionan en Linux con SAMBA 4 son aún poco operativos a nivel empresarial. Es preferible a día de hoy emplear estos sistemas en forma autónoma de los controladores de dominio Windows Server.

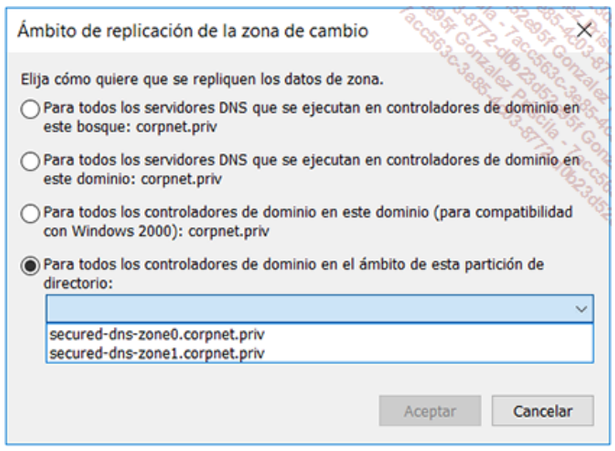
El equipo Samba recibe documentos de protocolos Microsoft: el 20 de diciembre de 2007, el organismo PFIF - *Protocol Freedom Information Foundation*, una entidad sin ánimo de lucro creada por la Software Freedom Law Center, firmó un acuerdo con Microsoft para obtener un acceso completo a la documentación de los protocolos necesarios para la interoperabilidad entre los servidores Microsoft Windows Server y el software libre como Samba. Esta apertura iniciada tras la llegada de Windows 2000 Server es hoy una realidad con el compromiso de Microsoft en torno a la comunidad open source en muchos ámbitos. Para más información sobre estos acuerdos estratégicos, podemos consultar el enlace: https://www.microsoft.com/en-us/openness/

Estructura DNS e integración en el directorio Active Directory

La localización de los servicios de Active Directory por los clientes de Windows depende de la disponibilidad de la zona DNS. Es por esta razón que las versiones de -Windows Server 2003 hasta Windows Server 2016 disponen de medios modernos para garantizar una alta disponibilidad de todos los tipos de zonas y, en particular, de la zona DNS correspondientes a la raíz del bosque Active Directory.

Sabemos que el directorio Active Directory puede integrar las zonas y registros de recursos (RR) como objetos del directorio (objetos dnsZone y dnsNode). En efecto, la información DNS que debe ser protegida no pueden contentarse con un simple almacenamiento de tipo archivo de texto. Este punto es en especial importante para la protección de los registros contenidos en las zonas DNS dinámicas y, de hecho, se recomienda utilizar siempre las zonas integradas en Active Directory.

El uso de controladores de dominio Windows Server 2003 hasta Windows Server 2016, permite utilizar las particiones del directorio de aplicaciones y así poder almacenar cualquier zona DNS en extensiones de replicación diferentes. A continuación presentamos estas distintas extensiones de replicación:



Extensiones de replicación de una zona con Windows Server 2003

Para todos los servidores DNS que se ejecutan en este dominio: esta opción permite almacenar la zona DNS en una partición del directorio de aplicaciones. La zona se replicará en todos los servidores DNS que funcionen en controladores de dominio Windows Server 2003 hasta Windows Server 2016 en todo el bosque.

Esta partición del directorio de aplicaciones se crea durante la instalación del servicio de servidor DNS en el primer controlador de Dominio Windows Server del bosque.

Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: esta opción permite almacenar las zonas DNS en los servidores DNS que funcionan en controladores de dominio Windows Server 2003, hasta Windows Server 2016, en todo el dominio.

En el caso del dominio raíz del bosque, esta partición del directorio de aplicaciones se crea durante la instalación del servicio Servidor DNS en el primer controlador de dominio Windows Server 2003 hasta Windows Server 2016. Luego, para cada nuevo dominio creado en el bosque, una nueva partición del directorio de aplicaciones se crea durante la instalación del servicio de servidor DNS en un controlador del nuevo dominio.

Para todos los controladores de dominio en este dominio: esta opción permite almacenar las zonas DNS en la partición del dominio, para cada dominio del bosque. En este caso, las zonas DNS se replican en todos los controladores de dominio del -dominio.

Tenga en cuenta que esta es la única opción de almacenamiento posible cuando se cuenta todavía con controladores de dominio Windows 2000 Server. Aunque esta opción haya sido implementada para garantizar el soporte de los controladores de dominio Windows 2000 Server, esta opción puede utilizarse también para los controladores de dominio que utilizan las versiones de Windows Server 2003 hasta Windows Server 2016.

Para todos los controladores de dominio en el ámbito de esta partición de directorio: esta opción permite almacenar las zonas DNS en una partición del directorio de aplicaciones creada de forma previa. Las zonas DNS almacenadas en esta partición del directorio de aplicaciones se replicarán a todos los servidores DNS que funcionen en los controladores de dominio pertinentes para esta partición.

Hemos visto antes que los registros de recursos utilizados por el servicio de localización principal para un dominio Active Directory dado se almacenan en el subdominio **_msdcs.NombredeDominioDns**. A partir de Windows Server 2003, y hasta Windows Server 2016, cuando el dominio raíz del bosque se crea, una zona DNS específica se implementa de forma automática para el subdominio **_msdcs.NombredeBosque** en la partición del directorio de aplicaciones dedicadas a las zonas DNS de tipo *bosque*. Estas particiones disponen de un almacenamiento en toda la extensión del bosque y por lo tanto se replican en todos los controladores de dominio de todos los dominios del bosque.

Observe que las zonas DNS almacenadas en las particiones del directorio de aplicaciones no pueden ser vistas por los controladores Windows 2000 Server. Este punto es lógico, ya que los controladores Windows 2000 Server solo reconocen las particiones de esquema, configuración y de dominio(s). Las particiones del directorio de aplicaciones solo son reconocidas por las versiones de Windows Server 2003 y posteriores hasta Windows Server 2016, un antiguo controlador Windows 2000 Server se negará a replicar este tipo de contexto de nombres.

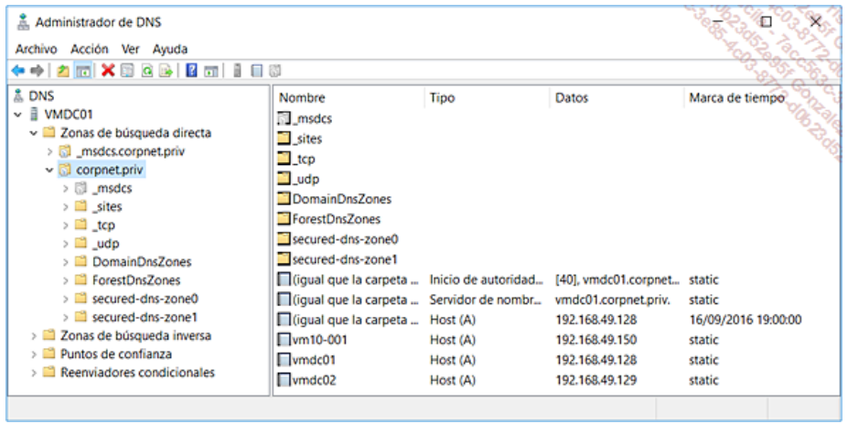
Registros DNS de Ubicación del servicio de los controladores de dominio

Los clientes Active Directory emplean el sistema de resolución DNS de forma exclusiva para localizar los controladores de dominio Active Directory. Esta operación fundamental se inicia por el cliente a través de las solicitudes de resolución de registros de recurso de tipo SRV (*Service Locator Resource Record*) definidos en el marco de la RFC 2782, sucesora de la RFC 2052.

Estos registros son utilizados para localizar la ubicación de los servicios correspondientes a los equipos, puertos y protocolos requeridos por el cliente. Entre los servicios localizados, vamos a encontrar los servicios de directorio LDAP, los servicios de autenticación Kerberos y los servicios de catálogo ofrecidos por los controladores de dominio de tipo catálogo global. La idea es que los controladores de dominio organizan los registros de recursos de tipo SRV de manera estructurada de tal forma que los clientes Active Directory puedan localizar el controlador que presta el servicio o servicios deseados dentro de un dominio o en un sitio Active Directory.

1. Estructura de mantenimiento de la zona DNS para los registros de recursos de tipo SRV

La estructura DNS utilizada para alojar a los registros requeridos por el servicio de localización de los controladores de dominio se basa en una jerarquía de dominios DNS. La imagen siguiente muestra el contenido de estas zonas DNS:



La imagen ilustra la estructura de los cuatro subdominios técnicos DNS en relación con un dominio Active Directory

Estos diferentes subdominios agrupan los registros en función de la naturaleza de las búsquedas a realizar. A continuación presentamos estos diferentes tipos de subdominios y registros:

_MSDCS: este subdominio contiene un conjunto de registros de tipo SRV. Estos registros son función del estado de los controladores de dominio, del tipo de peticiones y también los roles del catálogo global y el controlador de dominio primario. Los controladores de dominio y catálogos globales se reparten por sitios. De esta manera, los clientes Active Directory son capaces de localizar de forma instantánea los servicios más "próximos" a ellos.

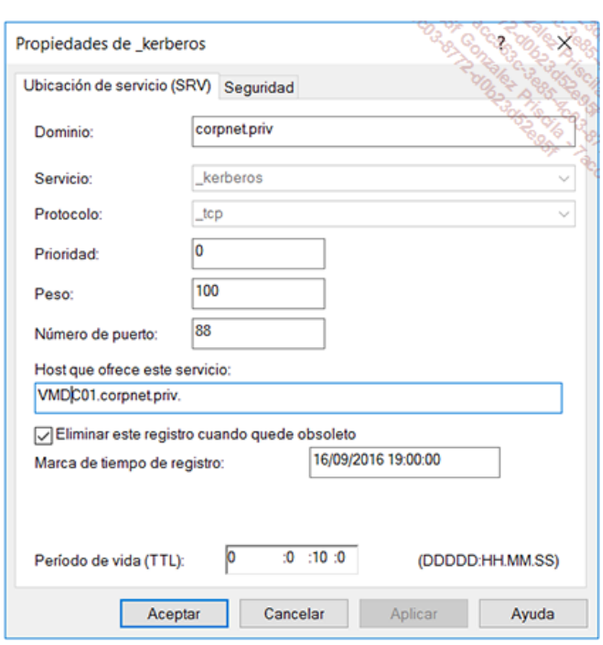
_SITES: este subdominio contiene todos los sitios Active Directory declarados en la infraestructura física basado en las subredes IP asociadas. El hecho de determinar los controladores de dominio en función de su pertenencia a los sitios permite a los clientes Active Directory localizar con facilidad los controladores de dominio en función de los servicios que prestan y su ubicación. Este método permite evitar varias búsquedas LDAP a través de conexiones lentas. Observe que los controladores de dominio dispuestos en los sitios Active Directory utilizan los puertos TCP y UDP 389 para el protocolo estándar LDAP, mientras que las equipos de tipo catálogo global utilizan el puerto TCP 3268. En el caso en que se utilice el protocolo LDAPS, se empleará para los mensajes LDAP y los mensajes a los catálogos generales los puertos TCP/UDP 636 y TCP 3269 de forma respectiva.

_TCP: este subdominio contiene todos los controladores de dominio de la zona DNS. El hecho de agrupar todos los controladores de dominio por protocolo será útil a los clientes que no sean capaces de localizar un controlador disponible en su sitio local. En este caso, los clientes Active Directory seleccionarán un controlador de dominio de cualquier ubicación de la red.

_UDP: en este subdominio se identifican los Servicios Kerberos v5 disponibles en modo no conectado a través del protocolo de transporte UDP. Estas operaciones se realizan de la misma forma que con el transporte TCP. Observe que las operaciones de peticiones de tickets utilizan el puerto UDP 88 mientras que las operaciones de cambio de contraseña utilizan el puerto UDP 464.

a. Acerca del registro de recursos DNS de tipo SRV

El registro de recursos de tipo SRV (*Service Locator Resource Record*) se define según descrito en la RFC 2782 y contiene los datos mostrados en la imagen siguiente:



Registro SRV para especificar que el equipo desempeña el rol de servidor Kerberos (V5) en el puerto TCP 88

Los diferentes parámetros de un registro de recursos de tipo SRV se presentan en el cuadro siguiente.

Componentes del registro SRV	Ejemplos de valores	Comentarios
Servicio	_gc _kerberos _ldap	Identifica el servicio a localizar en el espacio de nombres DNS.
Protocolo	_tcp _udp	Declaración del protocolo de transporte a utilizar.
Nombre	corpnet.priv	Es el nombre de dominio DNS que contiene el registro.
TTL	10 minutos	Representa la duración de vida del registro en segundos (600 segundos) en la caché de los clientes.
Clase	IN	Declara el tipo de registro como registro estándar de tipo DNS de Internet.
Registro de recurso	SRV	Declara el tipo de registro como registro estándar de tipo ubicación de servicios SRV.
Prioridad	0	Identifica la prioridad del registro. Cuando existen varios registros para el mismo servicio, el cliente selecciona el registro con el valor de prioridad mas bajo.
Peso	100	Permite la gestión de las funciones de reparto de carga. Si para el mismo servicio existen varios registros de SRV de la misma prioridad, los clientes seleccionan el o los registros de mayor peso.
Puerto	3268 para _gc 88 para _kerberos 389 para _ldap	Identifica el número de puerto sobre el que se encuentra disponible el servicio solicitado.
Objetivo	Nombre DNS (FQDN) del servidor Windows Server	Representa el nombre completo del equipo que proporciona el servicio identificado por el registro.

Utilización de caracteres underscore

Observamos que el formato de los registros de recursos SRV emplean en gran medida el carácter *underscore (_)*. En efecto, la RFC 2782 declara el uso de este carácter para resolver el problema de una posible colisión con un nombre idéntico.

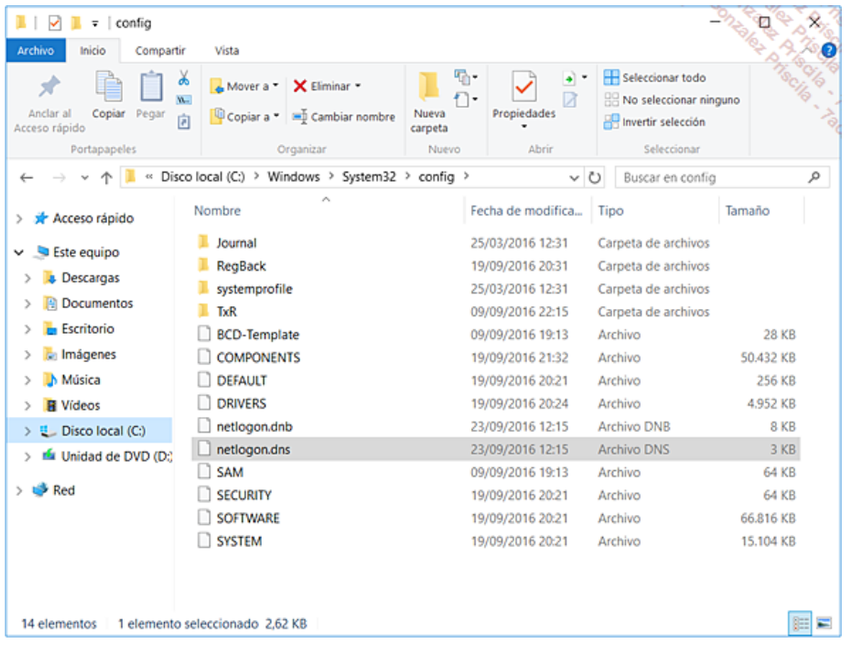
En 1996 en la RFC 2052, en 2000 en la RFC 2782: las primeras implementaciones del servicio DNS para localizar servicios de Active Directory se realizaron en las primeras versiones de prueba de Windows NT 5.0, durante 1997. Microsoft se basó en las primeras recomendaciones que aparecen en la RFC 2052 con fecha de 1996. Es mucho más tarde, en febrero de 2000, fecha de la salida oficial de Windows 2000, que esta RFC pasará del estado "Draft" al estado "Proposed Standard". También será objeto de un nuevo registro por parte de la IETF, empleando el número 2782, y reemplazará la RFC 2052. El Sr. Levon ESIBOV, Gestor de proyectos de Microsoft, participará en esta RFC fundamental para la búsqueda y localización de los servicios de Active Directory.

Para saber más sobre el contenido de estas RFC, visitar el sitio http://www.rfc-editor.org. En Internet, ¡muchos sitios contienen las RFC, pero pocos de estos están actualizados! Este sitio es un sitio oficial de la Internet Society. Tiene por objeto mantener el conjunto de los documentos RFC para toda la comunidad de Internet.

Los registros de recursos grabados por los controladores de dominio se describen más adelante. Antes de entrar en los detalles de éstos, ¡recordemos que estos registros SRV y A son vitales! El comando **DNSLint** podrá ser de gran ayuda para controlar que todos los registros de todos los controladores de dominio estén presentes.

Observe que un controlador de dominio graba como mínimo quince registros de recursos y veinte cuando desempeña también la función de Catálogo Global.

En caso de necesidad, consulte el archivo **%SystemRoot%\system32\config\Netlogon.DNS**.



Archivo Netlogon.DNS y registros SRV

Este archivo, mantenido por cada controlador de dominio, se actualiza de forma automática para reflejar la estructura física del bosque.

```
corpnet.priv. 600 IN A 192.168.1.100
_ldap._tcp.corpnet.priv. 600 IN SRV 0 100 389 vmdc01.corpnet.priv.
_ldap._tcp.pdc._msdcs.corpnet.priv. 600 IN SRV 0 100 389 vmdc01.corpnet.priv.
_ldap._tcp.gc._msdcs.corpnet.priv. 600 IN SRV 0 100 3268 vmdc01.corpnet.priv.
_ldap._tcp.2ddc1bad-b6b7-4448-8d79-52383b97db4f.domains._msdcs.corpnet.priv.
600 IN SRV 0 100 389 vmdc01.corpnet.priv.
```

```
gc._msdcs.corpnet.priv. 600 IN A 192.168.1.100
6143dbaa-715b-4651-b1da-80e754256c8a._msdcs.corpnet.priv. 600 IN CNAME
vmdc01.corpnet.priv.
_kerberos._tcp.dc._msdcs.corpnet.priv. 600 IN SRV 0 100 88
vmdc01.corpnet.priv.
_ldap._tcp.dc._msdcs.corpnet.priv. 600 IN SRV 0 100 389 vmdc01.corpnet.priv.
_kerberos._tcp.corpnet.priv. 600 IN SRV 0 100 88 vmdc01.corpnet.priv.
_gc._tcp.corpnet.priv. 600 IN SRV 0 100 3268 vmdc01.corpnet.priv.
_kerberos._udp.corpnet.priv. 600 IN SRV 0 100 88 vmdc01.corpnet.priv.
_kpasswd._tcp.corpnet.priv. 600 IN SRV 0 100 464 vmdc01.corpnet.priv.
_kpasswd._udp.corpnet.priv. 600 IN SRV 0 100 464 vmdc01.corpnet.priv.
DomainDnsZones.corpnet.priv. 600 IN A 192.168.1.100
_ldap._tcp.DomainDnsZones.corpnet.priv. 600 IN SRV 0 100 389
vmdc01.corpnet.priv.
ForestDnsZones.corpnet.priv. 600 IN A 192.168.1.100
_ldap._tcp.ForestDnsZones.corpnet.priv. 600 IN SRV 0 100 389
vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.corpnet.priv. 600 IN SRV 0 100 389
vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.gc._msdcs.corpnet.priv. 600 IN SRV 0 100
3268 vmdc01.corpnet.priv.
_kerberos._tcp.Sophia-Antipolis._sites.dc._msdcs.corpnet.priv. 600 IN SRV 0 100
88 vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.dc._msdcs.corpnet.priv. 600 IN SRV 0 100 389
vmdc01.corpnet.priv.
_kerberos._tcp.Sophia-Antipolis._sites.corpnet.priv. 600 IN SRV 0 100 88
vmdc01.corpnet.priv.
_gc._tcp.Sophia-Antipolis._sites.corpnet.priv. 600 IN SRV 0 100 3268
vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.ForestDnsZones.corpnet.priv. 600 IN SRV 0
100 389 vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.DomainDnsZones.corpnet.priv. 600 IN SRV 0
100 389 vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.secured-dns-zone0.corpnet.priv. 600 IN SRV 0
100 389 vmdc01.corpnet.priv.
_ldap._tcp.Sophia-Antipolis._sites.secured-dns-zone1.corpnet.priv. 600 IN SRV 0
100 389 vmdc01.corpnet.priv.
```

Microsoft recomienda que los servidores DNS con autoridad sobre las zonas necesarias para el buen funcionamiento del directorio Active Directory funcionen en servidores más modernos. De esta manera, las zonas se mantendrán de forma dinámica por Active Directory con la máxima seguridad. Esta observación también tiende a preferir las arquitecturas que implementen un número limitado de controladores de dominio. De esta forma, las operaciones de actualización de la infraestructura de Active Directory se podrán contemplar con un mínimo de esfuerzo e impacto.

b. Registros SRV grabados por el Servicio Inicio de sesión Red

Para responder a la problemática de la localización de un servicio dentro de una infraestructura Active Directory, se requieren muchos registros SRV.

A continuación listamos los registros DNS de tipo SRV correspondiente a los diferentes servicios de Active Directory y su entorno:

_ldap._tcp.NombredeDominio.

Permite a un cliente localizar un servidor LDAP en el dominio llamado **NombredeDominio**. Observe que el servidor no es por necesidad un controlador de dominio, aunque sea siempre el caso. De hecho, el punto más importante es que soporte las API LDAP. Todos los controladores de dominio registran esta grabación.

_ldap._tcp.NombredeSitio._sites.NombredeDominio.

Permite a un cliente localizar un servidor LDAP en el dominio llamado **NombredeDominio** y en el sitio llamado **NombredeSitio. NombredeSitio** corresponde al RDN (*Relative Distinguished Name*) del objeto sitio almacenado en la configuración Active Directory. Todos los controladores de dominio graban este registro.

_ldap._tcp.dc._msdcs.NombredeDominio.

Permite a un cliente localizar un controlador de dominio (**dc**) en el dominio llamado **NombredeDominio**. Todos los controladores de dominio graban este registro.

_ldap._tcp.NombredeSitio.sitios.dc._msdcs.NombredeDominio.

Permite a un cliente localizar un controlador de dominio en el dominio llamado **NombredeDominio** y en el sitio llamado**NombredeSitio**. Todos los controladores de dominio graban este registro.

_ldap._tcp.pdc._msdcs.NombredeDominio.

Permite a un cliente localizar el servidor PDC Emulator en el dominio llamado **Nombrededominio** que trabaja en modo mixto. Solo los PDCE FSMO (*Flexible Single Master Operations*) graban este registro.

_ldap._tcp.gc._msdcs.NombredeBosque.

Permite a un cliente localizar un catálogo global (**gc**) para el bosque. Sólo los controladores de dominio que actúan como GC graban este registro.

_ldap._tcp.NombredeSitio._sitios.gc._msdcs.NombredeBosque.

Permite a un cliente localizar un catálogo global (**gc**) dentro del bosque. Sólo los controladores de dominio que actúan como GC graban este registro.

_gc._tcp.NombredeBosque.

Permite a un cliente localizar un catálogo global (**gc**) en el dominio raíz del bosque. Este servidor no es por necesidad un controlador de dominio. Basta con que el protocolo LDAP funcione y que el servidor funcione como GC. Otras implementaciones de los servicios de directorio pueden a su vez registrar los servidores de directorio como GC.

_gc._tcp.NombredeSitio._sitios.NombredeBosque.

Permite a un cliente localizar un catálogo global (**gc**) para el bosque en el sitio llamado **NombredeSitio**. El servidor no es por necesidad un controlador de dominio, aunque sea siempre el caso. Sólo los servidores que actúan como servidores LDAP y GC

graban este registro.

_ldap._tcp.DomainGuid.domains._msdcs.NombredeBosque.

Permite a un cliente localizar un controlador de dominio en un dominio empleando el GUID (*Globally Unique IDentifier*) de este último. El GUID es un valor de 128 bits generado de forma automática en el momento de la creación del dominio y utilizado en raras ocasiones. De hecho, esta información solo deberá utilizarse si el nombre de dominio ha cambiado, pero el dominio raíz sigue siendo conocido. Todos los controladores de dominio graban este registro.

_kerberos._tcp.NombredeDominio.

Permite a un cliente localizar un KDC Kerberos en el dominio llamado **NombredeDominio**. El servidor no es por necesidad un controlador de dominio, aunque sea siempre el caso. Todos los servidores Windows Server que desempeñan el rol de Kerberos KDC cumplen con la RFC 1510 grabando este registro de recurso.

_kerberos._udp.NombredeDominio.

Este registro permite el mismo proceso que **_kerberos_tcp.NombredeDominio**, pero basándose en el protocolo de transporte UDP.

_kerberos._tcp.NombredeSitio._sitios.NombredeDominio.

Permite a un cliente localizar un KDC Kerberos para el dominio llamado **NombredeDominio** dentro del sitio llamado **NombredeSitio**. El servidor no es por necesidad un controlador de dominio. Todos los servidores Windows Server que desempeñan el rol de Kerberos KDC cumplen con la RFC 1510 grabando este registro de recurso.

_kerberos._tcp.dc._msdcs.NombredeDominio.

Permite a un cliente localizar un controlador de dominio que soporte la implementación de Windows Server 2003 del Servicio Kerberos KDC en el dominio llamado **NombredeDominio**. Todos los controladores de dominio Windows Server que ejecutan el servicio KDC graban este registro de recurso SRV. Estos servidores implementan una extensión de tipo clave pública con el protocolo Kerberos v5 llamada subprotocolo "Authentication Service Exchange" (subprotocol) y graban este registro SRV.

_kerberos.tcp.NombredeSitio._sitios.dc._msdcs.NombredeDominio.

Permite a un cliente localizar un controlador de dominio que soporte la implementación de Windows Server del Servicio Kerberos KDC en el dominio llamado **NombredeDominio** y en el sitio llamado **NombredeSitio**. Todos los controladores de dominio Windows Server que ejecutan el servicio KDC graban este registro de recurso SRV. Estos servidores implementan una extensión de tipo clave pública con el protocolo Kerberos v5 llamada subprotocolo "Authentication Service Exchange (subprotocol) y graban este registro SRV.

_kpasswd._tcp.NombredeDominio.

Permite a un cliente localizar un servidor de cambio de contraseña Kerberos para el dominio especificado. Todos los controladores de dominio Windows graban este registro. Dicho servidor debe soportar el protocolo de cambio de contraseña Kerberos. Este servidor no es por necesidad un controlador de dominio, aunque sea siempre el caso. Todos los controladores de dominio Windows Server que ejecutan el servicio Kerberos KDC cumplen con la RFC 1510 grabando este registro de recurso.

_kpasswd._udp.NombredeDominio.

Este registro permite el mismo proceso que **_kpasswd_tcp.NombredeDominio**, pero basándose en el protocolo de transporte UDP.

DsaGuid._msdcs.NombredeBosque

El servicio de acceso a la red (Net Logon) registra también un alias (CNAME) utilizado para la replicación de Active Directory. El sistema de localización de los controladores no utiliza directamente este registro vital para la infraestructura. Todos los controladores de dominio de todos los dominios del bosque se registran directamente en el dominio raíz del bosque en**_msdcs.NombredeBosque**.

c. Con respecto al registro DsaGuid._msdcs.NombredeBosque

El registro de recurso **DsaGuid._msdcs.NombredeBosque** permite la localización de cualquier controlador de dominio miembro del bosque. Corresponde al valor del GUID del controlador de dominio que es el valor del objeto DSA (*Directory System Agent*).

Este registro se utiliza en el marco de la replicación de los controladores de dominio en base a la configuración de la topología de replicación. Microsoft especifica que este registro también se utiliza para las operaciones de cambio de nombre de los equipos controladores de dominio en un dominio que funcione en un nivel funcional desde Windows Server 2003 hasta Windows Server 2016.

El valor de **DSAGuid** es igual al valor del atributo **objectDSA** del contenedor **NTDS Settings** del objeto servidor correspondiente al controlador de dominio.

d. Registros de recursos para los clientes no compatibles con los registros SRV

El servicio "Net Logon - Servicio Inicio de sesión red", registrará los registros de tipo A para los clientes LDAP que no soportan los registros SRV conformes con la RFC 2782. Por lo tanto, estos registros no se refieren a la metodología de selección presentada antes.

El registro A correspondiente al NombredeDominio permite a un cliente no compatible con los registros SRV localizar un controlador de dominio presente en el dominio basándose en este registro.

El registro A correspondiente a **gc._msdcs.Nombredebosque** permite a un cliente no compatible con los registros SRV localizar un controlador de dominio de catálogo global ubicado en el bosque.

2. Servidores DNS no dinámicos y registros dinámicos de los controladores de dominio

Por lo general, las zonas DNS utilizadas en el marco del directorio Active Directory son soportados por los servidores DNS que funcionan en todas las versiones de Windows Server y las zonas DNS integradas en Active Directory.

Sin embargo, si es necesario utilizar servidores DNS no Windows y en este caso, elegimos utilizar zonas DNS no dinámicas, entonces podemos impedir la grabación de todos o parte de los registros SRV grabados por los controladores de dominio.

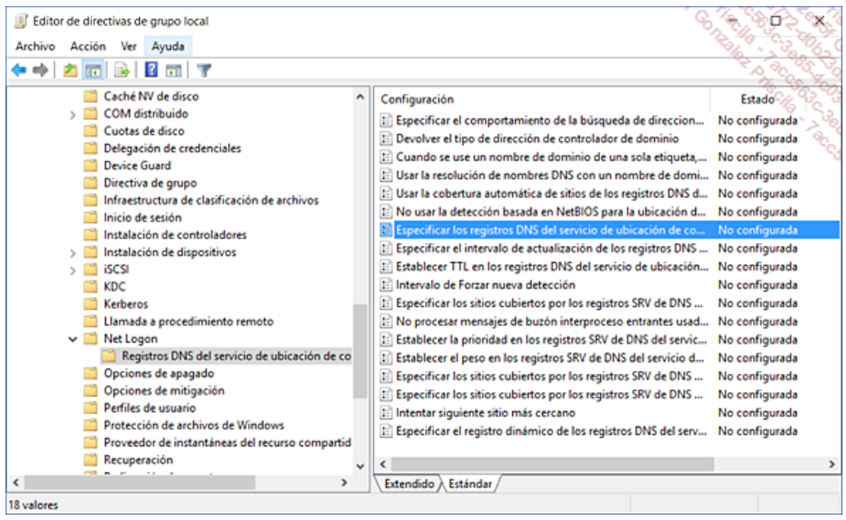
Esta configuración se puede efectuar de forma directa creando un objeto de directiva de grupo y configurando el parámetro especificado a continuación:

Configuración del Equipo/Plantillas administrativas/Sistema/Inicio de sesión de Red /registros DNS del localizador de controladores de

dominio/registros DNS del localizador de controladores de dominio no inscrito por los controladores de dominio.

Para activar este parámetro, seleccionamos la opción y luego especificamos una lista de mnemotécnicos (Instrucciones) delimitados por espacios para los registros DNS del localizador de controladores de dominio que no serán almacenados por los controladores de dominio para los que se aplica este parámetro.

La lista de palabras clave que podemos usar se especifica a continuación bajo el formato palabra clave / Tipo de registro / nombre



Seleccione los mnemotécnicos de la lista siguiente:

Mnemotécnico	Tipo	Registro DNS
LdapIpAddress	A	<NombreDominioDNS>
Ldap	SRV	_ldap._tcp.<NombreDominioDNS>
LdapAtSite	SRV	_ldap._tcp.<NombreSitio>._sites.<NombreDominioDNS>
Pdc	SRV	_ldap._tcp.pdc._msdcs.<NombreDominioDNS>
Gc	SRV	_ldap._tcp.gc._msdcs.<NombreBosqueDNS>
GcAtSite	SRV	_ldap._tcp.<NombreSitio>._sites.gc._msdcs.<NombreBosqueDNS>
DcByGuid	SRV	_ldap._tcp.<GUIDdominio>.domains._msdcs.<NombreBosqueDNS>
GcIpAddress	A	gc._msdcs.<NombreBosqueDNS>
DsaCname	CNAME	<GUIDDSA>._msdcs.<NombreBosqueDNS>
Kdc	SRV	_kerberos._tcp.dc._msdcs.<NombreDominioDNS>
KdcAtSite	SRV	_kerberos._tcp.<NombreSitio>._sites.dc._msdcs.<NombreDominioDNS>
Dc	SRV	_ldap._tcp.dc._msdcs.<NombreDominioDNS>
DcAtSite	SRV	_ldap._tcp.<NombreSitio>._sites.dc._msdcs.<NombreDominioDNS>
Rfc1510Kdc	SRV	_kerberos._tcp.<NombreDominioDNS>
Rfc1510KdcAtSite	SRV	_kerberos._tcp.<NombreSitio>._sites.<NombreDominioDNS>
GenericGc	SRV	_gc._tcp.<NombreBosqueDNS>
GenericGcAtSite	SRV	_gc._tcp.<NombreSitio>._sites.<NombreBosqueDNS>
Rfc1510UdpKdc	SRV	_kerberos._udp.<NombreDominioDNS>
Rfc1510Kpwd	SRV	_kpasswd._tcp.<NombreDominioDNS>
Rfc1510UdpKpwd	SRV	_kpasswd._udp.<NombreDominioDNS>

Este parámetro se encuentra desactivado por defecto. En consecuencia, los controladores de dominio, configurados para realizar una grabación dinámica de los registros DNS del localizador de controladores de dominio, graban todos los registros de recurso DNS del localizador de controladores de dominio en una zona DNS dinámica.

3. Con respecto a la zona DNS del dominio raíz del bosque

En un bosque compuesto por varios dominios, es importante prestar gran atención al dominio raíz del bosque. Para ilustrar esta necesidad, los siguientes puntos nos podrán servir de guía:

- Entre los errores a evitar, no debemos confundir el dominio raíz del bosque con el dominio raíz de un árbol del bosque. Recuerde que el dominio raíz del bosque es siempre el primer dominio creado.
- El dominio raíz del bosque "añade" a los otros dominios DNS al dominio raíz. Por supuesto, sólo el primer dominio de un bosque puede desempeñar este papel. En el caso de que un dominio adicional exista dentro del bosque, los equipos que desempeñen el papel de catálogo global siguen grabando sus registros de recursos SRV en la zona **_msdcs.root.dns**.

Todos los registros necesarios para la localización de los controladores de dominio que desempeñen el rol de catálogo Global se registran en el dominio raíz del bosque. Este punto es muy lógico, porque si bien es cierto que un controlador de dominio de un determinado dominio ofrece sus servicios en este dominio, es también cierto que la función de un Catálogo Global consiste en ofrecer sus servicios a todos los dominios del bosque.

Limitaciones y problemas potenciales

La necesidad de disponer de servicios DNS configurados de forma correcta es tal que podemos desde ya incluir dos tipos de limitaciones y problemas potenciales:

- El primer tipo de limitaciones se refieren al directorio Active Directory, los controladores de dominio y otros componentes o aplicaciones que utilizan el directorio, tal como se especifica a continuación. Si los servicios DNS no permiten ayudar a la resolución de las búsquedas necesarias a los controladores de dominio, puede tener lugar un fallo grave, e incluso total, de las replicaciones de Active Directory entre controladores de dominio. En el mismo orden de ideas, podemos citar, por ejemplo, aplicaciones de empresa como Microsoft Exchange o Microsoft System Center Configuration Manager. Al contar estas aplicaciones con un importante nivel de integración con el directorio Active Directory, también podrán verse más o menos afectadas en caso de fallo de los servidores DNS y/o de autenticación.
- El segundo tipo de limitaciones DNS se refiere a los puestos de trabajo y servidores miembro del dominio . En el caso de los equipos cliente de Active Directory, los posibles fallos de los servicios DNS pueden ser menos dramáticos. En efecto, la falta de servicios DNS tendrá como principal efecto el aumento del tiempo de búsqueda de un controlador Windows Server hasta su fallo.


Infraestructura Windows Active Directory y fallos DNS: El sistema DNS es hoy en día el sistema de resolución y localización preferido tanto por la infraestructura Windows misma como las aplicaciones que permanecen en esta. Por lo tanto, entendamos el hecho de que una fallo o un error de configuración en el nivel de servicios DNS puede tener efectos devastadores sobre la infraestructura Windows completa y también sobre las aplicaciones que este abarca.

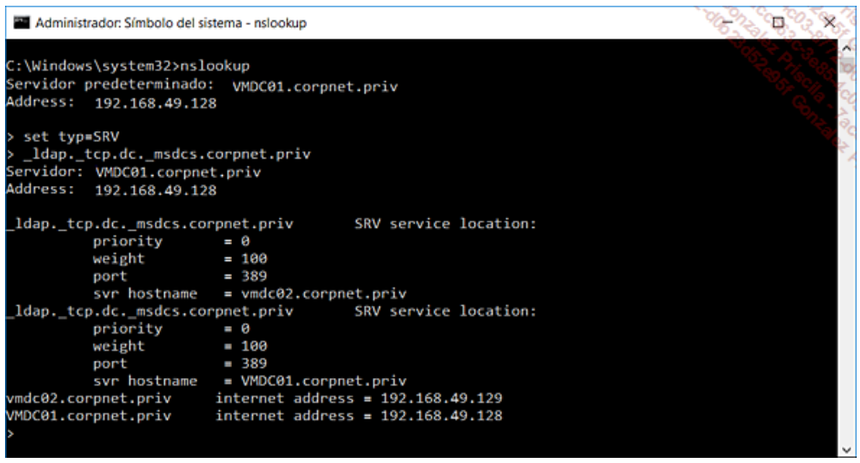
Control rápido de los registros de recursos

La detección de un problema de localización de uno o varios controladores de dominio suele ser bastante rápida. En efecto, el fallo de disponibilidad de un controlador de dominio en un sitio determinado suele ser sinónimo de una ralentización de las conexiones de red, e incluso de la falta de disponibilidad de determinados servicios de infraestructura o también aplicaciones.

1. Pruebas de los registros DNS

Para comprobar la configuración de nuestros registros, podemos usar las siguientes herramientas:

NSLookup: por ejemplo, podemos probar la correcta grabación de los registros de catálogo global. El primer comando set type=SRV nos permite solicitar a su vez los detalles de un registro de recurso de tipo SRV RR.



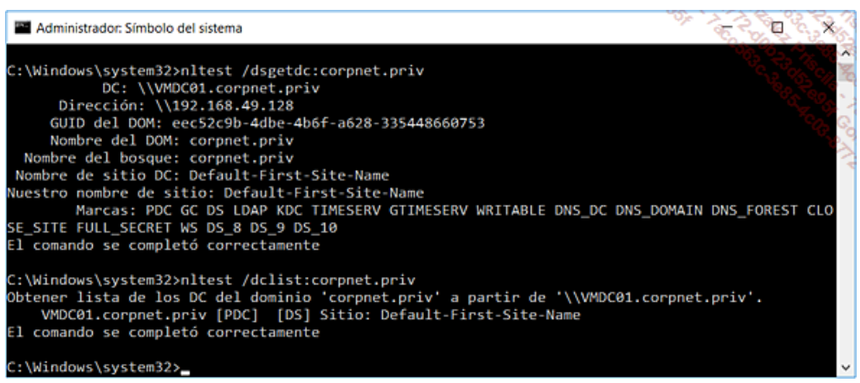
DCDiag: podemos utilizar el comando `DCDiag` (*Domain Controller Diagnostics*) para controlar los registros DNS de los «partners» de replicación.

NetDiag: podemos usar el comando `NetDiag` para comprobar los registros DNS correspondientes a un controlador de dominio específico. Para esto, utilizamos el siguiente comando en el controlador de dominio que deseamos probar: `Netdiag /test:DNS /v`

NLTests: podemos usar el comando NLTest (*Net Logon Test*) para probar todas las funciones soportadas por el servicio Inicio de sesión Red/Net Logon. Los muchos parámetros disponibles con este comando lo hacen muy completo para comprobar el estado de los canales seguros (*Secure Channel*), la selección de los controladores, los servidores de tiempo, los controladores disponibles en sitios Active Directory y las relaciones de aprobación entre dominios. También lo podemos emplear para probar los registros DNS utilizando el comando NLTest /DSQUERYDNS.

La imagen siguiente ilustra dos comandos muy útiles:

- El comando nltest `/dsgetdc:corpnet.priv` para listar el estado del controlador de dominio utilizado, así como el conjunto de funciones y roles de Active Directory soportadas.
- El comando `nltest /dclist:corpnet.priv` para listar los controladores y el nombre del sitio Active Directory considerado por el equipo.



Al igual que en la versiones anteriores de Windows Server, casi la totalidad de las herramientas de soporte se encuentran disponibles por defecto con Windows Server 2016.

Observe que el comando NLTest comprueba las zonas implicadas en el funcionamiento de Active Directory, pero no prueba las zonas adicionales o específicas creadas en las particiones del directorio de aplicaciones.

2. Regrabación de registros de tipo SRV de los controladores de dominio

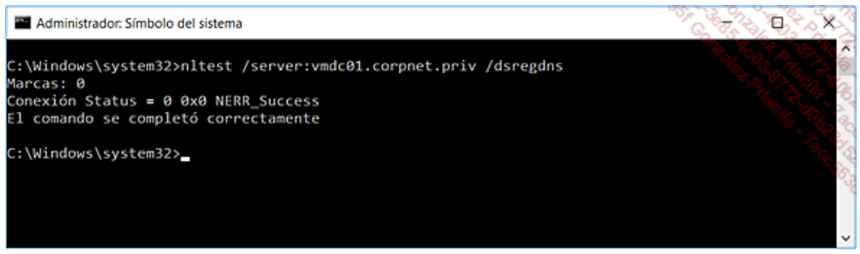
Podemos utilizar los siguientes comandos para forzar la regrabación de los registros DNS necesarios para el buen funcionamiento de los equipos controladores de dominio.

IPConfig: utilizar el comando `IPConfig /registerdns`. Observe que este comando no soporta las particiones del directorio de aplicaciones.

Servicio Inicio de sesión Red (en inglés Net Logon): reinicia el servicio "Inicio de sesión Red" en el controlador de dominio cuyos registros DNS deben ser regrabados.

NLTest: utilice el comando `NLTest /dsregdns` para forzar la regrabación de todos los registros de recursos necesarios para el controlador de dominio.

Este comando funciona también a través de la red. Así, para forzar la regrabación de los registros de un servidor remoto podemos usar el comando `NLTest /server: nombre_del_servidor /DSREGDNS`.



Observe que el comando NLTEST también permite reiniciar un servidor remoto y anular un proceso de de apagado remoto en curso de ejecución. Para esto podemos utilizar los comandos siguientes: `NLTest /server:nombre_del_servidor /SHUTDOWN:<Razón> [<nb_de_segundos>]` y `NLTest /server:nombre_del_servidor /SHUTDOWN_ABORT`.

3. Borrado de registros de tipo SRV de los controladores de dominio

Es posible que deseemos borrar los registros de recurso de tipo SRV relativos a un antiguo controlador de dominio. Esta operación de limpieza no es obligatoria pero si recomendable ya que tendrá el efecto de evitar intentos fallidos de conexión a un controlador de dominio inexistente.

Para realizar esta operación, podemos usar el siguiente comando NLTest: `NLTest /dsderegdns:FQDN_del_servidor`

También podemos especificar el tipo o tipos de registros de Active Directory a suprimir especificando los parámetros /dom, /domguid, /dsaguid

/DOM: el parámetro `/DOM:nombre_de_dominio_DNS` especifica el nombre DNS del dominio a utilizar para buscar el registro. Si este parámetro no se especifica, se emplea el sufijo utilizado con el parámetro `/DSDEREGDNS`.

/DOMGUID: este parámetro permite eliminar los registros DNS basados en los GUID.

/DSAGUID: este parámetro permite eliminar los registros DNS de tipo DSA basados en los GUID.

4. Borrado de las cachés del sistema de resolución DNS

Las diferentes herramientas que acabamos de ver nos permitirán identificar de forma muy rápida y resolver los problemas relativos a los registros de recursos necesarios para los controladores de dominio de un bosque Active Directory.

Observe que estas herramientas se ajustan a los mecanismos de resolución y métodos configurados.

Esto implica que debemos garantizar que:

- La caché del o los servidores DNS implicados no contiene registros antiguos obsoletos. Para esto, necesitaremos, por ejemplo, limpiar la caché de un servidor DNS particular usando el comando `DNSCmd nombre_del_servidor /clearcache`.
- La caché de la parte cliente DNS de un determinado equipo: esta operación equivale a purgar la caché del módulo DNSR - *Domain Name Resolver*, de cualquier registro en la caché de manera positiva o negativa. Para conseguirlo, necesitaremos, por ejemplo, usar el comando `IPConfig /flushdns`.
- Las zonas DNS a actualizar permiten la actualización dinámica de los registros.

Introducción a los componentes de la estructura lógica

La estructura lógica de Active Directory se compone de dominios y bosques que -permiten la representación lógica del espacio del directorio Active Directory.

Este espacio lógico (llamado también infraestructura lógica Active Directory), permite a los administradores abstraerse de la estructura técnica. En este último caso hablaremos de la infraestructura física de Active Directory. Esta separación entre el espacio lógico y el espacio físico permitirá una mejor organización de los elementos que componen la red en función de la naturaleza de los objetos y, porque no, en función de la organización de la empresa.

Este capítulo nos permitirá explorar la utilización de los dominios y los bosques para que los servicios de directorio Active Directory jueguen el rol del punto central en términos de la gestión de identidades y de consolidación de los objetos «importantes». De esta forma, todos los datos y los servicios ofrecidos grabados dentro de los servicios de dominio de Active Directory podrán ser localizados en cualquier punto de la red por los usuarios y a su vez por las aplicaciones empresariales.

Los dominios

El dominio es un componente fundamental de la estructura lógica de Active Directory. Por definición, se trata de un conjunto de objetos de tipo equipo, usuario y otras clases de objetos que comparten una base de datos de directorio común. Estos objetos interactúan con el dominio en función de sus respectivos roles tales como, por ejemplo, los controladores de dominio o simplemente los equipos miembros del citado dominio.

El dominio puede ponerse en marcha para implementar una zona de administración dentro de la empresa. De esta forma, podemos implementar una delegación eficaz de la administración o alcanzar un mejor control de los flujos de replicación.

En referencia a las infraestructuras Active Directory, podemos decir que el criterio de elección utilizado con menor frecuencia para la creación o no de un nuevo dominio concierne a la separación de los flujos de replicación entre varios dominios y pues un mejor control del tráfico dentro de un bosque.

A pesar de que una jerarquía de dominios puede en cierta medida obtener esto, las unidades organizativas (OU - *Organizational Units*) están en particular adaptadas para una estructura jerárquica sobre la cual será posible delegar todas o parte de las operaciones de administración a las personas habilitadas para asumir tal o cual tarea específica.

Aparte de estas consideraciones, el objeto dominio permite dividir el bosque Active Directory (entidad muy grande, Active Directory) en tantas particiones como dominios. De esta forma decimos que un dominio es una partición dentro de un bosque. Podemos por ejemplo imaginar que una empresa posee un bosque; estando este último compuesto por tres dominios. Y estos mantienen a los usuarios y equipos ubicados respectivamente en Canadá, los Estados Unidos y Europa.

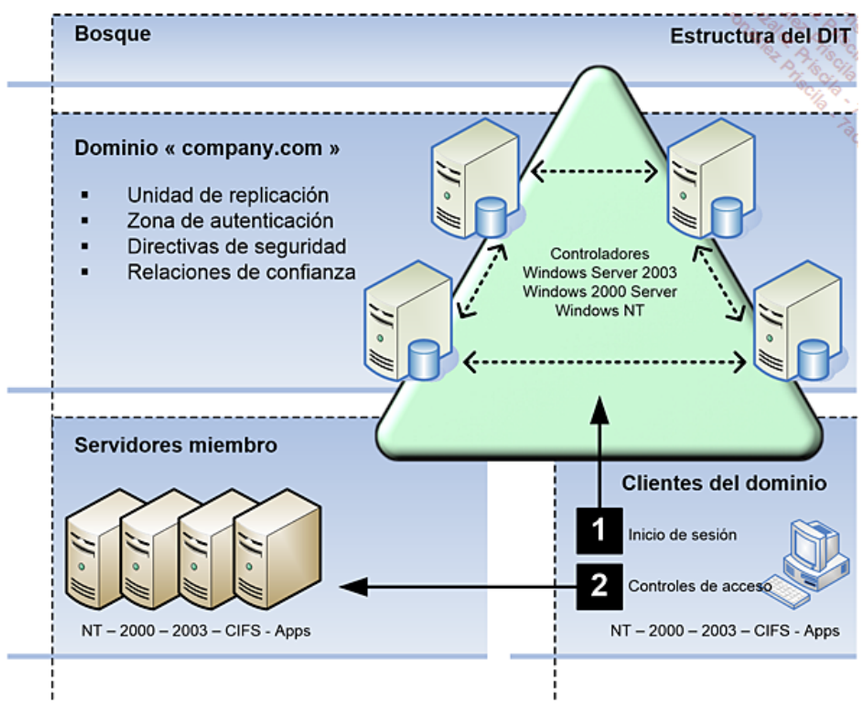
Tal arquitectura permite al bosque evolucionar con facilidad a medida que estos tres «grandes» dominios se vuelven más voluminosos.

El dominio Active Directory es pues un elemento que convendrá crear con prudencia y por consiguiente ser capaces de justificar la creación con referencia a los temas o funciones especificadas a continuación:

- Un dominio es un contenedor dentro de un bosque.
- Un dominio es una unidad de replicación.
- Un dominio es una unida sobre la cual se aplican las directivas de seguridad.
- Un dominio es una zona de autenticación y de autorización.
- Un dominio es miembro de un bosque, y como tal posee relaciones con los otros dominios del bosque.

Cada dominio posee su propia autonomía de administración y como tal los miembros del grupo **Admins del dominio** de un dominio dado no cuentan con ningún permiso en los otros dominios del bosque, a menos que por supuesto, se haya especificado de otra forma.

La figura siguiente muestra que el dominio es miembro de un bosque y que ofrece servicios de autenticación y de control de acceso a los clientes y servidores miembros del mismo.



Relaciones entre los miembros de un dominio Active Directory

El dominio puede contener cualquier equipo compatible con Active Directory y a su vez dominios Samba, que funcionen con un sistema operativo Microsoft o no Microsoft. Todas las versiones a partir de Windows XP hasta Windows 10 al igual que las versiones Unix/Linux estándar del mercado están soportadas.

Por ejemplo, cualquier dispositivo de tipo NAS (*Network Access Server*), que soporte el protocolo CIFS/SMB versión 2 o 3.x, o que emplee una versión de Samba en Linux o Apple OS X (con los módulos Samba) puede formar parte de un dominio Active Directory.

El dominio existe a través de cada uno de los controladores de dominio de dicho dominio. De esta forma, cada controlador de dominio posee su propia copia y versión de la base de datos del directorio. En el caso que un controlador no se encuentre disponible, los usuarios, equipos y servicios podrán continuar accediendo a Active Directory, solicitando otro controlador. Los controladores de dominio participan de manera activa en la disponibilidad del directorio y sus servicios, mediante los servicios de resolución DNS y el protocolo de autenticación Kerberos v5.

Por supuesto, el directorio Active Directory solo se instala en los equipos llamados **controladores de dominio** que funcionen con Windows Server desde Windows Server 2008 hasta Windows Server 2016. En la medida que el dominio esté compuesto de más de un solo controlador de dominio, las operaciones de creación y de modificación de los objetos y otros atributos de objetos serán replicados de manera uniforme en el conjunto de los controladores de dominio. Los mecanísmos de replicación, indispensables para la coherencia de la información ofrecida por el directorio son fundamentales para que los servicios de directorio Active Directory mismos funcionen de forma correcta.

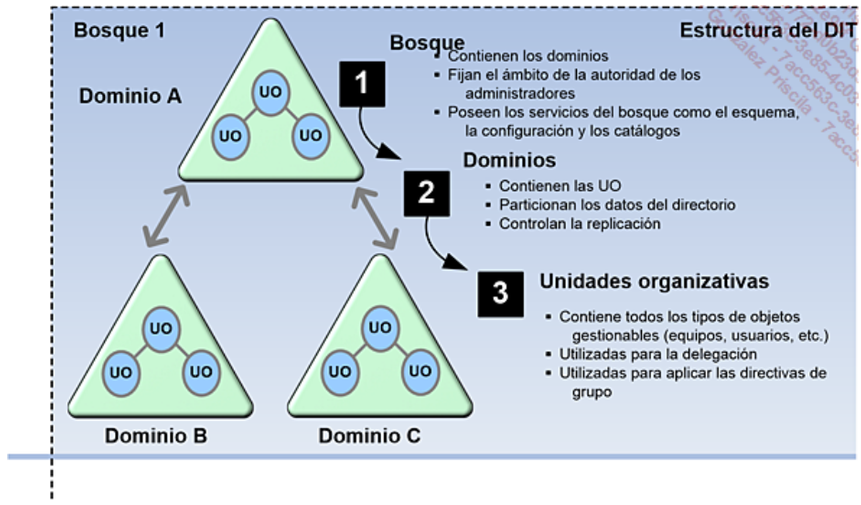
1. Contenedor (container) dentro de un bosque

El bosque juega el rol de contenedor para acoger a los dominios que juegan a su vez el rol de contenedores para múltiples clases de objetos. Dicho de otra forma, el bosque es el elemento o el marco que federa o unifica a varios dominios entre sí.

Esto significa que desde el punto de vista de las autenticaciones los objetos dominio se aprueban mutuamente. De esta forma, todo nuevo

dominio creado en el bosque generará de forma automática una relación de confianza bidireccional transitiva entre este nuevo dominio y el dominio situado en el nivel superior inmediato.

Las relaciones de confianza interdominio permiten a los dominios soportar las peticiones de autenticación de los dominios aprobados. Hemos visto antes que cada dominio dispone de una relación de confianza con su dominio padre. Como estas relaciones interdominio son por naturaleza transitivas y bidireccionales, está claro que los objetos contenidos en un dominio x del bosque pueden beneficiarse de la ACL (*Access Control List*) que contiene a los usuarios de cualquier dominio del bosque.



Bosque, dominios, UO y aprobaciones

Tomemos ahora un ejemplo acerca del almacenamiento propiamente dicho de los objetos del directorio. Las zonas DNS son también consideradas como objetos (objetos emitidos de la clase dnsZone) y hemos visto en los capítulos anteriores que de esta forma es posible y muy recomendable almacenarlos dentro de los servicios de dominio Active Directory. En función de las necesidades, algunas zonas podrán residir en un dominio particular mientras que otras se encontrarán a nivel de todo el bosque.

Este ejemplo muestra hasta que punto los objetos de dominio (clase domainDNS) y bosque utilizados en el entorno Active Directory pueden contener objetos diferentes y variados tales como objetos de unidades organizativas (UO - clase organizationalUnit), objetos usuario (clase user o inetOrgPerson) y muchos otros.

Bosque, RootDSE y punto de entrada: el soporte de protocolo LDAP versión 3.0 permite acceder a las propiedades de un objeto particular llamado RootDSE. El RootDSE se encuentra definido en la raíz del árbol del directorio almacenado en un servidor de directorio dado. De hecho, este punto de acceso no pertenece a ningún espacio de nombres (NC o dominio Windows) en concreto. Permite solo obtener información concerniente al servidor de directorio propiamente dicho y no debe ser confundido con un punto de entrada cualquiera del bosque.

Para más información acerca del objeto RootDSE, consulte la ayuda en línea de SDK Active Directory disponible en la siguiente dirección, o busque Active Directory SDK en el sitio Microsoft MSDN: https://msdn.microsoft.com/en-us/library/ms675874(v=vs.85).aspx

2. Niveles funcionales de los dominios

Un dominio Active Directory puede funcionar en diferentes modos o niveles funcionales. La noción de nivel funcional, específica de un dominio Active Directory, se define utilizando el atributo **domainFunctionality**.

Este atributo indica el nivel funcional de un dominio Active Directory:

"0" Dominio Windows 2000 en modo mixto.

"1" Dominio Windows 2000 en modo nativo.

"2" Dominio Windows Server 2003.

"3" Dominio Windows Server 2008.

"4" Dominio Windows Server 2008 R2.

"5" Dominio Windows Server 2012.

"6" Dominio Windows Server 2012 R2.

"7" Dominio Windows Server 2016.

El nivel funcional del dominio permite activar algunas funcionalidades específicas del dominio Active Directory. Como hemos podido ver, existen hoy en día siete niveles de funcionamiento diferentes.

Dominio Windows 2000 mixto: este modo de funcionamiento permite una interoperabilidad entre los controladores de dominio Windows Server 2003, Windows 2000 Server y/o Windows NT Server 4.0.

Observe: los controladores de dominio Windows NT y Windows Server 2008 o Windows Server 2008 R2 no son compatibles entre sí.

El modo Windows 2000 mixto fue concebido inicialmente para ayudar a la migración de entornos de dominio Windows NT a Windows 2000 Server y a su vez a Windows Server 2003.

Desde entonces, el tiempo ha pasado y la tecnología ha evolucionado, y salvo si el entorno de producción contiene todavía controladores de dominio secundario antiguos funcionando con Windows NT no existe ninguna razón para utilizar este modo, que debe considerarse obsoleto. Aparte, los controladores Windows Server 2008 no son compatibles con los controladores secundarios Windows NT 4.0. En otras palabras, si el dominio contiene controladores de dominio Windows NT y Windows 2000, es posible añadir controladores de dominio Windows Server 2003 o 2003 R2, pero no controladores de dominio Windows Server 2008 o Windows Server 2008 R2 y menos aún de versiones posteriores.

Dominio Windows 2000 nativo: este nivel funcional permite un soporte de los controladores de dominio Windows 2000, Windows Server 2003, Windows Server 2008 y Windows Server 2008 R2.

Dominio Windows Server 2003, versión preliminar (modo específico): este modo de funcionamiento permite una interoperabilidad limitada porque el dominio podrá contener solo controladores de dominio Windows Server 2003 y/o Windows NT Server 4.0.

Este modo de dominio fue previsto por Microsoft para ayudar a la migración de los dominios que contienen controladores Windows NT hasta

controladores Windows Server 2003, prohibiendo la instalación de controladores Windows 2000. El interés de este enfoque consistía en utilizar la replicación LVR (*Link Valued Replication*) de los entornos Windows Server 2003 para garantizar un soporte de los grupos de usuarios que tuvieran más de 5000 miembros. Este modo de funcionamiento soporta solo controladores Windows NT y Windows Server 2003. No es posible incluir en este modo controladores de dominio Windows 2000, Windows Server 2008 o Windows Server 2008 R2.

Dominio Windows Server 2003: este nivel funcional permite un soporte de los controladores de dominio Windows Server 2003, Windows Server 2008 y Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2.

En Windows 2000, los niveles funcionales de dominios se llaman "dominios en modo mixto" o "dominio en modo nativo".

Dominio Windows Server 2008: este nivel funcional permite un soporte de los controladores de dominio Windows Server 2008, Windows Server 2008 R2 y Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

Dominio Windows 2008 R2: este nivel funcional permite un soporte de los controladores de dominio Windows 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

Dominio Windows 2012: este nivel funcional permite un soporte de los controladores de dominio Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

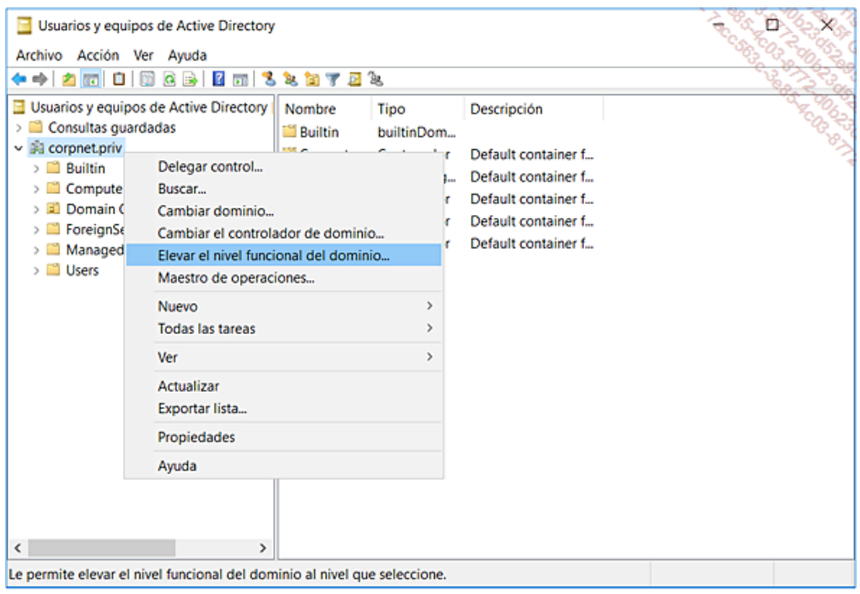
Dominio Windows 2012 R2: este nivel funcional permite un soporte de los controladores de dominio Windows Server 2012 R2 y Windows Server 2016.

Dominio Windows 2016: este nivel funcional permite un soporte de los controladores de dominio Windows Server 2016.

Elevación de los niveles funcionales de los dominios

Cuando un servidor Windows Server se instala como controlador de dominio, un conjunto de funcionalidades de Active Directory se activa por defecto. Antes de entrar en los detalles, podemos señalar que la mayor parte de las novedades introducidas por los servicios de directorio Active Directory están disponibles de forma independiente del nivel funcional del dominio. Sin embargo, además de las funcionalidades de Active Directory básicas, podemos en nuestro caso beneficiarnos de nuevas funcionalidades de Active Directory, aumentando el nivel de los antiguos controladores a Windows Server 2012 R2 o mejor a Windows Server 2016.

¡Por supuesto, el enfoque a adoptar es "despiadado" ya que para alcanzar un nivel determinado, será necesario que todos los controladores de dominio empleen una versión de Windows Server igual o superior al nivel funcional deseado!



Elevación del nivel funcional del dominio...

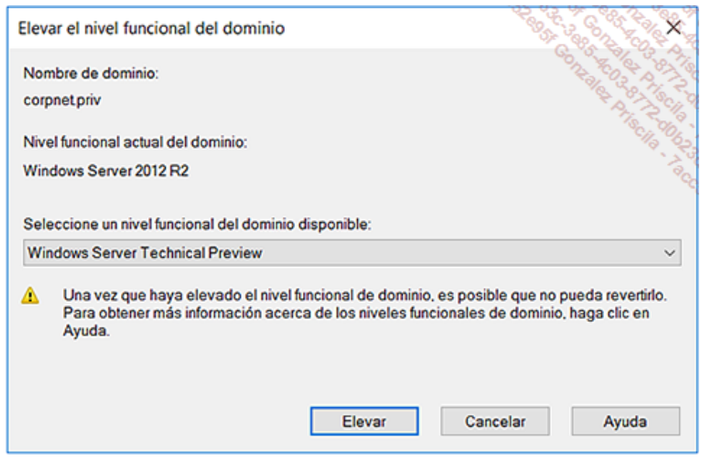
Cuando todos los controladores de dominio funcionan con la versión requerida de Windows Server, entonces podemos decidir -en función de nuestras necesidades- elevar el nivel funcional al nivel inmediatamente superior, o más si la tecnología lo permite.

Con respecto a la elevación del nivel funcional: observe que no se trata de un parámetro que se refiere a un controlador de dominio en particular, sino al dominio mismo en su totalidad. Es importante señalar que esta operación es irreversible y no podrá ser cancelada en modo alguno, a menos que se proceda a una restauración del directorio Active Directory, lo que en el caso de las grandes empresas es difícil de realizar.

El modo que caracteriza a un dominio solo tiene impacto en los controladores de dicho dominio. Los servidores miembro y los puestos de trabajo del dominio siguen funcionando, pero consideran que las nuevas características del dominio están disponibles. Esto significa que un dominio que funciona en el nivel funcional Windows Server 2016, Windows Server 2012 R2 o en un nivel aún inferior es también visto como un simple dominio NetBIOS LAN Manager por las equipos miembro del dominio Windows NT o una versión de SAMBA equivalente.

En nuestro ejemplo, para activar las nuevas funcionalidades disponibles en el nivel Windows Server 2003, en todo el dominio, todos los controladores de dominio del dominio deben ejecutar Windows Server 2003.

La pantalla siguiente muestra que el dominio corpnet.priv funciona de partida en el nivel funcional Windows Server 2012 R2.



Selección del nivel deseado cuando se cumplen las condiciones previas

Como todos los controladores de dominio son controladores Windows Server 2012 R2, la consola de gestión MMC **Usuarios y equipos de Active Directory** permite a los miembros del Grupo **Admins del dominio** o del grupo **Administradores de empresas** realizar la elevación del nivel funcional Windows Server 2012 R2 a Windows Server 2016.

Si dispone o tiene planeando contar con controladores de dominio que ejecuten Windows Server 2012 R2, no aumente el nivel funcional del dominio a Windows Server 2016.

Para más información sobre la elevación del nivel funcional de un dominio, busque en la ayuda en línea de Windows Server 2016 **Elevar el nivel funcional del dominio**.

3. Gestión de estrategias a nivel de los dominios

Como contenedor, un dominio puede contener muchos objetos y ofrecer sus servicios básicos (autenticación, catalogación y búsqueda de servicios globales) a los usuarios, equipos y aplicaciones de la empresa.

Como ocurría en el inicio de Windows NT, un dominio posee una directiva de seguridad, sabiendo que el dominio delimita el alcance de gestión. Así, algunos parámetros solo se aplican sobre un objeto de tipo dominio. Por ejemplo, la directiva de cuentas del dominio existe dentro del dominio, y se aplica de manera uniforme a todos los usuarios del dominio.

Observe que a partir del nivel funcional de dominio Windows Server 2008 y los niveles superiores, las directivas de cuenta granulares permiten una aplicación de los parámetros de cuenta de forma directa sobre los usuarios o grupos de usuarios.

Aunque no es el contenedor más pequeño dentro del directorio Active Directory (recuérdese que disponemos de una jerarquía de contenedores de tipo Bosque/Dominios/Unidades Organizativas), el dominio es cin frecuencia utilizado para aplicar directivas de seguridad globales. Este punto se justifica en principio para las organizaciones que son afectadas por ubicaciones geográficas diferentes o zonas de administración diferentes.

Como zona de seguridad especial, un dominio Active Directory permite aplicar las directivas de gestión de cuenta separadas dentro del mismo bosque. ¡Aunque es posible especificar directivas de cuenta sobre UO, observará que estas directivas no son operativas, si no es a nivel local, en el o los equipos afectados y no en el dominio! De hecho, este punto es por completo normal.

¡Observe! Veremos más adelante que los dominios que trabajan en el nivel funcional en Windows Server 2008 y versiones posteriores soportan ahora varias directivas de cuenta dentro del mismo dominio. Esta nueva funcionalidad, disponible solo en este modo, es posible gracias a los objetos PSO - *Password Settings Object*. En efecto, conviene recordar que un usuario no se autentica en una UO sino en un dominio. La entidad de dominio Windows utilizada y utilizable por el protocolo Kerberos versión 5 dentro de un reino Kerberos es mapeada sobre el dominio de Active Directory, mientras que las UO pertenecen al espacio LDAP y las convenciones de nombres X.500.

En el caso de que deseemos contar con parámetros distintos en función de ciertas regiones de la red o de departamentos que deban disponer de reglas específicas, y en la medida en que estos parámetros se refieren al dominio de Active Directory en su totalidad, podemos decidir establecer un nuevo dominio en el misma bosque o en un bosque diferente.

4. Delegación de la administración de los dominios y control de los parámetros específicos al dominio

Los servicios de seguridad integrados en el directorio Active Directory permiten a los administradores construir un plan de delegación de la administración. Al término de esta reflexión, será más fácil gestionar entornos con un gran número de objetos y disponer de varias entidades separadas.

El concepto de delegación permite a los propietarios de los objetos transferir todo o parte del control a otros usuarios o grupos de usuarios seleccionados de forma cuidadosa.

El principio de la delegación es muy importante, ya que permite distribuir la gestión de los objetos a terceros aprobados dentro de una entidad mayor. Recordemos que en Windows NT el único nivel de delegación era el dominio. Luego, el administrador del dominio podía apoyarse en los grupos por defecto, como los grupos **Administradores del dominio** o los diferentes grupos de tipo **operadores**. Hoy en día, el concepto de delegación de los servicios de directorio Active Directory permite trabajar en el bosque, los dominios, las unidades organizativas, los sitios, y en sentido amplio todos los objetos, pudiendo también descender hasta un atributo particular de un objeto entre millones.

Los puntos siguientes nos ayudarán a entender lo que caracteriza de manera muy especia un objeto de tipo dominio dentro de un bosque.

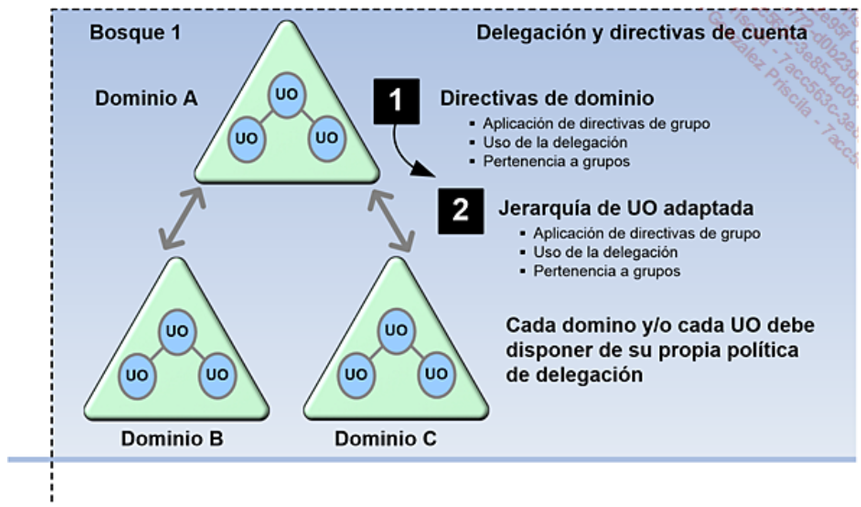
El dominio y las directivas de cuenta: por definición, las directivas de cuenta y las directivas de clave pública e inscripción automática se gestionan y aplican de forma amplia sobre el objeto dominio empleando una directiva de grupo (GPO - *Group Policy Object*).

El dominio y las directivas de contraseña: las directivas de contraseña nos permiten determinar cómo las contraseñas de dominio serán gestionados en términos de longitud, registro y duración de vida.

El dominio y las directivas de bloqueo de cuenta: las directivas de bloqueo de cuenta nos permiten determinar cómo se actúa ante los errores de inicio de sesión en el dominio por el uso de una mala contraseña. El objetivo es detectar posibles intentos de intrusión y así bloquear la cuenta del usuario afectado por un período determinado.

El dominio y las directivas de vales Kerberos: las directivas de gestión de los vales Kerberos permiten determinar la duración de vida de estructuras de seguridad importantes. Para un servidor o servicio determinado, un vale Kerberos se expedirá al solicitante una vez que éste

haya podido autenticarse ante el AS - *Authentication Service*. Este componente del sistema de seguridad es parte integral del servidor que actúa como **Centro de distribución de claves Kerberos**. Este servicio siempre se garantiza por una equipo de tipo "controlador de dominio de Active Directory".



Componentes de Active Directory y conceptos de delegación

La imagen anterior muestra una infraestructura compuesta por varios dominios. Cada uno de estos dominios tiene sus propios objetos y existe como zona de seguridad separada. Por lo tanto, cada dominio tiene una directiva de cuentas y de seguridad que habrá que adaptar en función de la política de seguridad global de la empresa, si existe.

Se recomienda definir con precisión los detalles de la directiva de gestión de cuentas de cada uno de los dominios de la empresa. De esta forma, podremos imponer una política uniforme de forma global capaz de fortalecer de manera eficaz el nivel de seguridad global de la red. ¡Quizás podemos recordar que una caja de seguridad no puede desempeñar plenamente su papel de espacio protegido si las claves de este mismo cofre carecen también de una gran protección!

Luego, cada dominio podrá en función de la política de gestión aplicar o no un plan de delegación. Este plan tendrá como objetivo principal definir quién asumirá la responsabilidad de controlar o modificar todo o parte del espacio Active Directory y los objetos que allí se almacenan. Descubriremos que los mecanismos de seguridad, de delegación y de aplicación de los objetos de directivas de grupo se aplican sobre los componentes principales de la infraestructura Active Directory, es decir, los sitios, los dominios y las unidades organizativas.

Creación de consolas MMC personalizadas

Para que la delegación de la administración sea completamente segura, podemos crear consolas MMC personalizadas que luego podremos distribuir a los usuarios o grupos de usuarios seleccionados para realizar las tareas de delegación. La consola MMC nos permite crear versiones limitadas de un componente de software particular. Por supuesto, este sería el caso del componente **Usuarios y equipos de Active Directory**, que es la herramienta que contiene más de funcionalidades de administración. De esta manera, los administradores pueden controlar las opciones ofrecidas a los responsables de una determinada tarea.

Utilización de estrategias de grupo para publicar o distribuir las consolas personalizadas

Podemos usar los objetos de directivas de grupo para distribuir las consolas de administración personalizadas a determinados usuarios o grupos de dos maneras.

Por publicación: este método permite publicar el elemento en cuestión en la lista de programas disponibles en la herramienta **Agregar o quitar programas**. Los usuarios autorizados pueden luego instalar la nueva consola. El usuario realiza la instalación cuando considere necesaria la aplicación.

Por asignación: a diferencia de la publicación, la asignación de una aplicación empleando una directiva de grupo automatiza la instalación de ésta para todas las cuentas especificadas. En este caso, la instalación se realiza de forma automática sin que el usuario esté implicado.

Para más información sobre los conceptos de delegación, busque **delegar el control** en la ayuda en línea de Windows Server 2016.

5. Utilización del dominio como unidad de replicación elemental

Sabemos que el objeto dominio es un elemento de la estructura lógica del directorio Active Directory. En efecto, cualquier dominio Active Directory existe en el bosque empleando un nombre DNS, y por lo tanto la estructura lógica del directorio será modificada de forma considerable.

Sin embargo, en algunos aspectos, debemos considerar el dominio como un elemento físico involucrado por igual en los mecanismos de replicación del directorio. En efecto, a partir MS OS/2 LAN Manager, con los dominios Windows NT y hoy en día con los directorios Active Directory, el dominio es siempre la unidad básica de replicación.

De hecho, el dominio es la unidad más pequeña de replicación controlable dentro del bosque. No se trata de una crítica o de una limitación técnica, sino simple de un hecho. Por definición, los objetos de un dominio se almacenan en éste y deberán ser replicados en los controladores de dominio del dominio.

Observe que el grupo **Controladores de dominio** tiene el permiso de **Replicar todos los cambios de directorio**. Podemos utilizar la consola de gestión MMC **Usuarios y equipos de Active Directory** para consultar la pestaña **Seguridad** de un objeto controlador de dominio.

Esta información puede parecer elemental, pero en realidad es de vital importancia en la comprensión de los elementos que componen el directorio Active Directory. Sin duda, un dominio existe a través de sus controladores, pero, antes de eso, el bosque con su papel de autoridad de más alto nivel existe gracias al primer controlador del primer dominio del bosque. En consecuencia, los controladores de cualquier dominio del bosque son, en cierto modo, en primer lugar los controladores pertenecientes a un bosque.

De hecho, la unidad de replicación más pequeña no es el propio dominio, sino las particiones del directorio de aplicaciones a través de la partición del dominio.

Cabe recordar que hemos visto estas particiones en el contexto del almacenamiento de las zonas DNS en Active Directory. Los miembros del grupo **Administradores de empresas** tienen la posibilidad de crear una partición cuyas réplicas pueden colocarse en los controladores de su elección. El hecho de que no consideremos las particiones del directorio de aplicaciones es porque esas particiones no pueden almacenar los SID, que son necesarios para la creación de objetos usuarios y equipos.

6. Límites del dominio de Active Directory y delegación limitada

Microsoft requiere que los dominios no sean "realmente" fronteras de seguridad a nivel de Active Directory. En efecto, una instancia Active Directory está representada por el bosque, que es en si representada por el dominio raíz del bosque, es decir, el primer dominio del bosque - siempre situado en lo más alto.

En la medida en que la entidad más alta es el bosque, Microsoft requiere que el dominio no proporcione un aislamiento total si existe en su propia partición y si tiene sus propios SID y sus propias cuentas integradas (administradores, operadores, etc.). En efecto, tras un ataque de un servicio malicioso que intente usurpar la identidad del administrador del dominio raíz sería en potencia posible obtener un acceso completo a cualquier dominio o a cualquier equipo de cualquier dominio del bosque.

Definir una política de seguridad en todo el sistema de información: esa problemática, incluso si existe realmente, debería desaparecer a lo largo del tiempo y así quitar dramatismo al riesgo. En efecto, el protocolo Kerberos versión 5 es un método de autenticación de red muy robusto y los sistemas también a su vez alcanzar niveles de robustez elevados contra las agresiones. Para ello es necesario definir las normas de uso, actualizar los parches de sistema y aplicación de forma regular, disponer de una estrategia de seguridad aprobada por todos y evaluada de forma periódica y por último disponer de soluciones de vigilancia y análisis como System Center Operations Manager o 5nine Cloud Security.

La transmisibilidad (o transmisión posible) de privilegios es un tema fundamental de la seguridad de los sistemas. Observe sin embargo que el bosque no toma ninguna iniciativa en términos de herencia o de transmisión de privilegios. Así, los privilegios de administración no son por completo transmitidos en la jerarquía de los dominios Active Directory o incluso entre los distintos dominios externos aprobados. Por lo tanto, para que un usuario de un dominio obtenga derechos o privilegios, incluso menores, en otro dominio será necesario que una autoridad facultada en dicho dominio lo apruebe.

Este concepto existe desde Windows NT hasta Windows Server 2016 con las relaciones de confianza interdominios. La relación de confianza propiamente dicha no es más que un tubo que permite crear la confianza de manera unidireccional entre dos contextos de seguridad diferentes: uno de los dominios es aprobado (*the trusted domain*) mientras que el otro es el aprobador (*the trusting domain*). Luego, queda a discreción del administrador del dominio aprobador permitir a los usuarios y grupos globales del dominio aprobado disponer de permisos sobre los objetos, e incluso de autorizaciones para disponer de algún privilegio.

Delegación de los objetos equipo Windows

Los equipos con Windows Server 2003 hasta Windows Server 2016, pueden aprovechar funcionalidades de seguridad mejoradas. Este tema pone de relieve el hecho de que el bosque, los dominios, los servidores y aplicaciones forman un todo que requiere de funcionalidades muy avanzadas para ofrecer una interoperabilidad mínima, una administración centralizada y un marco de delegación controlado.

La **delegación restringida** es una nueva opción que solo puede usarse en los servidores que funcionen al menos con Windows Server 2003. Mediante esta opción, el administrador puede especificar los nombres principales de los servicios (SPN, *Service Principal Names*) en los que esta cuenta podrá delegar. Procediendo de esta forma, el servicio puede ser aprobado para la delegación, sabiendo que esta confianza puede ser limitada a un grupo de servicios seleccionados. Esta operación de delegación controlada es por supuesto declarada de forma explícita por un administrador de dominio.

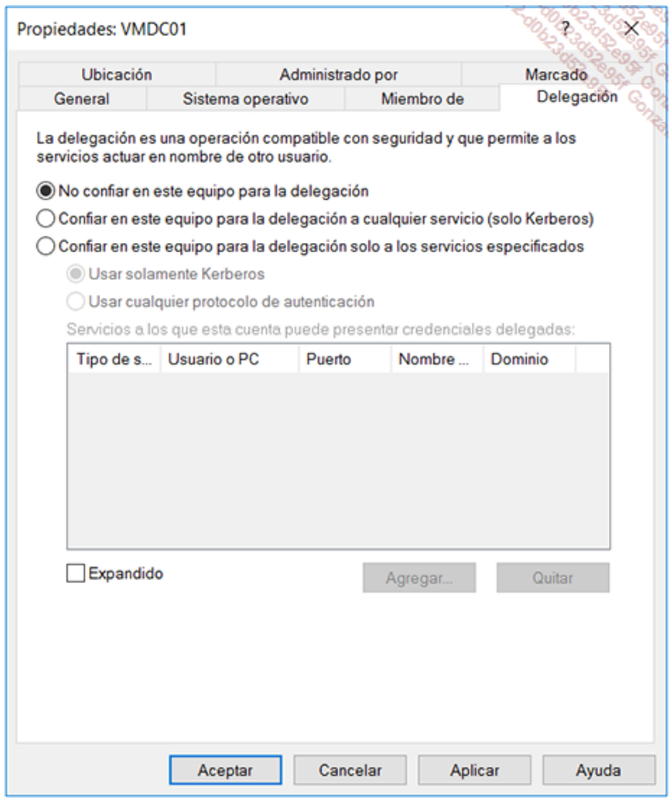
Para aprobar o no un equipo o un servicio específico para la delegación, podemos optar por una de las opciones que se presentan a continuación:

No confiar en este equipo para la delegación: esta opción es el parámetro por defecto. De esta manera, no es posible ninguna delegación de identidad para un proceso determinado.

Confiar en este equipo para la delegación a cualquier servicio (solo Kerberos): los impactos de seguridad relacionados con esta opción son desencadenados por el servicio y las acciones de todos sus administradores. Cuando se selecciona esta opción en un equipo, todos los servicios basados en el contexto de seguridad de la cuenta "sistema local" del equipo serán aprobados por la delegación. Por lo tanto, el equipo aprobado de forma global podrá acceder a cualquier recurso de red mediante el «préstamo» de una identidad, por ejemplo, un usuario. De hecho, los servicios del equipo actúan por cuenta del solicitante.

Confiar en este equipo para la delegación solo a los servicios especificados: esta característica se denomina **delegación restringida**. Permite alcanzar una mayor granularidad en la delegación ya que el equipo no será aprobado de forma global sino solo los servicios que elijamos.

De esta forma, mediante la delegación restringida, el administrador puede especificar los nombres principales de los servicios (SPN) en los que esta cuenta podrá delegar. Se trata, por supuesto de la opción más segura. La delegación para los servicios especificados permite a un administrador elegir los servicios de la red a quién delegar eligiendo un servicio específico o una cuenta de equipo. Permitiendo únicamente la delegación de servicios específicos, un administrador podrá controlar los recursos de red que pueden ser utilizados por el servicio o el equipo. La pantalla siguiente ilustra la activación de la delegación en un equipo determinado.



Propiedades de delegación

Para más información sobre la delegación restringida, consulte la ayuda en línea de Windows Server 2016.

Los dominios Active Directory son unidades de confianza

El objeto dominio es, como contenedor del directorio Active Directory, el elemento más pequeño utilizable en el marco de una relación de confianza. Por definición, todos los dominios del mismo bosque están vinculados por relaciones de confianza Kerberos versión 5. Las aprobaciones que unen a los dominios entre ellos dentro del bosque son, por definición, bidireccionales y transitorias y son mantenidas de forma automática por los controladores de dominio.

De esta manera, es posible en cualquier dominio del bosque autentificar cualquier usuario o cualquier equipo del bosque.

En base a los nombres DNS que rigen los dominios Active Directory y el espacio de nombres del bosque, el primer dominio, situado en lo más alto del espacio, desempeñará el papel de raíz del bosque y servirá de punto de paso obligado para soportar las autenticaciones entre los dominios situados en los demás árboles.

La estructura del bosque se detalla en la sección Los bosques de este capítulo.

Controladores de dominio y estructura lógica

Los controladores de dominio de un dominio Active Directory son, por definición, todos iguales entre sí. De esta forma, los objetos y los servicios que el dominio pone a disposición están disponibles a través de todos los controladores de dominio.

Así, los controladores de dominio Windows Server utilizan un modelo de replicación donde todos los controladores están disponibles en lectura y escritura. Este modelo, llamado **modelo de replicación de varios maestros** (*Multi Master Replication*), permite no tener que depender de un solo controlador en especial como ocurría antes en el entorno Windows NT con el controlador de dominio principal.

De esta forma, cualquier objeto de un dominio Active Directory puede ser creado en cualquier controlador de dominio de dicho dominio y cualquier propiedad de un objeto puede ser modificada en cualquier controlador de dominio que mantenga al objeto. El directorio Active Directory permite una disponibilidad total del directorio en cualquier punto de la red. En efecto, la idea es lograr que sea posible modificar el objeto más cerca de la administración o mejor, más cerca de los usuarios, equipos o aplicaciones que requieran un valor más actualizado posible.

Recordemos, en los antiguos dominios Windows NT o Samba, todas las modificaciones deben ser realizadas en el Controlador de Dominio Primario, este controlador es el único controlador de dominio que está disponible en lectura y escritura.

Los controladores de dominio también se hacen cargo de la replicación de los datos que se refieren al bosque o las particiones del directorio de aplicaciones utilizadas por el servicio DNS. Es así como un controlador de dominio replica las particiones que se especifican a continuación:

- La partición del dominio del controlador mismo;
- La partición de esquema del bosque de Active Directory;
- La partición de configuración del bosque de Active Directory;
- La o las particiones de los demás dominios del bosque cuando el controlador también desempeña el papel de catálogo global.

Sabemos que los controladores de dominio de Active Directory están todos disponibles en lectura y escritura. Observe sin embargo que esto no afecta en ningún caso a las particiones usadas por los servidores de catálogo global. En efecto, los datos contenidos en estas particiones solo son utilizables a fines de búsqueda y no en el marco de las modificaciones que un administrador de dicho dominio debe poder aportar. Por lo tanto, las particiones réplicas contenidas en los controladores de dominio que actúan como catálogos globales sólo están disponibles para lectura y no son modificables como en el dominio de origen. Estas particiones se llaman particiones de tipo PAS - para *Partial Attribute Set*, y representan un conjunto parcial de atributos.

La partición del directorio de aplicaciones que contiene la zona DNS integrada en Active Directory actual, así como la partición del directorio de aplicaciones que contiene la zona DNS integrada en Active Directory del dominio _msdcs.NombredeDominioDnsRaízdelBosque son dos espacios de almacenamiento críticos.

Estos últimos puntos muestran claramente que el controlador de dominio de un dominio deberá mantener actualizados los datos de su dominio, a su vez que los datos que no le conciernen directamente, sino que se refieren a aplicaciones o bien la estructura misma del bosque.

Así, a diferencia de las particiones de esquema y de configuración, las particiones del directorio de aplicaciones no son almacenadas en todos los controladores de dominio del bosque, si no sólo sobre los controladores seleccionados por un administrador como réplicas.

El hecho de particionar técnicamente el directorio Active Directory en varias particiones mantenidas por un Controlador de Dominio permite controlar mejor la replicación hacia uno u otro controlador o socio de replicación. De esta manera, el directorio Active Directory puede ser desplegado de forma global en entornos donde el ancho de banda disponible es limitado.

Para obtener más información sobre la replicación de Active Directory, busque **Funcionamiento de la replicación** en la ayuda en línea de Windows Server 2016 o visite el sitio Web de Microsoft y busque **Active Directory Topology Replication Technical Reference**.

Maestros de operaciones de dominio Active Directory

La replicación de varios maestros soportada por Active Directory es indispensable para que sea posible implementar infraestructuras de directorios capaces de soportar empresas con millones de objetos.

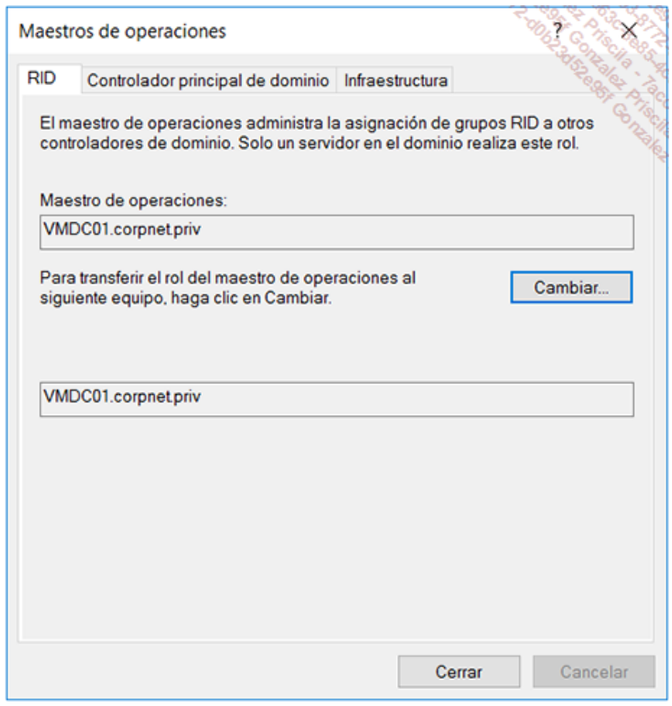
Sin embargo, algunas operaciones de cambio no pueden ser realizadas de esta manera y en la práctica, estas operaciones de carácter conflictivo o peligrosas serán dirigidas hacia un controlador particular llamado el **maestro de operaciones**.

Todo dominio Active Directory deberá disponer de las funciones siguientes:

- El maestro de ID relativos (RID, *Relative ID Master*).
- El maestro de emulador del controlador principal de dominio (*PDC Emulator*).
- El maestro de infraestructura (*Infraestructure Master*).

Estas funciones deben ser únicas dentro de cada dominio. En otras palabras, no puede existir un maestro RID, un maestro de emulador PDC y un maestro de infraestructura en cada dominio del bosque.

La imagen siguiente se obtiene al acceder a las propiedades del dominio Active Directory empleando la consola de gestión MMC **Usuarios y equipos de Active Directory**.



Maestros FSMO de dominio

Los maestros de operaciones desempeñan un papel importante en el marco de las operaciones de actualización en relación con algunas tareas de administración y de cambio de la configuración del directorio Active Directory.

El hecho de asignar algunas operaciones específicas a ciertos controladores de dominio protege a Active Directory contra ciertos tipos de conflictos y permite garantizar la disponibilidad operacional del directorio.

Las operaciones soportadas por los maestros de operaciones de dominios(en inglés FSMO, *Flexible Single Master Operations*) se resumen a continuación:

- El maestro de ID relativos (RID) gestiona el llenado del conjunto RID para cada controlador de dominio del dominio.
- El Maestro de emulador del controlador principal de dominio (PDC *Emulator*) garantiza el rol de PDC para asegurar la compatibilidad con los antiguos controladores de dominio Windows NT, la gestión de la autenticación cuando un usuario emplea una contraseña incorrecta y los mecanismos de sincronización horaria necesarios para las marcas de tiempo insertadas en los paquetes de autenticación Kerberos versión 5. Tenga en cuenta que este rol es obligatorio para soportar dentro de un dominio Active Directory clientes antiguos de tipo NetBIOS, aún cuando todos los controladores de dominio utilicen las últimas versiones como Windows Server 2016 o Windows Server 2012 R2.
- El maestro de infraestructura (*Infraestructura Master*) garantiza la actualización de las referencias relativas a los objetos situados en otros dominios.

Veremos que hay dos maestros de operaciones adicionales a nivel del bosque. Las operaciones soportadas por los maestros de operaciones a nivel del bosque se refieren a la protección de las operaciones que modifican el esquema, así como las operaciones de modificación del DIT (*Directory Information Tree*). Este último maestro de operaciones tendrá como principal objetivo comprobar el carácter único de las operaciones de adición y eliminación de los objetos de tipo dominio dentro del bosque.

Los maestros de operaciones garantizan también la interoperabilidad entre los controladores de dominio que utilizan versiones diferentes de Windows Server, así como muchos otros controles entre los dominios del mismo bosque.

Observe que los administradores del dominio y/o de la empresa en cualquier momento pueden gestionar el posicionamiento de las funciones FSMO a través de operaciones de transferencia o de imposición de roles para los cinco tipos de maestros de operaciones.

Las unidades organizativas (UO)

Las unidades organizativas (UO - *Organizational Unit*) son los objetos contenedores más comúnmente utilizados dentro de un dominio Active Directory. En efecto, aunque la estructura de dominios y bosques (DIT - *Directory Information Tree*) es rígida y compleja, las UO son fáciles de crear, editar, mover y borrar.

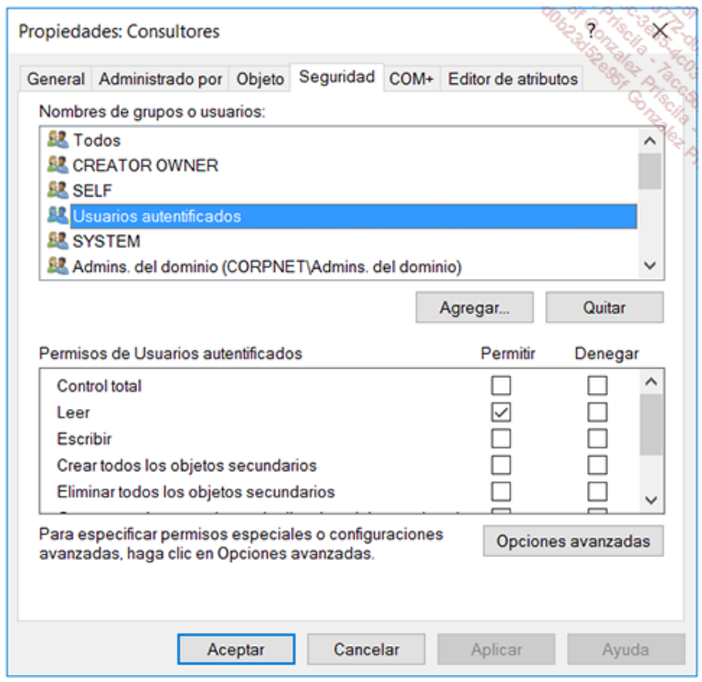
Este contenedor puede incluir muchos tipos de objetos tales como usuarios, contactos, equipos, impresoras, carpetas compartidas y por supuesto también otras unidades organizativas.

El hecho de que el contenedor de clase UO pueda ayudarnos a organizar el espacio de almacenamiento de objetos de un dominio particular del bosque es interesante en más de un sentido. En efecto, los siguientes puntos caracterizan el buen uso de las unidades organizativas:

- Desde un punto de vista del contenido, la unidad organizativa puede incluir a los objetos más usados (objetos usuarios, grupos, equipos, carpetas compartidas, impresoras).
- Desde un punto de vista de las funcionalidades de gestión de los cambios en la configuración, la unidad organizativa es el contenedor más pequeño que puede ser objeto de la aplicación de directivas de grupo.
- Desde un punto de vista de la implementación de privilegios de administración, la unidad organizativa puede ser objeto de múltiples delegaciones.
- Desde un punto de vista de la **modelización** de un espacio organizado, las unidades organizativas pueden ser combinadas de forma sencilla para reflejar su modelo de administración o de organización, de forma independiente del tamaño y el número de objetos contenidos.

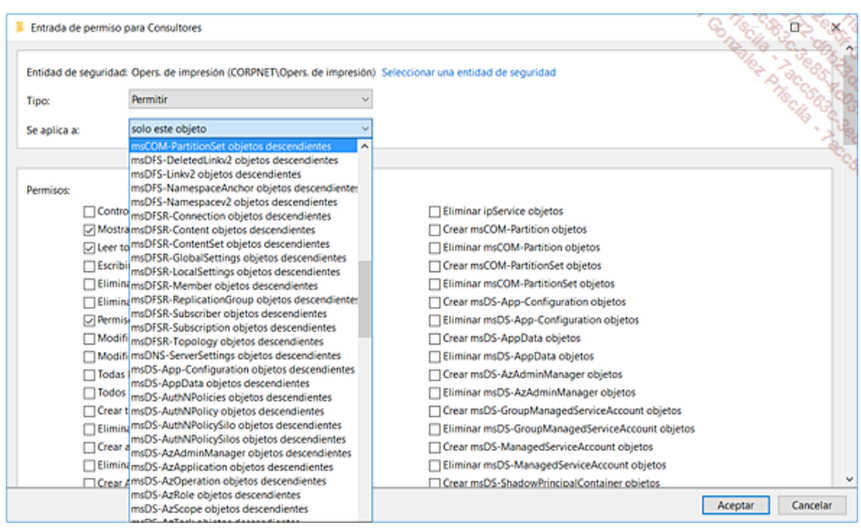
Podemos utilizar las UO de forma individual o en el marco de una jerarquía de UO anidadas. En este último caso, podemos decidir sacar partido de los poderosos mecanismos de herencia. De hecho, el comportamiento de una UO se parece mucho al de un directorio NTFS. La diferencia más notable se refiere a la naturaleza de los objetos soportados. Por supuesto, un directorio NTFS no puede contener archivos u otros directorios con las autorizaciones que conocemos, mientras que los objetos contenidos en una UO serán mucho más ricos en razón de su naturaleza compuesta por muchos atributos.

La pantalla siguiente muestra la posibilidad que tiene el administrador para jugar con los permisos de la Unidad Organizativa *Consultores*. Observe que esta ventana se parece mucho a una ventana de permisos NTFS.



Permisos de una unidad organizativa

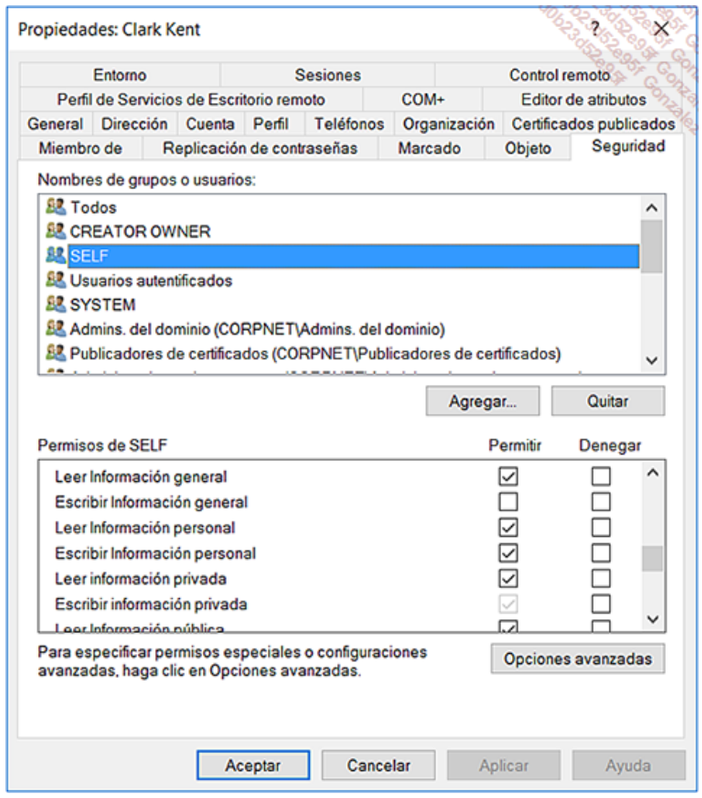
La ventana de selección de los permisos permite declarar los permisos más comunes y genéricos. Sin embargo, teniendo en cuenta la naturaleza tan diversa de los objetos que se pueden encontrar, el administrador utilizará con mayor frecuencia el botón **Opciones avanzadas**.



Asignación de permisos sobre las clases de objetos

Podemos consultar la ventana de selección del tipo de objeto sobre el cual aplicar los permisos en una UO.

Esta ventana nos puede hacer pensar que es posible gestionar dentro de una unidad organizativa los objetos instanciados a partir de todas las categorías declaradas en el esquema del directorio Active Directory. Observe que esta ventana de selección es una ventana genérica.



Asignación de permisos en las propiedades en función de la clase de objeto

La pantalla anterior muestra que los permisos sobre los tipos de objeto dependerán de la naturaleza de los objetos.

Modelización de una jerarquía de UO

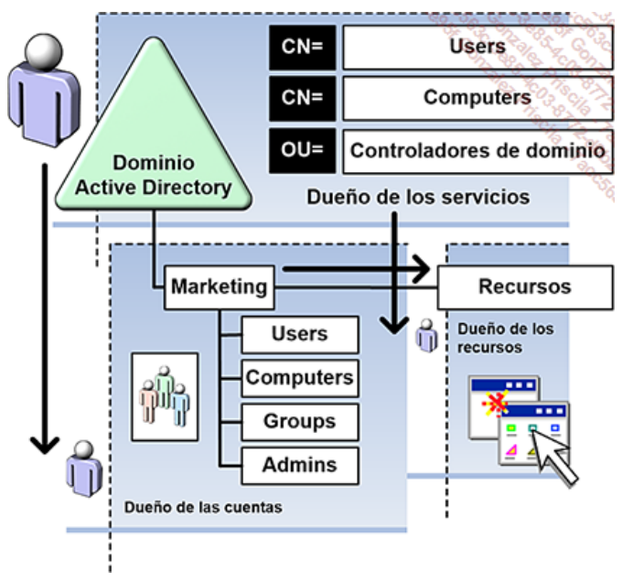
Con respecto a los entornos formados por varios dominios Active Directory, habrá que determinar si el modelo de jerarquía de UO definido es idéntico o, al contrario, si contiene características específicas para cada uno de los dominios. En términos absolutos, aunque algunos usuarios están afectados por la naturaleza de la estructura jerárquica de las UO en varios dominios, sería conveniente verificar que los dos o tres primeros niveles de UO sean comunes para todos los dominios afectados. De esta forma, los administradores de los distintos dominios se encontrarán con una jerarquía de UO normalizada.

En cualquier caso, recuerde que una jerarquía de UO en un dominio determinado no tiene ninguna relación con una jerarquía de UO definida en otro dominio.

El único punto común que puede existir entre las UO situadas en diferentes dominios o dentro del mismo dominio se refiere a su RDN respectivo (*Relative Distinguished Name*). En efecto, éste podría ser idéntico.

De esta forma, es posible tener varias UO con el mismo nombre. En nuestro ejemplo, otras UO con el RDN "UO=Consultores" pueden existir en el dominio o en otros dominios del bosque. Este tipo de operación es posible porque todos los objetos son únicos de forma global y referenciados de forma única empleando un atributo y un valor de tipo GUID (*Globally Universal Identifier Descriptor*).

La imagen siguiente ilustra una primera aproximación de una estructura de UO. En términos absolutos, la definición de la estructura está en relación directa con las operaciones de administración de los elementos contenidos en las UO así como con la posibilidad de hacer uso o no de los servicios de delegación, en función de la directiva de la empresa.



Delegación y propietarios de las unidades organizativas

Al principio, el administrador tiene la facultad de delegar en algunas UO o jerarquías UO, todas o parte de las operaciones de administración a simples usuarios del dominio o de cualquier dominio aprobado. Siguiendo las buenas prácticas, se puede definir tres tipos de administradores:

Los propietarios de los servicios: se trata de las cuentas de administración habituales que tienen por definición todos los permisos, incluido el de apropiarse de los objetos que no les pertenecen.

Los propietarios de cuentas: se trata de cuentas que son objeto de una o varias delegaciones. Estas cuentas pueden gestionar todas o parte de las cuentas de un departamento o de una unidad particular de la empresa En función de las delegaciones a realizar, puede ser necesario tener varios propietarios de las cuentas cuyas autorizaciones se adaptarán en función de las necesidades.

Los propietarios de recursos: se trata de cuentas que son objeto de una o varias delegaciones. Estas cuentas pueden gestionar todos o parte de los recursos de un departamento o de una unidad particular de la empresa En función de las delegaciones a realizar, puede ser

necesario contar con varios propietarios de los recursos cuyos permisos se adaptarán en función de las necesidades.

En este ejemplo, las cuentas de recursos serán objeto de delegación de la gestión de determinados recursos por parte de los propietarios de los servicios y/o por parte de los propietarios de las cuentas. La directiva de delegación deberá determinar y luego formalizar el plan más adecuado a las prácticas y la política de la empresa.

Si las tecnologías y métodos propuestos son utilizadas, entonces los equipos informáticos se concentrarán en su cometido real, es decir, los servicios de infraestructura y la gestión de la información en el sentido estratégico del término. En el marco del **Plan de delegación**, cada departamento de la empresa se encargará de gestionar sus propios objetos dentro de su propia zona de autoridad.

Para saber más sobre la aplicación de una arquitectura de unidades organizativas, consulte los artículos y documentos de referencia de Microsoft de la serie Active Directory Collection disponibles en el sitio web de Microsoft.

Unidades organizativas y unicidad de las cuentas de usuarios

Cuando creamos una cuenta de usuario, Active Directory genera un SIA (*Security Identifier Descriptor*) y un GUID. Este último se utiliza para identificar la entidad de seguridad. Active Directory crea también un nombre LDAP (RDN - *Relative Distinguished Name*) único relativo basado en el nombre de la entidad de seguridad. Este nombre único LDAP, y también el nombre canónico Active Directory, se forman en función del nombre único relativo LDAP los nombres de los contextos del dominio y de los contenedores donde se crea el objeto entidad de Seguridad.

Si la empresa está compuesta por varios dominios, podemos usar el mismo nombre de usuario (o nombre de equipo) en diferentes dominios. El ID de seguridad, el identificador universal único (GUID), el nombre único LDAP y el nombre canónico generados por Active Directory se determinarán de manera única para cada usuario, equipo o grupo dentro del bosque.

Si el objeto entidad de seguridad es renombrado o desplazado hacia otro dominio, el ID de seguridad, el nombre único relativo LDAP, el nombre único LDAP y el nombre canónico serán modificados de forma automática. Por contra, ya que se trata del mismo objeto, el identificador único universal generado por Active Directory se mantendrá invariable.

Si intentamos crear una segunda cuenta de usuario con el mismo nombre de visualización en la misma UO, entonces obtendremos un mensaje de error indicando que el nombre ya existe.

Para poder disponer de dos objetos usuario con el mismo "nombre completo" en el mismo dominio, necesitará asegurarse de que sean almacenados en unidades organizativas diferentes.

Una unidad organizativa no puede contener objetos procedentes de su propio dominio, sea cual fuere el tipo de objetos. No es posible insertar en una UO del dominio A los objetos procedentes del dominio B.

Los árboles

Un árbol de dominio(s) es un conjunto de dominios agrupado para formar una estructura jerárquica. Por definición, al añadir un dominio dentro de bosque, pueden ocurrir dos supuestos:

- El dominio se inserta como nuevo dominio hijo en un árbol de dominio existente.
- El dominio crea un nuevo árbol en un bosque existente.

Con respecto al primer dominio del bosque: la elección para crear un nuevo dominio en un nuevo bosque corresponde a la creación inicial del bosque. Este dominio en particular se denomina **dominio raíz del bosque** y también desempeña el papel de dominio raíz de la primera estructura de árbol. La importancia del rol del dominio raíz del bosque se aborda más adelante.

A partir del momento en que se añade un nuevo dominio en un árbol existente, se convierte en un dominio hijo del dominio raíz del árbol. El dominio raíz del árbol es, en este caso, el dominio padre.

Sin embargo, un dominio hijo puede también tener uno o varios dominios hijos. Esta estructura compuesta de múltiples dominios formará una jerarquía de dominios donde la base del nombre será el dominio raíz del árbol. Así, el nombre de un dominio hijo en un árbol es solo su nombre DNS. Este nombre es una combinación del nombre de cada uno de los dominios hasta el dominio raíz del árbol, tal como, por ejemplo, el dominio de Active Directory responsable de la zona EMEA (*Europe, Middle East and Africa*) cuyo nombre DNS sería, por ejemplo, emea.corpnet.corporate.net.

Por definición, un árbol Active Directory es un espacio de nombres DNS contiguo, por lo tanto, cualquier nuevo espacio de nombres DNS deberá ser objeto de la creación de un nuevo árbol dentro del bosque Active Directory.

Aunque el dominio sea la unidad de administración, seguridad y replicación básicas, es probable que en función del modelo de administración o de organización de la empresa, sea necesario crear uno o varios dominios adicionales. Por ejemplo, podríamos necesitar agregar dominios dentro de un bosque existente en los casos presentados a continuación:

- Permitir la implementación de un modelo de administración descentralizado.
- Utilizar directivas y parámetros de seguridad diferentes para cada uno de los dominios.
- Aumentar el rendimiento de los replicaciones mediante un mejor control y una utilización mínima de la red.
- Suprimir algunas limitaciones técnicas como el número de objetos soportados o el número de controladores de dominio por dominio.

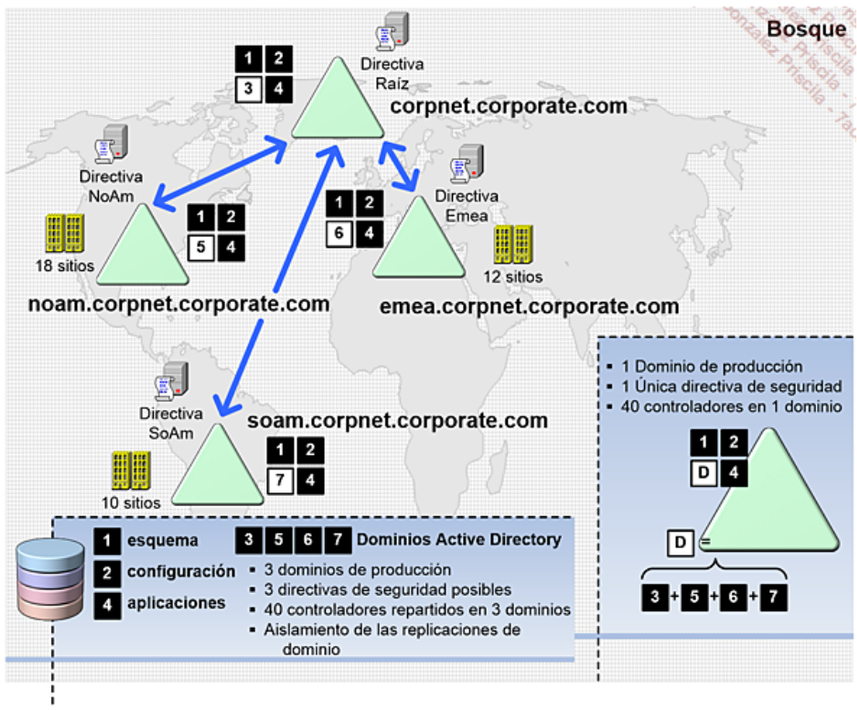
La creación de un árbol puede justificarse cuando una empresa tiene varias oficinas en diferentes países. Si la red de la empresa está compuesta por un único dominio, entonces será necesario disponer como mínimo de un controlador de dominio por sitio para poder garantizar los servicios globales.

Se tratará en concreto de los servicios que soporta la autenticación de usuarios y quizá también la gestión y la configuración de equipos empleando la tecnología IntelliMirror y directivas de grupo.

Microsoft IntelliMirror agrupa un conjunto de tecnologías que permiten combinar las ventajas de una informática centralizada con el rendimiento y la flexibilidad de una informática distribuida. Esta tecnología garantiza la disponibilidad de datos y parámetros personales de los usuarios, la disponibilidad de software así como su persistencia cuando los usuarios abren una sesión en un dominio Active Directory, desde cualquier equipo del dominio o incluso desde un dominio aprobado.

Supongamos una empresa compuesta por un único dominio Active Directory que soporta diez sitios geográficos repartidos en cinco países. Unos meses más tarde, la empresa está en plena expansión y se compone de cuarenta sitios en ocho países.

Esta significativa evolución de la topología física de la empresa puede requerir una evolución del modelo original compuesto por un único dominio hacia una arquitectura de dominios múltiples. La siguiente imagen muestra esta evolución.



Evolución del DIT (Directory Information Tree)

Una evolución como esta debe estar justificada a nivel técnico y financiero. Es posible que se desee un cierto nivel de autonomía o bien que los flujos de replicación requieran un cierto nivel de aislamiento. En efecto, el hecho de dividir la red en varios trozos podría permitir al equipo informático disponer de un dominio Active Directory por país en lugar de un único dominio.

Aunque la solución perfecta, en términos de simplicidad de aplicación, mantenimiento y evolución, sería disponer de un bosque compuesto por un dominio que incluya a su vez un solo controlador, no hay que temer en exceso a las infraestructuras compuestas por múltiples dominios. El hecho de poseer varias dominios no significa en modo alguno que la administración sea más pesada o compleja.

En efecto, los dominios de un bosque comparten lo esencial, es decir, el esquema, la configuración, los catálogos globales, así como los espacios de nombres DNS ofrecidos por los diferentes árboles del bosque Active Directory. Por último, los puntos más importantes que

caracterizan a un árbol de dominios se indican a continuación:

- Un árbol es un nuevo espacio de nombres distinto de todos los demás. Por ejemplo, podemos crear un nuevo espacio de nombres DNS (*partners.net o partners.corporate.com*, etc.) y un nuevo dominio Active Directory para incluir a los socios aprobados dentro de su bosque Active Directory *corpnet.corporate.com*. Este tipo de configuración requiere una nueva estructura de árbol, ya que el espacio de nombres inicial *corpnet.corporate.com* se ve fragmentado.
- Los nombres creados por debajo de un dominio raíz de árbol son siempre contiguos o constituyen un espacio continuo.
- Los nombres DNS utilizados pueden reflejar una entidad en particular, la organización de la empresa de forma geográfica, de manera orgánica o una mezcla de ambos.

La aplicación de una nueva estructura de árbol de dominio permite a la empresa disponer de varios espacios de nombres. Este punto es en especial importante cuando una empresa es adquirida y su nombre debe ser preservado. ¡A pesar de todo intento el hecho de que la creación de un nuevo árbol vacío no permite la integración natural de un bosque A con un bosque B. Para poder recuperar los objetos del bosque B en el bosque A, deberemos realizar una operación de export/import o mejor, de clonación de objetos. El objetivo de la operación será un dominio existente o un nuevo dominio dentro del bosque, y como dominio fuente, el dominio que contiene los objetos a recuperar.

Esta operación de recuperación consiste en clonar los objetos empleando la herramienta Microsoft Active Directory Migration Tool - **ADMT**. En este caso, los nuevos objetos de seguridad creados dentro del directorio de destino utilizarán el atributo **sIDHistory**, usado para recuperar el SID original.

El principio del atributo sIDHistory se presenta más adelante en esta sección.

Herramienta de migración de Active Directory ADMT Versión 3.x

La herramienta de migración de Active Directory (ADMT, *Active Directory Migration Tool*) puede ayudarnos a migrar las cuentas de usuario, grupos, así como las cuentas de equipo de dominios antiguos a dominios Active Directory, y también reestructurar los dominios Active Directory existentes dentro de un mismo bosque o en bosques diferentes.

ADMT Versión 3.x aporta las siguientes mejoras: la ejecución simultánea de varias operaciones ADMT, el soporte de Microsoft SQL Server para el almacenamiento de datos de migración, la posibilidad de modificar de forma directa los nombres de cuentas, los nombres relativos (RDN), los nombres de cuentas SAM y nombres principales universales (UPN). Estas opciones están disponibles a través de la página Opción de selección de los objetos del Asistente de Migración de cuentas de usuarios, de equipos y cuentas de grupo. ADMT Versión 3.x también mejora el servidor de exportación de contraseñas (PES, *Password Exportation Service*) que se ejecuta ahora como servicio. De esta manera, es posible iniciarlo a través de la información de autenticación de un usuario autenticado en un dominio de migración objetivo. Por último, el conjunto de registros se almacena ahora en la base de datos SQL de ADMT para una consulta posterior. Para descargar ADMT Versión 3, busque **Active Directory Migration Tool** en el sitio de Microsoft.

Para más información, consulte **Diseño y despliegue de servicios de directorio y los servicios de seguridad** en el sitio Web de Microsoft.

Para maximizar el nivel de seguridad de las operaciones de recuperación de contraseñas, Microsoft recomienda que el servidor exportador de las contraseñas del dominio fuente sea un controlador de dominio "dedicado" a esta tarea y colocado en un lugar cuyo acceso físico y de redes sea seguro.

ADMT Versión 3.2 aporta las siguientes mejoras:

- Instalación en Windows Server 2008 R2 hasta Windows Server 2012 R2.
- El soporte de controladores de dominio Windows Server 2008 R2 hasta Windows Server 2012 R2 se ha añadido y los controladores de dominio Windows Server 2016 son soportados de forma normal.
- El nivel funcional mínimo del dominio fuente debe ser Windows Server 2003.
- El nivel mínimo del dominio objetivo debe ser Windows Server 2003.
- La migración de las "Cuentas de servicios gestionados" disponibles a partir de los sistemas operativos Windows 7 / Windows Server 2008 R2 hasta Windows 10 / Windows Server 2016.
- El soporte de cuentas de usuarios que utilizan los nuevos mecanismos AMA - *Authentication Mechanism Assurance*.

La herramienta ADMT es la empleada con mayor frecuencia para "clonar" los objetos de seguridad entre las dominios de origen y destino situados en bosques diferentes. Este tipo de utilización está vinculado de forma directa a las fusiones / adquisiciones de compañías. Observe que sin embargo puede ser empleado a su vez para la reorganización de un bosque para desplazar, y no para clonar, los objetos entre los dominios Active Directory de un mismo bosque.

Con respecto al sIDHistory - datos históricos del SID

Un objeto de seguridad "clonado" es una cuenta situada en un dominio Active Directory que funciona en modo nativo Windows 2000 o posterior para el que las propiedades de origen se copian a partir de la cuenta fuente. Aunque se trate de un nuevo objeto en el dominio Active Directory destino, y que por lo tanto tiene por necesidad un nuevo SID, el antiguo SID de la cuenta fuente será copiado en el atributo Active Directory sIDHistory del nuevo objeto, cuando la opción de migración del SID se active. El hecho de repatriar al ex SID es una gran facilidad que permite al objeto clonado poder seguir teniendo acceso a todos los recursos de red para los que la cuenta fuente tenía permisos.

Técnicamente, el acceso a los recursos de la Red está protegidos a través del sIDHistory porque el inicio de sesión crea una token de acceso - *Access Token* - que incluirá el SID principal del usuario y también su sIDHistory y sIDHistory de los grupos a los que pertenecía en el antiguo dominio fuente.

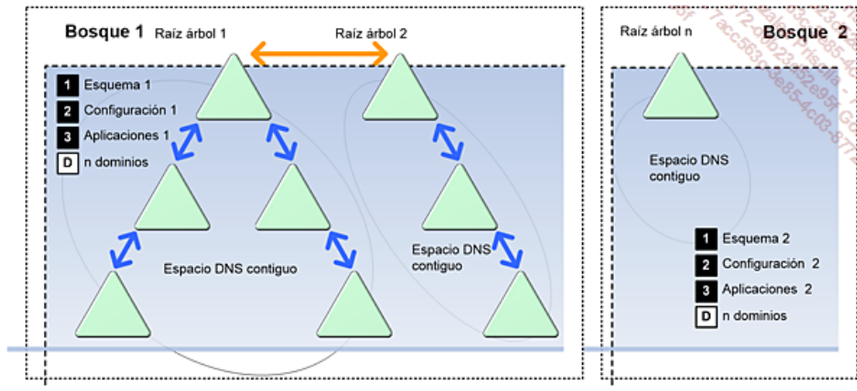
Ubicación de la nueva estructura de árbol

Estas pocas líneas nos permitirán entender que un nuevo árbol en un bosque existente permite la disponibilidad de un nuevo espacio de nombres DNS distinto y un nuevo dominio Active Directory virgen. Cabe señalar que el DIT de un bosque Active Directory es rígido y que no es posible "conectar" un árbol de un bosque X como un nuevo árbol del otro bosque.

Este punto nos permite ahora considerar la implementación de una nueva estructura de árbol de dominios en el bosque o quizás en un bosque diferente. En efecto, es muy importante plantearse esta cuestión para hacer la mejor elección en términos de evolución futura a corto o mediano plazo.

Antes de crear un nuevo árbol para implementar un nuevo espacio de nombres dentro del bosque, sería conveniente evaluar la posibilidad de crear un nuevo árbol en un nuevo bosque. Esta opción permitiría a la empresa a disfrutar de una autonomía total de la entidad de administración, de un esquema y una configuración diferente, así como de una separación total entre las infraestructuras técnicas. De esta forma, una separación o cesión de la actividad de una filial de la empresa puede ser posible.

La imagen siguiente ilustra estos diferentes enfoques.

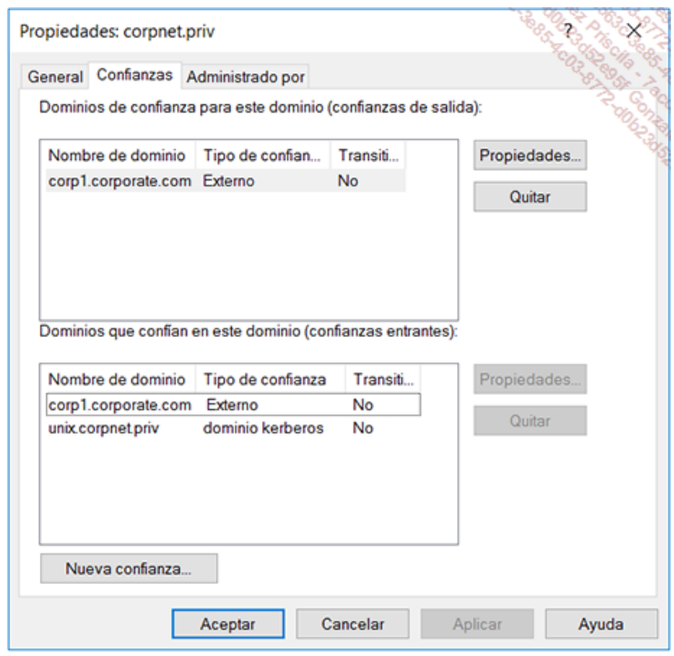


Árboles en el mismo bosque y en bosques separados

Una empresa implementa una infraestructura compuesta de **tres árboles**. Los dos primeros árboles son implementados en el **primer bosque**permitiendo a la empresa utilizar dos espacios de nombres diferentes en el mismo espacio de seguridad y la misma infraestructura técnica Active Directory. El tercer árbol es, esta vez, implementado en un **bosque diferente**. Este enfoque es una muy buena opción cuando debemos considerar una zona de seguridad separada o la posibilidad de una cesión de esta entidad de la empresa. La sección dedicada al rol del bosque presenta los conceptos de los bosques y la noción de confianza de bosques.

Las operaciones de construcción de los árboles se efectúan mediante el Asistente de instalación de Active Directory integrado en el Administrador del servidor de Windows Server 2016. Este asistente soportará la creación del nuevo dominio, así como la creación de una nueva relación de confianza Kerberos versión 5 bidireccional transitiva entre el dominio raíz del nuevo árbol y el dominio raíz del bosque. Del mismo modo, los otros árboles de dominios del bosque serán "conectados" empleando el mismo tipo de confianza en el dominio raíz del bosque.

En el ejemplo siguiente, la figura ilustra el hecho de que los dominios *corpnet.priv* y *corp1.corporate.com* poseen confianzas bidireccionales no transitorias cuyo tipo es **Externo**. El dominio unix.*corpnet.priv* se declara como dominio de confianza no transitivo con el modo dominio Kerberos (MIT).



Gestión de confianzas: dominios aprobados y dominios aprobadores

Disponibilidad del dominio raíz del bosque

Como ya se señaló antes, estas operaciones complejas se realizan de forma automática por el Asistente Configuración de servicios de dominio de Active Directory. Sin embargo, Microsoft sugiere que se haga todo lo posible para garantizar la disponibilidad del dominio raíz del bosque cara a cara con los dominios raíz de las estructuras de árbol.

En efecto, se considerarán dos aspectos fundamentales:

1. Las confianzas son transitivas: la transitividad de las relaciones de confianza Kerberos v5 requiere ponerse en contacto con el dominio raíz del bosque. Por lo tanto, habrá que asegurarse de que es posible ponerse en contacto con al menos un controlador de dominio de este dominio.

2. Los paquetes de autenticación Kerberos cuentan con marcadores de tiempo: sabemos que el protocolo Kerberos V5 es robusto. Las funcionalidades para evitar reposiciones integradas en el protocolo Kerberos requieren la marca de tiempo de los paquetes de autenticación. Por esta razón, el sistema de sincronización horario debe estar configurado de manera correcta y funcionar a nivel del bosque. La referencia global se define en el nivel de dominio raíz del bosque y luego se envía a los demás dominios del bosque a través de los diferentes árboles.

El sistema de sincronización horaria será implementado en los controladores de dominio con el rol de maestro de operaciones **PDC Emulator**. Estos equipos son en particular importantes para el buen funcionamiento del Protocolo de autenticación Kerberos v5, aparte de otras funciones que pueden desempeñar dentro del bosque.

El controlador mencionado dispone de los roles de maestro de operaciones FSMO PDC Emulator, catálogo global, controlador de dominio Active Directory, centro de distribución de claves Kerberos y servidor de tiempo Windows a través del servicio **Hora de Windows** o **W32Time**.

Con respecto a los nombres de dominios secundarios

Una vez el o los dominios raíz de árbol están creados, en función del nombre de la empresa o de una división específica, habrá que definir la política de nombres de los dominios secundarios dentro de un árbol de dominio dado.

Las modificaciones a aplicar a nivel de la infraestructura de dominios de un bosque Active Directory son sinónimo de complejidad, riesgos potenciales de indisponibilidad y en muchos casos de carencia de posibilidades. Desde los primeros modelos de arquitectura implementados en empresas de gran tamaño con el soporte de Microsoft, el editor siempre ha advertido de estas limitaciones, que sigue estando presentes, incluso 15 años después del éxito de los servicios de directorio de Windows 2000.

Los dominios secundarios de un dominio raíz de una estructura árbol pueden con facilidad representar entidades conocidas por los usuarios, por lo tanto aprobadas de forma global. Este podría ser el caso de los tipos de entidades siguientes:

- Regiones geográficas, países, sitios departamentales;
- Entidades administrativas, departamentos de la empresa;
- Entidades específicas de una actividad particular.

Una buena práctica que nos permitirá disfrutar de forma plena de nuestra arquitectura de dominios Active Directory, en relación con el sistema de nombres de los nombres de dominios secundarios de un dominio raíz de árbol, consiste en basarse en ubicaciones geográficas.

La definición de un espacio de nombres para el directorio Active Directory debe considerar la probabilidad de una reorganización inesperada con un impacto sobre la o las jerarquías de dominios con la mayor limitación posible. Por ejemplo, una buena práctica consiste en utilizar un sistema de nombres basado en la ubicación geográfica de los sitios. ¡Esto permite evitar con bastante facilidad este tipo de problema ya que el sitio llamado Madrid siempre estará en Madrid!

Creación de un árbol y controles realizados por DCPromo

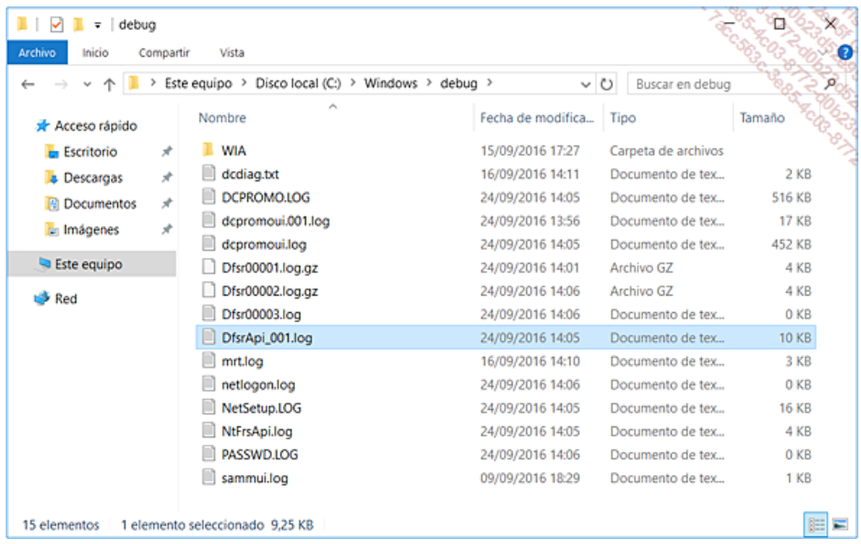
Cuando se implementa un nuevo dominio para crear un árbol de dominio, el asistente de instalación del directorio Active Directory realiza una serie de operaciones de control.

- Verificación del nombre DNS declarado. El nombre declarado debe crear una ruptura del espacio DNS existente en el bosque y el nombre NetBIOS del dominio debe ser único.
- Búsqueda de un controlador de dominio operativo para el dominio raíz del bosque.
- Replicación de las particiones de esquema y de configuración.
- Creación de la nueva partición necesaria para el nuevo dominio y los nuevos objetos por defecto de ésta.
- Generación del SID del nuevo dominio y de la directiva de seguridad asociada.
- Creación de un objeto TDO (*Trusted Domain Object*) en el dominio raíz para el nuevo dominio de la nueva estructura de árbol.
- Creación de un objeto TDO (*Trusted Domain Object*) en el dominio del nuevo árbol para el dominio raíz del bosque.
- Creación de una relación de confianza bidireccional entre los dos dominios.
- Creación de la directiva por defecto del dominio.
- Aplicación de los parámetros de seguridad en el equipo controlador de dominio (archivos, servicios y registro).

Aunque la interfaz gráfica y la literatura técnica nos explican que las confianzas creadas por el Asistente de Configuración de servicios de dominio de Active Directory son relaciones bidireccionales, tenga en cuenta que en realidad, se trata técnicamente de dos relaciones unidireccionales.

Para más detalles acerca de las operaciones realizadas por el Asistente de Configuración de servicios de dominio de Active Directory, consulte los registros de instalación del directorio Active Directory en la carpeta %Systemroot%\debug. Los archivos **DCPromo.log** y **DCpromoUI.log** llevarán un registro de todas las operaciones del proceso de instalación del directorio Active Directory en el equipo. Podremos consultar también los archivos DfsrApi_001.log y %SystemRoot%\system32\Winevt\logs\ DFS Replication.evtx para verificar las operaciones de implementación del volumen de sistema compartido Sysvol.

Los servidores Windows Server utilizan la carpeta %Systemroot%\debug para almacenar los archivos de registro de instalación y desinstalación de muchos componentes. Con respecto a Windows Server 2016, encontraremos múltiples registros en relación con las operaciones relativas a las nuevas funciones y servicios de roles soportados empleando el Administrador del servidor.



Los bosques

Un bosque es una instancia completa del directorio Active Directory. En primer lugar, parece que el Active Directory solo existe a partir del momento en que se crea un nuevo dominio. Sin embargo, la creación de este primer dominio sólo podrá hacerse si tienen previamente especificado que éste se adhiere a un nuevo bosque.

De manera más simple, para que el bosque exista, es necesario un árbol que contenga un dominio Active Directory, y por lo tanto al menos un dominio.

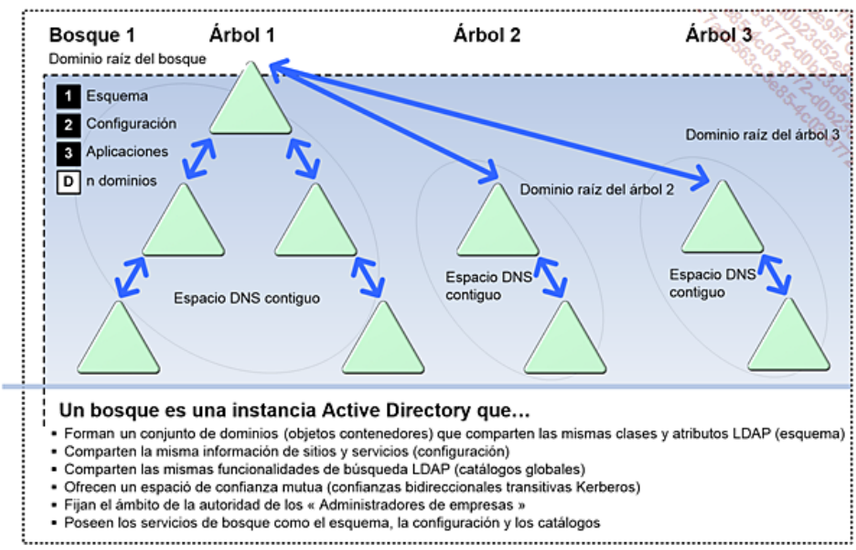
Cada bosque existe mediante el conjunto de todos los controladores de todos los dominios del bosque. Este tema significa también que, por último, un controlador de un dominio dado es "en primer lugar" un controlador del bosque antes de ser también un controlador de un dominio particular.

Por supuesto, el bosque no es operativo sino a través del primer dominio instalado. Luego, en función de las necesidades o las limitaciones de cada organización, será posible añadir otros dominios. Estos dominios podrían formar parte del espacio de nombres inicial o de un nuevo espacio de nombres por medio de una nueva estructura de árbol, o también podríamos decir de un nuevo árbol.

Por definición, todos los dominios de un bosque comparten:

- Un esquema común.
- Una configuración común.
- Una extensión de búsqueda global a través de los controladores de dominio que actúan como catálogos globales.
- Las relaciones de confianza bidireccionales transitorias que representan la estructura lógica del bosque.

El esquema siguiente muestra una instancia de Active Directory.



Estructura de un bosque Active Directory

Como podemos ver en esta imagen, el bosque posee un dominio particular situado en lo más alto del espacio: el dominio raíz del bosque.

El dominio raíz del bosque es el primer dominio instalado. De hecho, la implementación del bosque requiere la implementación de un árbol, que a su vez requiere la implementación de un dominio, que en si mismo requiere la instalación de un equipo con el estado de controlador de dominio y de catálogo global Active Directory.

Hemos visto antes cuáles eran las operaciones de construcción de un nuevo árbol realizadas a través del Asistente de Configuración de servicios de dominio Active Directory. Uno de los puntos importantes es la creación de objetos TDO (*Trusted Domain Object*) y las confianzas de los dominios.

Ahora, si miramos lo que respecta al bosque, el punto más importante es, naturalmente, el dominio raíz del bosque. Este dominio actúa como punto de control y de paso obligado para muchas operaciones de carácter global. Entre estas operaciones, podemos mencionar todo lo que respecta a la gestión de los permisos y la configuración a nivel del bosque y también la transitividad de autenticaciones entre los dominios del bosque empleando el protocolo Kerberos v5.

1. Criterios, papel y buen uso de los bosques

Esta sección tiene por objeto ayudarnos a tomar las decisiones adecuadas en función de los diferentes contextos o escenarios que podemos encontrar. Una de las cuestiones fundamentales es **"¿Cuando es realmente necesario o conveniente crear un nuevo bosque?"**.

Así, si bien es cierto que un bosque es una instancia completa del directorio Active Directory, y si Microsoft desde hace varios años puso de relieve el hecho de que un bosque representaba una empresa "entera" o una organización en el sentido Exchange del término, Microsoft siempre ha dado a entender que, más tarde, sería posible imaginar una mayor interoperabilidad en los entornos compuestos por más de un bosque.

Por lógica, y aunque la recomendación es construir infraestructuras fáciles de mantener, el hecho de crear varios bosques puede permitir a una empresa disponer de varias zonas de autoridad distintas.

Luego, será posible conectarlos mediante la creación de confianzas externas o confianzas de bosques. Esta evolución de la estrategia permite construir soluciones donde cada bosque de la empresa puede ser conectado a los otros bosques de la empresa o incluso bosques pertenecientes a socios externos.

Este enfoque permite percibir todas las posibilidades que pueden ser asociadas a los bosques de Active Directory, que se listan a continuación:

- El bosque Active Directory es un conjunto de dominios Active Directory. Como referencia, tengamos en cuenta que los objetos de tipo "dominio" son técnicamente contenedores basados en las clases domain, domainDNS y samDomain.
- El bosque Active Directory es un conjunto de unidades de replicación. Estas unidades de replicación son el resultado directo de las particiones soportadas por cada uno de los dominios del bosque.
- El bosque Active Directory es una frontera de seguridad y puede ser a su vez un contenedor de elección para estudiar una delegación de autoridad a escala del bosque.

Este puede ser el caso de los escenarios donde un «holding» controla N empresas. En este modelo, las operaciones de tipo fusión, adquisición, y también separación pueden ocurrir y una arquitectura compuesta de varios bosques facilitará las operaciones de reestructuración.

2. Configuración del bosque y dominio raíz

En el entorno de Windows 2000 Active Directory, no es posible realizar operaciones de cambio tan importantes como la supresión, modificación o cambio de nombre del dominio raíz del bosque. Incluso durante el desarrollo de Windows 2000 Server, estas limitaciones eran conocidas y Microsoft ya preveía que durante la disponibilidad de la próxima versión principal de Active Directory, esas operaciones serían mejoradas.

De esta forma, a partir de Windows Server 2003 hasta Windows Server 2016, los servicios de dominio Active Directory soportan el renombrado del dominio raíz del bosque. Tenga en cuenta que no siempre es posible borrar o "sustituir" el dominio raíz del bosque por otro.

Con respecto al renombrado de los dominios Active Directory: el comando rendom incluido con Windows Server soporta todas las etapas necesarias para cambiar el nombre DNS y el nombre NetBIOS de un dominio Active Directory. ¡Debemos prestar atención al hecho de que existen muchas limitaciones! Por ejemplo, esta herramienta no debe ser utilizada en bosques que dispongan de una organización Exchange Server compuesta por servidores Exchange Server 2007, 2010 y 2013. Para más información acerca de estas delicadas operaciones, busque How Domain Rename Works en el sitio de Microsoft.

Para más información sobre las incompatibilidades en las operaciones de renombrado de dominios Active Directory, consulte el artículo de Microsoft 300684 de la base de conocimientos.

¡Los dominios que funcionan en el nivel funcional Windows Server 2008 o posterior están sujetos a las mismas restricciones! Por ejemplo, la instalación de los servicios AD CS (*Active Directory Certificate Services*) prohíbe las operaciones de renombrado en los servidores Windows Server 2008 o posterior.

Particiones del bosque

El ámbito raíz del bosque es muy importante porque se utiliza para nombrar y localizar la partición de configuración así como la partición de esquema del bosque.

Así, en el dominio raíz *corpnet.corporate.com*, Active Directory muestra las DN de estos dos particiones de la forma siguiente:

Para la partición de configuración: cn=configuration,dc=corpnet,dc=corporate,dc= com

Para la partición de esquema: cn=schema,cn=configuration,dc=corpnet,dc=corporate,dc=com

De hecho, estos objetos no existen realmente como hijos del dominio raíz del bosque. Del mismo modo, puede parecer que la partición de esquema está contenida dentro de la partición de configuración, ¡mientras que no es realmente nada!

De hecho, la idea es lograr que sea cual fuere el dominio del bosque, estas importantes particiones sean referenciadas con los mismos nombres. De esta manera, cada controlador de dominio en cualquier dominio del bosque "posee" las particiones:

- cn=configuration, **DN del dominio Raíz del Bosque**;
- cn=schema,cn=configuration, **DN del dominio Raíz del Bosque**.

Los nombres comunes (DN - *Distinguished Names*) de las particiones de configuración y esquema proporcionan sólo una visión lógica de estos contenedores y no una representación física de su ubicación en Active Directory.

Creación del dominio raíz del bosque

La implementación de la raíz del bosque permite crear el DIT (*Directory Information Tree*) inicial que servirá de "esqueleto" a la infraestructura de servicios de directorio Active Directory.

Así, el Asistente de Configuración de servicios de dominio de Active Directory, realiza las operaciones siguientes:

- Se crean los contenedores de las particiones de esquema y de configuración.
- Se asignan los roles de maestros de operaciones - PDC Emulator, RID, Domain Naming, Schema e infraestructura. Como se trata del primer dominio instalado, el primer controlador del primer dominio del bosque tiene cinco maestros de operaciones.
- Se crean los grupos **Administradores de empresas** y **Administradores de esquema** en este dominio. Esta operación es muy importante ya que estos dos grupos permiten gestionar la infraestructura de Active Directory en su conjunto, la cual debe ser considerada como una zona de seguridad solo vinculada a esta instancia de Active Directory.

3. Activación de las nuevas características de bosque de Windows Server

Para activar las nuevas funcionalidades disponibles a nivel de un bosque, todos los controladores de dominio del bosque deben funcionar con la versión de Windows Server correspondiente al nivel deseado. Por ejemplo, para alcanzar el nivel funcional de bosque Windows Server 2012 R2 o Windows Server 2016, todos los controladores de dominio de todos los dominios del bosque deberán utilizar Windows Server 2012 R2 como mínimo para alcanzar el nivel de Windows Server 2012 R2 o utilizar Windows Server 2016 para alcanzar el nivel superior Windows Server 2016.

Tenga en cuenta que para alcanzar el nivel funcional de bosque Windows Server 2016, necesitará previamente aumentar el nivel funcional de dominio de cada uno de los dominios del bosque al nivel de Windows Server 2016.

El paso de un dominio de un modo determinado a un modo superior solo puede alcanzarse si todos los controladores de dominio son compatibles con el modo de solicitado. Por ejemplo, el paso de un dominio que utilice el nivel funcional de Dominio Windows Server 2012 al nivel funcional de Windows Server 2016 solo podrá iniciarse si todos los controladores de dominio del mencionado dominio utilizan Windows Server 2016. Como ocurre desde Windows 2000 Server, es imposible detener una operación en curso. Por último, tenga en cuenta que todas las operaciones de elevación de los niveles funcionales de los dominios y bosques son irreversibles.

Las mismas observaciones aplican para las operaciones que se refieren a los niveles funcionales de los bosques.

Modo de bosques y funcionalidades soportadas por Windows Server 2016

Windows Server 2016 no implementa nuevas funcionalidades directamente dependientes de los niveles funcionales de dominio y bosque. Sin embargo, esta versión proporciona nuevas para gestionar mejor los accesos privilegiados a través de la funcionalidad PMA (*Privileged Access Management*), así como la funcionalidad Azure AD Join.

Modo de bosques y funcionalidades soportadas por Windows Server 2012 R2

Los bosques que utilizan el nivel funcional Windows Server 2012 R2 no aportan nuevas funcionalidades.

Los dominios que usan el nivel funcional dominio Windows Server 2012 R2 soportan las nuevas funcionalidades siguientes:

- Los silos de directivas de autenticación: estos nuevos parámetros sirven para determinar las cuentas que pueden ser restringidas por dichos silos. Se definen las directivas de autenticación a aplicar a los miembros. Los silos son objetos de Active Directory destinados a los usuarios, equipos y servicios.
- Las directivas de autenticación: estos objetos de tipo bosque pueden aplicarse a las cuentas de usuario miembros de un dominio Windows Server 2012 R2 para controlar en qué equipos un usuario puede abrir una sesión a través de un control de acceso basado en condiciones.
- Mejoras de la protección del lado del controlador de dominio para eliminar el uso de NTLM, el uso de RC4 y DES con Kerberos, impedir la renovación de los vales de usuario (TGT) más allá de la duración de vida inicial de 4 horas.

Modo de bosques y funcionalidades soportadas por Windows Server 2012

Windows Server 2012 no implementa nuevas funcionalidades o posibilidades en relación con el nivel funcional de bosque. Con respecto al nivel funcional de dominio una mejora respecto al protocolo Kerberos Armoring. En este caso, si desea que los controladores de dominio Windows Server 2012 o posteriores anuncien que soportan notificaciones, necesitará actualizar todos los controladores a Windows Server 2012 o una versión posterior.

Observe también que durante la creación de un nuevo dominio, éste utilizará de forma automática Windows Server 2012.

Modo de bosques y funcionalidades soportadas por Windows Server 2008 R2

Los bosques que emplean el nivel funcional Windows Server 2008 R2 ofrecen a los administradores de Active Directory la posibilidad de implementar la papelera de Active Directory. Se trata de la única nueva funcionalidad aportada por el nivel funcional de bosque Windows Server 2008 R2. Por supuesto, un bosque que use el nivel funcional Windows Server 2008 R2 soporta todas las funcionalidades ofrecidas por el nivel funcional de bosque Windows Server 2003.

Modos de bosques y funcionalidades soportadas por Windows Server 2008

Los bosques que funcionan en el modo Windows Server 2008 soportan todas las funcionalidades del nivel funcional de bosque Windows Server 2003, pero ninguna funcionalidad adicional. Sin embargo, todos los dominios que se añadan al bosque funcionarán por defecto en el nivel funcional de dominio Windows Server 2008.

Modos de bosques y funcionalidades soportadas por Windows Server 2003

Las funcionalidades reservadas a los bosques Windows Server 2003 se enumeran a continuación:

Mejoras de la replicación del catálogo global

Esta función está desactivada en modo Windows 2000, salvo cuando los catálogos generales de replicación asociados de forma directa funcionan en Windows Server 2003.

Esta función está disponible en modo Windows Server 2003.

Objetos Esquema inactivos

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003.

Si el nivel funcional de su bosque se eleva a Windows Server 2003, entonces podemos redefinir una clase o un atributo después de haberlo desactivado. Recordemos que en Windows 2000, las clases y los atributos añadidos al esquema básico base pueden ser desactivados sin elevar el nivel funcional del bosque, sin embargo, no será posible cambiar si el nivel funcional del bosque es Windows Server 2003 (o superior).

Confianzas de los bosques

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003.

Si el nivel funcional de nuestro bosque es elevado a Windows Server 2003, entonces podemos conectar o conectar dos bosques Windows Server 2003, diferentes empleando una relación de confianza transitiva unidireccional o bidireccional. En el caso de que la confianza creada sea bidireccional, cada dominio de cada uno de los dos bosques se puede aprobar. Las confianzas de bosque son interesantes ya que puede obtener los beneficios siguientes:

- Gestión simplificada, reduciendo el número de aprobaciones externas necesarias.
- Relaciones bidireccionales completas entre todos los dominios de cada bosque.
- Soporte de la apertura de sesiones a través del UPN (*User Principal Name*) entre dos bosques.
- Soporte de los protocolos de Kerberos V5 y NTLM v2.
- Flexibilidad de administración, ya que cada bosque es una zona de poder.

Replicación de valores vinculados

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003.

La replicación de valores vinculados (LVR - *Linked Value Replication*) permite replicar por separado los diferentes valores de un atributo compuesto de múltiples valores. Por ejemplo, en los controladores de dominio Windows 2000 Server, cuando se efectúa una modificación a un miembro de un grupo, el atributo en cuestión y su contenido completo debe ser replicado. La replicación LVR permite replicar de manera independiente cada valor modificado y no el contenido del grupo entero. Como para las funcionalidades ya descritas antes, debemos elevar el nivel funcional del bosque a Windows Server 2003.

Cambio de nombre de un dominio

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003 y en los niveles funcionales superiores.

Mientras que siempre había sido posible cambiar de nombre a los dominios Windows NT, y Windows 2000 y el directorio Active Directory aportaban una multitud de nuevas funcionalidades, la asignación de nombres DNS a dominios Windows 2000, debía ser planificada al no poder renombrar toda o parte de la estructura de dominios. Los servidores Windows Server 2003 soportan ahora esta funcionalidad bajo la condición de que todos los controladores de dominio del bosque funcionen bajo Windows Server 2003, que todos los dominios funcionen en el modo Windows Server 2003 y que el bosque, también funcione en el nivel funcional de bosque Windows Server 2003.

La funcionalidad de renombrado de un dominio será en especial útil si la empresa procede a una adquisición o, a un cambio de razón social. De

hecho, el cambio de los nombres de dominio permite realizar todas las operaciones siguientes:

- Cambiar los nombres DNS y los nombres NetBIOS de cualquier dominio de un bosque, incluido el dominio raíz del bosque.
- Reestructurar la posición de cualquier dominio de un bosque, salvo la del dominio raíz del bosque que sigue siendo de forma obligatorio el más alto de la estructura.
- Reestructurar la jerarquía de los dominios para que un dominio situado en un árbol X pueda ser trasladado a un árbol Y.

La herramienta de cambios de nombres de dominio **Rendom.exe** permite las operaciones de renombrado de un dominio cuando el dominio funciona en modo Windows Server 2003 o posterior.

Observe el hecho de que el cambio de nombre de dominio tiene efectos importantes sobre todos los controladores de dicho dominio.

Algoritmos de replicación Active Directory mejorados

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003.

Los controladores de dominio Windows Server 2003 hasta Windows Server 2016 mejoran significativamente el funcionamiento de los servicios de dominio de Active Directory. Así, el uso de la memoria y el nuevo algoritmo de manejo de los sitios Active Directory son grandes mejoras.

Estas mejoras permiten a las grandes empresas soportar infraestructuras compuestas por un mayor número de dominios y sitios. Descubriremos más adelante que cada sitio Active Directory tiene un controlador de dominio que actúa como generador de la topología intersites (ISTG - *Inter Site Topology Generator*). El hecho de utilizar controladores de dominio que funcionen con una versión reciente de Windows Server como Windows Server 2012 R2 o Windows Server 2016, mejorará las replicaciones aunque los sitios y los dominios aún contengan controladores de dominio que empleen una versión inferior de Windows Server.

La recomendación de Microsoft es colocar en cada sitio Active Directory que deba disponer de un controlador de dominio, un controlador que utilice la versión más reciente del sistema operativo. De esta forma, utilizará la versión más reciente del controlador de dominio desempeñando el rol de catálogo global e ISTG. Por supuesto, para los clientes que disponen de un único controlador de dominio por sitio, esto significa que hay que actualizar todos los controladores.

Como la mayoría de las nuevas funcionalidades aportadas por Windows Server tiene por objeto mejorar y optimizar el funcionamiento, podrá acordarse la realización de estas actualizaciones solo en los sitios que se beneficiarán de estas mejoras.

Observe el hecho de que algunas funcionalidades no pueden ser activadas salvo que el bosque utilice como mínimo el nivel funcional Windows Server 2003. Este será el caso para el nuevo algoritmo de gestión de conexiones intersites. A modo de información, la capacidad de la ISTG dentro de los bosques Windows 2000 Server permitía correr con una topología de unos pocos cientos de sitios como máximo (300 sitios). Los controladores Windows Server 2012 y las versiones posteriores que funcionan en un bosque Windows Server 2003 o superior pueden generar una topología de replicación de hasta varios miles de sitios.

Además de esta nueva capacidad, la ISTG de cada sitio pasa a ser capaz de realizar una selección aleatoria de los servidores cabeza de puente del sitio para distribuir de forma más equitativa la carga de replicación intersite. Esta posibilidad es por supuesto en particular interesante cuando un sitio sirve a muchos otros sitios en modo estrella. En Windows Server 2003, la herramienta *Active Directory Load Balancing*, **adlb.exe**, ofrecida en el Kit de recursos técnicos de Microsoft Windows Server 2003, debe ser utilizada sabiendo que esta característica de equilibrar la carga fue implementada a partir de Windows Server 2008 R2 hasta Windows Server 2016.

Con respecto a la ISTG, de KCC y BHC: El KCC (*Knowledge Consistency Checker*) es un componente disponible en todas las versiones desde Windows Server 2003 hasta Windows Server 2016. Su función consiste en mantener la topología de replicación intra e intersite. Creando objetos de tipo conexión, se puede ajustar la topología física en función de la disponibilidad de controladores de dominio, los costes de replicación y las horas de apertura de los vínculos de sitios. El KCC realiza un control de la topología de replicación cada 15 minutos y aplica de forma automática los cambios necesarios. Por definición, cada sitio Active Directory tiene (al menos) un controlador de dominio que actúa como ISTG, KCC y también de servidor cabeza de puente (o BHS para *Bridge Head Server*). A partir de Windows Server 2008 R2 hasta Windows Server 2016, el KCC puede distribuir las replicaciones entre varios servidores BHS, creando o modificando los objetos de conexión existentes sin que sea necesario usar la utilidad ADLB (*Active Directory Load Balancing Tool*) para reequilibrar la carga entre los distintos BHS.

Para más información sobre la replicación de Active Directory y sus mejoras con las diferentes versiones de Windows Server, consulte el sitio de Microsoft: http://www.microsoft.com/adds

Clases auxiliares dinámicas

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003 y versiones posteriores.

El soporte de las clases auxiliares dinámicas significa que ahora es posible vincular estas clases con objetos particulares y ya no a clases enteras de objetos. Observe que es posible eliminarlos de la instancia a posteriori.

Modificación de la clase de objetos inetOrgPerson

Esta función está desactivada en modo Windows 2000.

Esta función está disponible en modo Windows Server 2003.

El directorio de Active Directory soporta la clase de objetos **inetOrgPerson** y sus atributos, según lo especificado en la RFC 2798. Microsoft ha implementado esta clase ausente del esquema original para ofrecer una mejor interoperabilidad del directorio Active Directory con otros servicios de directorio LDAP y X.500 no Microsoft, en particular concernientes a la migración de los objetos de estos directorios a Active Directory. De hecho, la clase **inetOrgPerson** es derivada de la clase **user** y puede también ser usada como entidad de seguridad. Cuando el dominio trabaja en el nivel funcional Windows Server 2003, pasará a ser posible utilizar el atributo **userPassword** con la clase **inetOrgPerson** y también con la clase de objetos **user**. Tenga en cuenta que hasta ahora, la contraseña de un objeto de la clase **user** se administraba empleando el atributo **unicodePwd**.

Las clases **user** e **inetOrgPerson** disponen ambas de los atributos **userPassword** y **unicodePwd**. El atributo **userPassword** se hereda de forma directa de la clase **Person** mientras que el atributo **unicodePwd** se hereda de forma directa de la clase **user**.

Conjunto de dominios de confianza mutua

Al principio, con los primeros entornos Active Directory que trabajaban con Windows 2000 Server, Microsoft prefirió "idealizar" la empresa en un solo bosque Active Directory, explicando que los entornos de bosques múltiples presentan restricciones y un menor "valor añadido" en comparación con un entorno compuesto por un único bosque -más fácil de mantener y gestionar.

Las nuevas posibilidades presentadas a partir de Windows Server 2003 hasta Windows Server 2016 permiten hoy ofrecer soluciones más sutiles. En efecto, hoy es posible, fuera de las tradicionales confianzas externas, crear confianzas de bosques que permitirán a las empresas que requieren varios bosques construir una solución más abierta. Es así como en las organizaciones compuestas por varias zonas de poder, puede ser buena idea crear más de un bosque, es decir, un bosque por zona de administración.

Posibilidad de despliegue de un controlador de dominio en solo lectura que ejecuta Windows Server 2012 R2 o Windows Server 2016

Un controlador de dominio en solo lectura es un nuevo tipo de controlador de dominio surgido a partir de Windows Server 2008 hasta Windows Server 2016. Este tipo de controlador de dominio mantiene particiones de Active Directory en solo lectura. Los RODC, *Read Only Domain Controllers*, nos permiten desplegar un controlador de dominio cuando la seguridad física del equipo no puede garantizarse. Antes de poder instalar un controlador de dominio en modo sólo lectura, el nivel funcional del bosque debe ser como mínimo Windows Server 2003 o superior. Observe que en función de la versión del sistema operativo que deseemos implementar dentro del dominio, necesitaremos actualizar el esquema del bosque Active Directory como se indica a continuación:

- Windows Server 2008 : Versión 44
- Windows Server 2008 R2 : Versión 47
- Windows Server 2012 : Versión 56
- Windows Server 2012 R2 : Versión 69
- Windows Server 2016 : Versión 82

4. Unidades de replicación y rol de los bosques

Un bosque es la unidad de replicación más amplia que pueda existir dentro de una instancia del directorio Active Directory. Los datos a sincronizar en los distintos controladores de dominio del bosque se replican y sincronizan en base a las particiones del directorio Active Directory.

Hemos visto en el capítulo relativo a la integración de las zonas DNS en Active Directory que existían varias particiones. Estas particiones tienen por objeto organizar el directorio en diferentes regiones y así controlar mejor y dominar cómo tienen lugar las replicaciones dentro del bosque.

El directorio Active Directory está compuesto por cuatro grandes tipos de datos. Por esto, existen cuatro grandes tipos de particiones que serán utilizadas para albergar estos datos específicos.

- Los datos que conciernen al mismo dominio se almacenan en la partición del dominio.
- Los datos que se refieren al bosque entero se almacenan en la partición de configuración y la partición de esquema. En el caso de los controladores de dominio Windows Server 2003 hasta Windows Server 2016, el bosque también podrá incluir un nuevo tipo de particiones dedicadas a las aplicaciones: las particiones del directorio de aplicaciones.

Por supuesto, los objetos de un dominio Active Directory se almacenarán en la partición del dominio y se replicarán en todos los controladores de dominio del dominio, mientras que los datos relativos a los objetos de la configuración o del esquema se replicarán en las particiones de configuración o esquema en todos los controladores de dominio del bosque.

Las diferentes particiones y el impacto de la replicación en el bosque se describen a continuación:

Partición de esquema: cada instancia de Active Directory es un único bosque de Active Directory, el cual contiene una sola versión del esquema del directorio de tal manera que solo puede existir una única definición a nivel del bosque. El esquema contiene las definiciones de cada clase de objeto sabiendo que puede ampliarse según las necesidades de la empresa. Del mismo modo que todos los objetos de los sistemas basados en Windows NT son protegidos por las ACL, esto es lo mismo para las clases de objetos declarados en el esquema.

Partición de configuración: cada instancia de Active Directory contiene una sola configuración del directorio a escala del bosque. La configuración describe la topología y otros parámetros del bosque como la lista de los dominios, los árboles, los bosques, así como la ubicación de los controladores de dominio y catálogos globales en relación con los sitios Active Directory. Como es el caso para la partición de esquema, la partición de configuración se replica en todos los controladores de dominio del bosque.

Particiones del directorio de aplicaciones: los datos específicos de las aplicaciones pueden ser almacenados en las particiones del directorio de aplicaciones de Active Directory. A diferencia de las aplicaciones empresariales tales como Microsoft Exchange Server o Microsoft System Center Configuration Manager que modifican el esquema y luego se integran en las particiones de configuración y/o de dominio, algunas aplicaciones podrán almacenar en estas nuevas particiones los datos de carácter "menos global". De esta forma, podemos crear particiones específicas que solo son replicadas en los controladores de nuestra elección, de forma independiente de su ubicación dentro del bosque. Uno de los principales beneficios de este nuevo tipo de partición es poder ofrecer a las aplicaciones un espacio de almacenamiento altamente tolerante y disponible de forma global a escala empresarial.

Desde el punto de vista funcional, el motor de replicación del directorio Active Directory trabaja con varios maestros. Esto significa que cualquier objeto puede ser creado y modificado en cualquier controlador de dominio del bosque. Se trata, por supuesto, de un concepto general pero fundamental, ya que permite que el directorio Active Directory sea extensible de forma global, disponible y pueda administrarse en cualquier punto de la red, sin depender de un único Maestro, tal y como siempre ha sido el caso de LAN Manager, Windows NT u otros sistemas operativos no Microsoft.

La granularidad de replicación se aplicará a los objetos, los atributos de objetos y también los valores "múltiples" propios de determinados atributos. Este último punto se refiere a la replicación de valores vinculados, también denominada replicación LVR - *Linked Value Replication*.

A modo de ejemplo, en los controladores de dominio Windows 2000, cuando se efectúa una modificación a un grupo -tal como la adición o eliminación de un miembro- todo el grupo se replica. Cuando el dominio se eleva al nivel funcional Windows Server 2003 o posterior, entonces se activa la replicación LVR, y en este caso solo el o los valores modificados serán replicados. Este punto es en especial interesante para las empresas que disponen de infraestructuras compuestas por varios cientos o incluso miles de controladores de dominio.

Sin embargo, seamos conscientes de que las operaciones de carácter único controladas por los maestros de operaciones a nivel del bosque hacen que no sea posible realizar ciertas operaciones en cualquier controlador de dominio del bosque, sino sólo en los controladores de dominio que poseen un papel FSMO particular.

Observe: la replicación de Active Directory respeta las excepciones relativas a los cinco roles FSMO que son los tres FSMO de cada dominio al que habrá que añadir dos FSMO dedicados a las operaciones del bosque.

Por lo tanto, debemos considerar que para que la replicación sea por completo operativa a nivel del bosque, es necesario que los controladores de dominio, los cinco maestros de operaciones simples (FSMO, *Flexible Single Master Operations*), la topología intersite así como los equipos que desempeñen el papel de catálogos globales estén configurados de manera correcta y, si es posible, operativos. En el caso de que uno de estos elementos experimente un fallo, entonces los servicios ofrecidos por el elemento en cuestión no estarán disponibles y podrán producirse los casos siguientes:

- Si un controlador de dominio no se encuentra en un sitio, entonces se solicitará otro controlador de sitio.
- Si el único controlador de un sitio web está ausente, entonces otro controlador de otro sitio del mismo dominio será nominado para "rescatar" al sitio. Luego será seleccionado por los clientes del sitio.
- Si los maestros de operaciones del bosque no estuvieran disponibles, entonces las funciones de esquema de creación y supresión de áreas dentro del bosque no estarán disponibles, sin alterar el normal funcionamiento de los dominios del bosque.

- Si el catálogo global de un sitio no está disponible, entonces otro catálogo situado en otro sitio será elegido y seleccionado. Si ningún catálogo está disponible, entonces los inicios de sesión de los usuarios podrán tener lugar, salvo para los usuarios que nunca hayan abierto sesión de dominio a partir del controlador de dominio elegido, a menos que tengamos desactivado el uso de los GC para la autenticación cuando el dominio funciona en modo Windows 2000 nativo o en un nivel funcional posterior.

Observe: los miembros del grupo **Administradores del dominio** siempre tendrán la posibilidad de autenticarse en el dominio cuando los controladores GC no estén disponibles. Esta posibilidad permite a los administradores del dominio conectarse al dominio incluso en modo degradado.

5. Maestros de operaciones FSMO de bosques

Hemos visto antes que cada dominio Active Directory dispone de tres maestros de operaciones a través de los PDC Emulator, RID Master e Infraestructure Master, para gestionar las operaciones de carácter único.

La misma problemática se plantea a nivel del bosque selva que tiene dos roles de maestro de operaciones simples. De igual forma que los roles FSMO de dominio son únicos a nivel de cada dominio, estas funciones FSMO de bosque lo son dentro del bosque. En otras palabras, no puede existir un único controlador de esquema y un solo y único maestro de asignación de nombres de dominio para todo el bosque.

El maestro de operaciones Controlador de esquema: el controlador de dominio que actúa como controlador de esquema controla todas las operaciones de actualización y modificación del esquema del directorio Active Directory. Por lo tanto, para actualizar el esquema de un bosque, hay que ser capaz de ponerse en contacto con el equipo Controlador de esquema. Como se explica más arriba, no puede existir un solo Controlador de esquema para un bosque.

El maestro de operaciones Maestro de asignación de nombres de dominio: el controlador de dominio que actúa como maestro de asignación de nombres de dominio controla todas las operaciones de adición o eliminación de los dominios en el bosque. Como esto es, por supuesto, el caso con el Controlador de esquema, no puede existir un solo maestro de asignación de nombres de dominio para un bosque.

6. El bosque y la infraestructura física de Active Directory

Acabamos de ver que el Bosque de Active Directory desempeña un papel fundamental como elemento de la estructura técnica de la instancia Active Directory. Para implementar el lado físico de la infraestructura técnica del bosque Active Directory, ahora tenemos que descubrir dos elementos fundamentales:

Los objetos sitios Active Directory: por definición, los sitios constituyen la estructura de la red física. A nivel del bosque, los objetos sitio permiten representar la topología real de la red en términos de zonas de conectividad. De esta forma, los controladores de dominio, servidores y equipos cliente miembros del mismo sitio Active Directory son beneficiados por comunicaciones más rápidas y frecuentes que si los socios están situados en diferentes lugares.

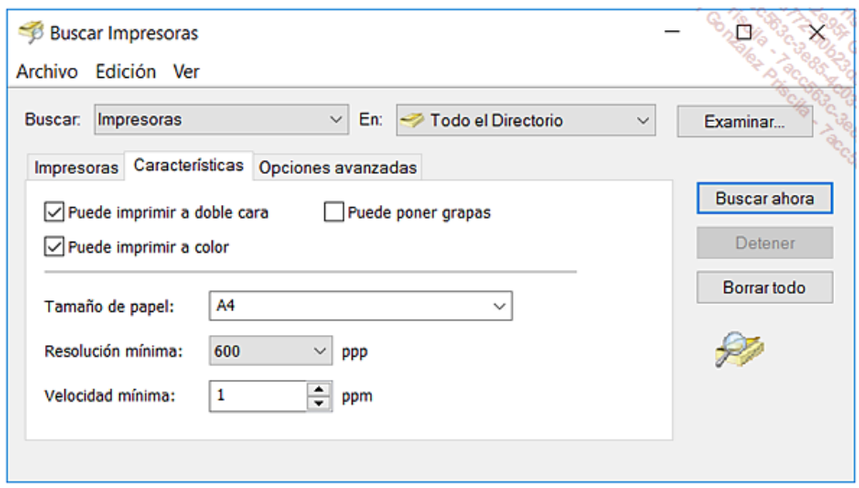
Los sitios son muy importantes para optimizar el uso del ancho de banda entre los controladores situados en lugares remotos y conectados por enlaces con poco ancho de banda.

Los controladores de dominio catálogos globales: por definición, los controladores de dominio que actúan como catálogos globales (o GC de*Global Catalog*) poseen una copia de todos los objetos de todos los dominios del bosque. Sin embargo, cuando un controlador de dominio de un determinado dominio asume la función de catálogo global del bosque, "conoce" de forma natural todos los objetos de su propio dominio, pero no poseerá una copia parcial de los objetos procedentes de otros dominios del bosque. Esto significa que todos los objetos son conocidos, sin excepción alguna, pero no todos los atributos de dichos objetos.

Las Particiones presentes en los GC procedentes de otros dominios del bosque se llaman conjuntos de atributos parciales o PAS (*Partial Attributes Set*).

Ni los usuarios, ni las aplicaciones necesitan conocer los "detalles" de la estructura de dominios y árboles del bosque. Les basta con invocar a uno de los catálogos globales del bosque para encontrar y localizar el objeto buscado basándose en los atributos más interesantes presentes en los catálogos globales.

Por defecto, el primer controlador de dominio del primer dominio del bosque es el primer catálogo global. Por ejemplo, la siguiente ventana dirige una petición LDAP hacia los catálogos globales para buscar en **Todo el Directorio** una impresora que soporte la impresión en color y el formato de papel A4.



Extensión de búsqueda global o dirigida a un árbol o un dominio particular

La definición de las zonas DNS de Active Directory permite localizar los distintos servicios dentro del bosque como por ejemplo, un controlador de dominio GC para un sitio determinado, a través del registro de recursos del servicio DNS _gc_tcp.NombredeSitio._sitios.NombredeBosque.

Por supuesto, "NombredeBosque" es el nombre de dominio raíz del bosque y el protocolo de transporte declarado en el registro de DNS declara la utilización del servicio _gc TCP en el puerto 3268, puerto utilizado por los controladores de dominio que incluyen la función de catálogo global. Los catálogos globales responden, por consiguiente para su ámbito en el puerto TCP 389 y de forma global para el bosque en el puerto TCP 3268.

Podremos y deberemos con seguridad declarar otros catálogos globales para ofrecer servicios de búsqueda global para todos los usuarios y aplicaciones que se encuentren en los distintos sitios geográficos de la empresa. De esta manera, les será posible:

- Buscar de forma "local" objetos en el conjunto del directorio Active Directory.
- Resolver los sufijos de nombres principales cuando un controlador de dominio debe autenticar a un usuario basado en su UPN (*User Principal Name*), tal como *BDurand@eu.corpnet.corporate.net*.

- Resolución de los miembros de grupos universales. Recordemos que los grupos de distribución y de seguridad de tipo universal se almacenan solo en los controladores de dominio que actúan como catálogos globales.
- Resolver las referencias a objetos situados en otros dominios del bosque.

7. Fronteras de seguridad y rol de los bosques

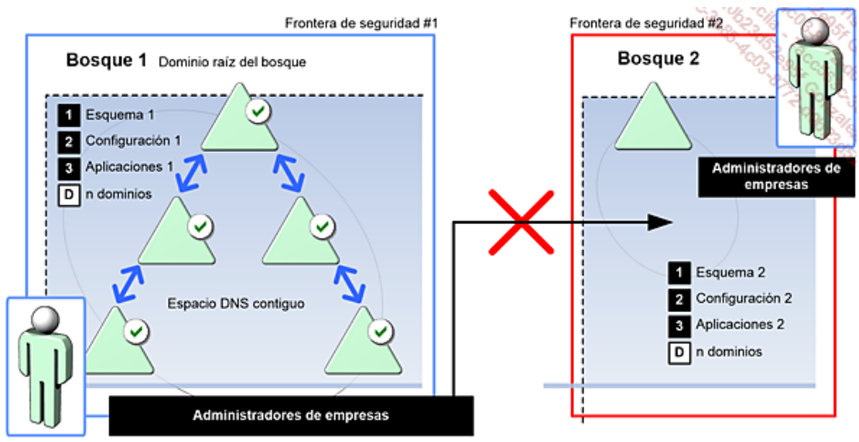
Sabemos que en un entorno compuesto por varios dominios Windows NT, el dominio es la más alta autoridad de gestión, administración y control. En efecto, el administrador de un dominio determinado puede, por esencia, tomar posesión de cualquier objeto situado en el ámbito de dicho dominio.

En cuanto al directorio Active Directory, la pregunta que debemos plantearnos es ¿Existe en el bosque una autoridad suprema que pueda apropiarse de los objetos situados en otros dominios del bosque?. La respuesta es "si" en la persona de un usuario miembro del grupo Administradores de empresas.

Precaución: los miembros del Grupo **Administradores de empresas** pueden controlar todos los objetos de todos los dominios del bosque. La protección de los miembros de este grupo es muy importante y depende de forma fundamental de la administración del dominio raíz del bosque. Observe a su vez que el grupo **Administradores de empresas** así como el grupo **Administradores de esquema** solo existen en el dominio raíz del bosque y no en otros dominios.

Al estar el contenedor situado en el nivel más alto del espacio controlado por el bosque, parece claro que los administradores de un bosque X no podrán tomar control de un objeto que esté ubicado en un dominio de otro bosque, salvo por supuesto en el caso de que un administrador del bosque posea el objeto deseado.

El esquema siguiente muestra la separación de poderes en la escala del bosque. Cada bosque tiene su propio grupo **Administradores de empresas** y cada bosque, es por definición una frontera de seguridad. Ya exista o no una confianza de dominio o de bosque entre los dominios raíz de los dos bosques, los miembros del grupo de **Administradores de empresas** de un bosque no podrán tomar posesión de objetos situados en el otro bosque.



Aislamiento de la seguridad de los controles de acceso a nivel de la entidad de bosque

Delegación a nivel de los bosques

El bosque es una verdadera unidad aislada y autosuficiente, es posible para los arquitectos de Active Directory ofrecerla como un elemento capaz de desempeñar el papel de frontera de seguridad y zona de administración y de poder. Acabamos de ver que los miembros del grupo de Administradores de empresas no pueden tomar el control de objetos situados en los dominios de otro bosque. En cambio, los Administradores de empresas cuentan con todos los poderes en todos los dominios miembros del bosque incluso en el caso de que decidamos retirar a los usuarios todos o parte de esos privilegios de administración.

Observe: debido a su condición, los Administradores de empresas tendrán siempre, por definición, la posibilidad de devolver de forma directa todos los derechos que falten.

Si es en realidad necesario crear una nueva zona de seguridad para disponer de un aislamiento real, la única solución consiste en crear un nuevo bosque y declarar de forma manual los permisos necesarios en función de las necesidades y limitaciones deseadas (confianza inter dominio o confianza inter bosque).

En el caso en que dos zonas de poderes separados deban ser implementadas, crear dos bosques. En el caso en que cada área requiera un aislamiento total, entonces crear un bosque para cada uno de los dominios que requieren un aislamiento de seguridad. Por supuesto, esto no funciona sin recordar lo que se hizo en el pasado en entornos Windows NT, pero para circunstancias excepcionales, soluciones excepcionales. Vamos, sin embargo a descubrir más adelante que las confianzas de bosques son mucho más ricas y poderosas que las antiguas relaciones de confianza NT.

La aplicación del aislamiento podrá justificarse en los casos siguientes:

- Debemos securizar el acceso a datos de manera exclusiva a los usuarios de un bosque dado.
- Debemos disponer de un aislamiento del esquema del directorio.
- Debemos dividir la partición de configuración en varias entidades para aislar a los cambios de configuración. De esta manera, los impactos del cambio de configuración de Active Directory están más controlados.

8. Confianzas dentro de bosques Active Directory

Por definición, los intercambios de autenticaciones y la seguridad de los controles de acceso dentro de un bosque son soportadas por las confianzas internas del bosque. Dichas confianzas son confianzas transitivas bidireccionales capaces de hacerse cargo de las relaciones de tipo "padre-hijo" y también "Raíces de árbol" en modo bidireccional y soportando la transitividad.

- El modo bidireccional permite al domino X aprobar al dominio Y y viceversa.
- La transitividad implica que cuando los dominios X e Y se aprueban y los dominios Y y Z se aprueban, entonces las dominios X y Z se aprueban a su vez.

Una confianza (o relación de aprobación) es una relación lógica establecida entre los dominios. Esta permite una autenticación directa durante la cual un dominio autorizado para aprobar garantiza las autenticaciones de inicio de sesión de un dominio de confianza. Las cuentas de usuario y grupos globales definidos en un dominio de confianza podrán recibir los derechos y permisos de acceso a un dominio de aprobación.

a. Beneficios aportados por la transitividad de las confianzas

La transitividad de las confianzas dentro de los bosques Active Directory permite un acceso inter-dominios simplificado. Este principio permite al conjunto de los usuarios del bosque un inicio de sesión único. El principio de inicio de sesión único surgió en 1993 con Windows NT 3.1. Esta característica fundamental, que permite a contextos de seguridad diferentes confiar en otros, simplifica la gestión de cuentas de usuario y grupos donde solo es necesario crearlos una única vez. Este concepto es uno de los conceptos fundamentales que permiten una centralización de la gestión de identidades.

El modo bidireccional presta servicio a la infraestructura técnica y es una facilidad para los administradores.

Estos dos grandes principios permiten a todos los dominios del bosque aprobarse de forma mutua. En este caso, las autenticaciones validadas en un domino determinado se convierten de forma potencial en aceptables en todos los demás dominios del bosque, siempre gracias a la transitividad y al lado bidireccional de confianzas internas. En la medida en que cualquier nuevo dominio del bosque es objeto de una confianza, el número de ratificaciones necesarias para "conectar" n dominios del bosque es igual a n-1.

Un bosque Active Directory es comparable a un entorno de dominios NT construido sobre un modelo de tipo **Modelo de aprobación total**. En comparación, podemos señalar que bajo Windows NT o con versiones antiguas de Samba, un modelo compuesto por diez dominios requería la creación y mantenimiento de n x n-1 relaciones de confianza, es decir, noventa, unidireccionales y no transitivas. En un entorno Active Directory, el mismo modelo no solo se requiere de nueve relaciones de confianza bidireccionales transitivas, creadas de forma automática, **¡O sea, diez veces menos!**

Las confianzas disponibles dentro de un bosque Active Directory tienen el mismo rol funcional que en el entorno de Windows NT. Crean una relación entre dos dominios permitiendo a los usuarios un área de acceso a los recursos situados en otro dominio y a los administradores de un dominio controlar los recursos de otro dominio y viceversa, si es necesario.

¡Una confianza no da ningún permiso ni ninguna autorización! Solo permite a dos contextos de seguridad independientes participar "de igual a igual" en una negociación de seguridad. Sólo en una segunda instancia el administrador de un dominio determinado, autorizará a un usuario o un grupo de otro dominio a manipular un recurso específico.

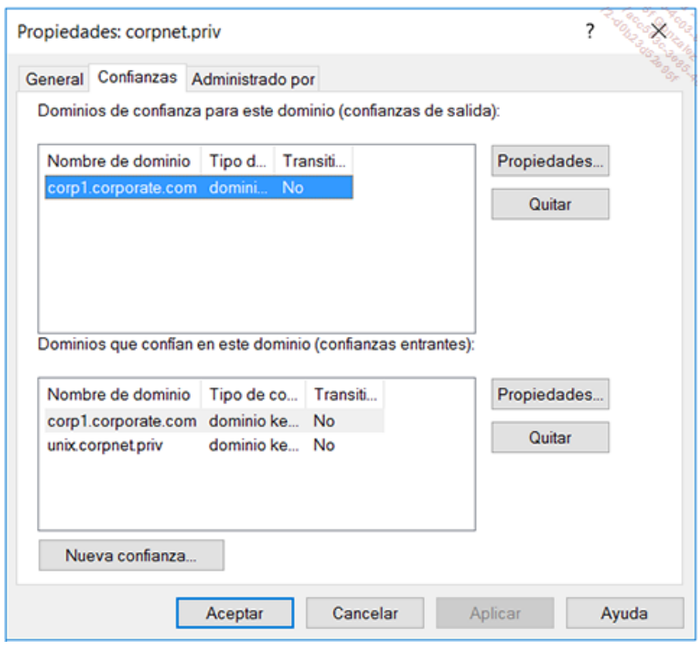
b. Estructura del bosque y confianzas

Desde el punto de vista de la estructura del bosque, cada vez que se añade un nuevo dominio, se crea una nueva confianza interna bidireccional transitiva de forma automática entre el dominio padre y el dominio hijo.

Ocurrirá lo mismo en la creación de un nuevo árbol mediante la creación de una nueva confianza de tipo **Raíz de árbol**.

La pantalla siguiente muestra las propiedades del dominio *corpnet.priv*. Este dominio dispone de una confianza de tipo **Raíz de árbol** y muestra claramente su naturaleza no-transitiva. Observe que la funcionalidad de transitividad depende exclusivamente de la elección realizada en el momento de la creación de la relación de confianza. En nuestro ejemplo, si se deseaba disponer del soporte de transitividad, la relación de confianza debería suprimirse y luego vuelta a crear, esta propiedad no puede ser modificada a posteriori.

Por último, el concepto de dominio y las relaciones de confianza permitirá "crear la confianza" entre las entidades técnicas que pueden funcionar en los diferentes niveles funcionales.



Confianza interna de tipo raíz de árbol transitiva y bidireccional

c. Confianzas y objetos TDO en los bosques de Active Directory

Es interesante observar que el bosque es la entidad más "Alta" de seguridad autónoma, nos es posible apoyarnos en las relaciones de confianza para crear e implementar la confianza entre espacios de seguridad distintos.

Las confianzas nos permitirán realizar todas las conexiones funcionales y tecnológicas que podamos vernos obligados a realizar. El concepto mismo del bosque se basa en las confianzas. Además de su uso dentro de los bosques de Active Directory, las confianzas permitirán la conexión de los dominios más antiguos o que utilicen tecnologías no Microsoft tales como los dominios Kerberos V5 no-Windows que funciona principalmente bajo UNIX.

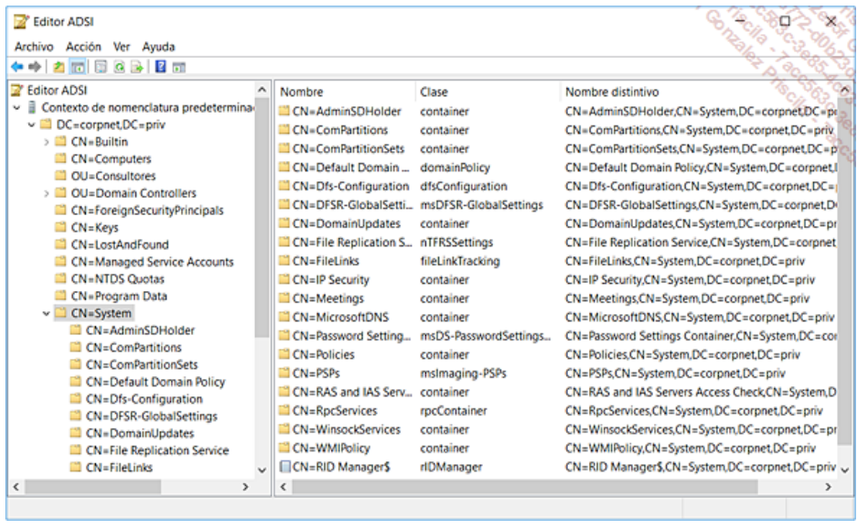
Tecnologías, protocolos de confianza y objetos TDO:

- Los controladores de dominio Windows Server 2003 hasta Windows Server 2016 utilizan los protocolos Kerberos V5 y NTLMv2 para la autenticación de usuarios y aplicaciones. Por defecto, los equipos Windows 7, Windows 8.x y Windows 10 miembros de un dominio Windows Server 2003 hasta Windows Server 2016 utilizan el protocolo Kerberos v5. En el caso en que un equipo no sea capaz de negociar el protocolo de autenticación Kerberos v5, entonces se utilizará el protocolo Windows NT NTLMv2.
- El protocolo Kerberos V5 es un protocolo moderno en la medida en que la autenticación inicial permite a los clientes solicitar un vale de demanda de vales. Los vales así obtenidos serán válidos para un determinado servicio alojado por un servidor particular. La autenticación Kerberos V5 es soportada en el controlador de dominio de Active Directory mediante el módulo AS (*Authentication*

Service), mientras que la expedición de los vales de servicio corre a cargo del módulo TGS (*Ticket Granting Services*). De hecho, el controlador de dominio desempeña el papel de autoridad aprobada entre el cliente y el servidor. Por último, el cliente presente el vale de servicio aprobado al servidor en el domino de aprobación para su autenticación.

- En cambio, el protocolo Windows NT NTLM requiere que el servidor que contiene los recursos contacte un controlador de dominio cliente para verificar la información de identificación de la cuenta presentada por comparación con las contenidas en el token de acceso del cliente.
- Objetos del dominio aprobado: Las relaciones de confianza de cada dominio son representadas en Active Directory por objetos de tipo dominio aprobado (TDO, *Trusted Domain Objects*). Cada vez que se establece una relación de confianza, un único objeto TDO se crea y almacena en el contenedor sistema de su dominio.

Los objetos TDO son objetos de gran importancia en la medida en que sus atributos describen todas las características de las confianzas que pueden existir entre dos dominios. Como se explicó antes, los objetos TDO de un dominio residen en el contenedor System de dicho dominio.



*Objeto de la clase **trustedDomain** para el dominio partners.net*

En función de las circunstancias de la creación de las confianzas, los objetos TDO procedentes de la clase **trustedDomain** son creados por el Asistente de Configuración de los servicios de directorio de Active Directory, por la consola de gestión MMC **Dominios y confianzas de Active Directory** o de forma manual a través del comando de sistema **Netdom**.

Los atributos de cada objeto TDO contienen la información que especifica el tipo de la confianza, su naturaleza, la transitividad de la aprobación, así como los nombres de los dominios recíprocos. En el caso de las confianzas de bosques, los objetos TDO almacenan también atributos adicionales para identificar todos los espacios de nombres aprobados por el bosque de su compañero.

A continuación encontraremos los detalles relativos a los atributos de un objeto TDO más importantes:

flatName: designa el nombre NetBIOS del dominio que está asociado a dicha confianza.

trustDirection: designa el sentido de la relación de confianza.

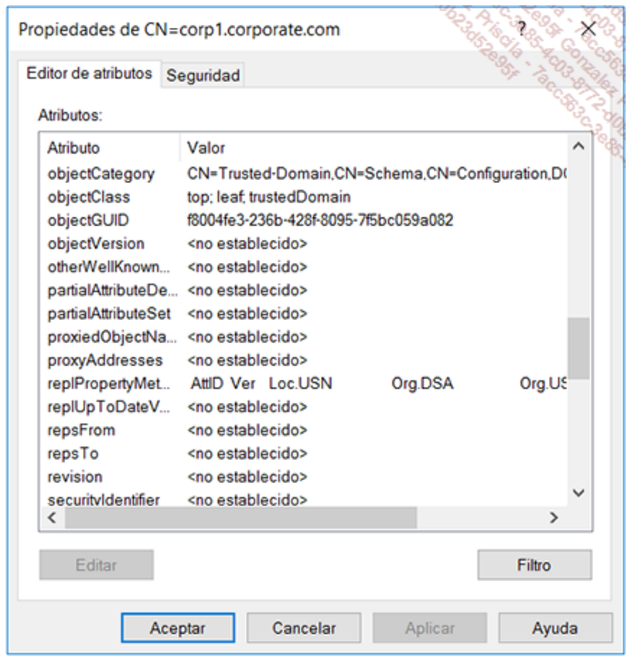
- **0**: La confianza está desactivada.
- **1**: La confianza es entrante. Esto significa que el dominio está autorizado a aprobar.
- **2**: La confianza es saliente. Esto significa que el dominio está aprobado.
- **3**: La confianza es a la vez entrante y saliente. Esto significa que el dominio está autorizado y también puede aprobar.

trustPartner: este atributo es el nombre en formato DNS asociado al dominio cuando se trata de un dominio Active Directory, o el nombre NetBIOS del dominio si se trata de una confianza de bajo nivel, es decir, Windows NT o compatible NT.

trustType: este atributo indica el tipo de relación de confianza con el dominio.

- **1**: Confianza de bajo nivel NT o compatible.
- **2**: Confianza Windows 2000.
- **3**: MIT.
- **4**: DCE.

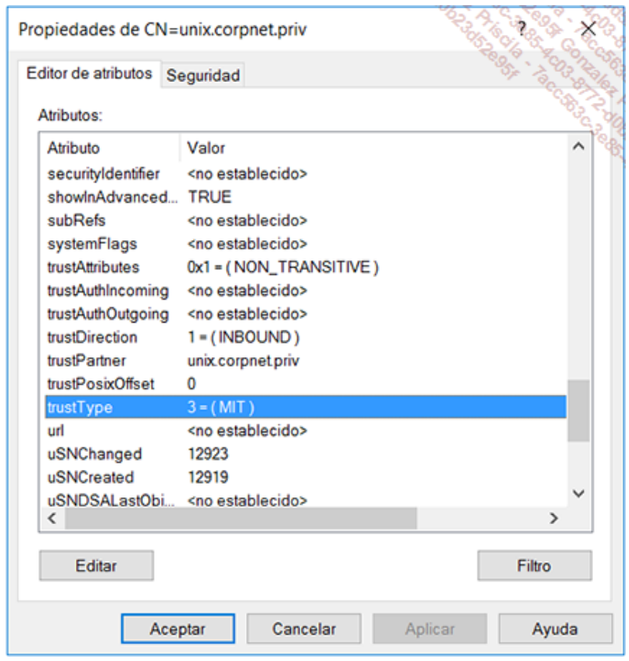
Los tipos de confianza MIT (*Massachussets Institute of Technology*) y DCE (*Distributed Computing Environment*) permiten la recepción de las diferentes implementaciones de Kerberos disponibles en entornos UNIX. Las implementaciones MIT y DCE del protocolo Kerberos están distribuidas de manera amplia en los sistemas Unix como Aix, Solaris, HPUX y muchos otros.



Relación de confianza bidireccional de tipo Windows

Como resultado de ADSI Edit, la pantalla anterior muestra los atributos de un objeto TDO que representa una confianza de árbol. Estos atributos incluyen los nombres de los diferentes árboles, los sufijos de nombres de usuarios principales (UPN, *User Principal Name*), los sufijos de nombre principal de servicios (SPN, *Service Principal Name*) y los espacios de nombres de ID de seguridad (SID, *Security ID*).

La figura siguiente muestra los parámetros de una aprobación de tipo Kerberos MIT:



Relación de confianza con un dominio Kerberos Unix

d. Tipos de confianzas soportadas

Acabamos de recordar que las confianzas permiten la comunicación entre los dominios. Así, las confianzas desempeñan el papel de canales de autenticación necesarios para los usuarios de un dominio X a fin de acceder a los recursos de un dominio Y. Cuando se añade un nuevo dominio a un bosque existente, se crean dos confianzas por el **Asistente Configuración de servicios de dominio de Active Directory**. Los diferentes tipos de confianzas que pueden ser creados empleando el **Asistente para nueva confianza** o la herramienta de línea de comandos**Netdom** se presentan a continuación.

Confianzas internas creadas por DCPromo

Cuando un nuevo dominio se añade al dominio raíz del bosque o como un nuevo árbol mediante el **Asistente Configuración de servicios de dominio de Active Directory**, las confianzas transitorias bidireccionales son creadas de forma automática.

Dichas aprobaciones pueden ser de dos tipos distintos:

Aprobaciones de tipo Padre-hijo: cuando un nuevo ámbito hijo se añade a un árbol de dominio existente, se establece una nueva relación de aprobación padre-hijo transitiva bidireccional. Las peticiones de autenticación efectuadas a partir de los dominios aprobados se remontan hacia arriba en la jerarquía de dominios, pasando por su padre, hasta el dominio autorizado para aprobar.

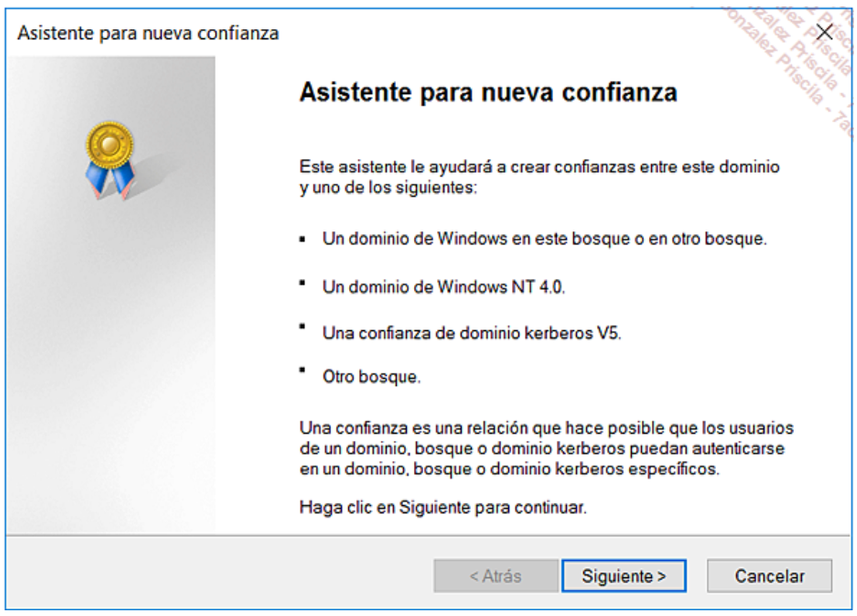
Aprobaciones de tipo raíz de árbol: cuando un árbol de dominio se creada en un bosque existente, se crea por defecto una nueva confianza de raíz de árbol transitiva bidireccional.

Las confianzas creadas por el Asistente Configuración de servicios de dominio de Active Directory son indestructibles. Dichas confianzas por consiguiente no pueden ser destruidas por un error de administración.

Los otros tipos de confianzas de Active Directory

Active Directory soporta otros cuatro tipos de confianzas. Podemos crear dichas confianzas empleando el **Asistente para nueva confianza** o

a través del comando **Netdom**. Estas confianzas son las aprobaciones externos, las confianzas de dominio Kerberos, las confianzas de bosques y las confianzas de acceso directo.



Asistente para nueva confianza

Las **confianzas externas** son por definición no transitivas y pueden ser unidireccionales o bidireccionales. Una confianza externa se utiliza para acceder a los recursos situados en un antiguo dominio Windows NT 4.0 u hoy en día un dominio que se encuentre en otro bosque (no relacionado con la confianza del bosque).

Las **confianzas de domino Kerberos v5** son por definición transitivas y pueden ser unidireccionales o bidireccionales. Una confianza de dominio Kerberos v5 permite a un dominio Windows Active Directory interactuar con un dominio Kerberos no-Windows.

Las **confianzas de acceso directo** son por definición no transitivas y pueden ser unidireccionales o bidireccionales. Las aprobaciones de este tipo permiten acortar el camino de autenticación Kerberos dentro de un bosque. Esto es en particular interesante para mejorar los inicios de sesión entre dos dominios cuando éstos se encuentran en árboles diferentes.

Las **confianzas de bosques** son por definición no transitivas y pueden ser unidireccionales o bidireccionales. Las confianzas de bosques permiten el "matrimonio" entre dos bosques. De esta manera, es posible compartir recursos entre dos bosques es decir, entre todos los dominios de cada uno de los bosques.

e. Bosques Windows Server y confianzas de los bosques

Las aprobaciones de los bosques son una nueva funcionalidad de los servicios de directorio surgida con Windows Server 2003 y las versiones más recientes, tales como Windows Server 2016. El principio fundamental se basa en la utilización de la transitividad de confianzas disponible mediante el uso del protocolo Kerberos v5.

En efecto, los dominio Windows NT y los dominios Active Directory Windows 2000 no permiten a los usuarios de un bosque acceder a los recursos que están situados en otro bosque. Este punto se explica por el hecho de que, en un bosque que funciona en modo Windows 2000, la transitividad de confianzas Kerberos solo está disponible en el caso de las confianzas internas del bosque, y no fuera de éstas.

Así, ya que las confianzas externas son por definición unidireccionales y no transitorias, no será posible que el camino de la confianza pueda extenderse a otras áreas de bosque objetivo.

Hoy, cuando el entorno está compuesto por dos bosques que funcionan en el nivel funcional Windows Server 2003 o un nivel superior hasta Windows Server 2016, y que existe una confianza de bosques entre los dos dominios raíz de los bosques respectivos, entonces las autenticaciones pueden encaminarse entre todos los dominios de los dos bosques. La aprobación de bosques permite un acceso de los usuarios de los bosques aprobados en todos los recursos de la red del bosque aprobador, por supuesto bajo la condición de que los usuarios autorizados tengan los permisos adecuados.

Las empresas que dispongan de más de un bosque podrán aprovechar las ventajas siguientes:

Un nuevo elemento de estructura: el bosque puede convertirse en un contenedor utilizable en el marco de la política de delegación de la empresa. De esta manera, se puede considerar la posibilidad de dividir la administración en varias entidades, teniendo la capacidad de ensamblarlas (en términos de seguridad y autenticación).

Una administración más sencilla: la transitividad de confianzas de bosques permite limitar el número de confianzas externas necesarias para el intercambio de recursos entre los dominios de dos bosques.

Los usuarios de los dos bosques pueden utilizar las autenticaciones basadas en UPN, tales como *BDurand@eu.corpnet.corporate.com*.

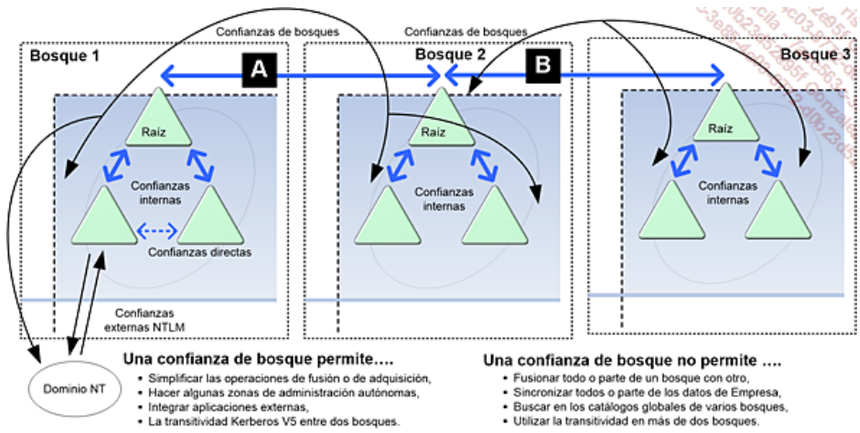
Los protocolos de Kerberos y NTLM pueden ser utilizados dentro de cada bosque al igual que entre los dos bosques.

Confianzas de bosques y nivel funcional de los bosques

Las aprobaciones de los bosques requieren por fuerza que los dos bosques asociados operen en el nivel funcional Windows Server 2003 como mínimo.

Hoy en día Windows Server 2003 es una versión obsoleta. En consecuencia, aunque el nivel funcional de dominio esté aún disponible para los dominios de los controladores de dominio Windows Server 2003, estos se han sustituido por versiones más recientes utilizando por ejemplo Windows Server 2008 R2 o Windows Server 2012 R2; se recomienda elevar el nivel funcional de dominio al más alto. Esta estrategia le permitirá disponer de las últimas características de infraestructura y las últimas mejoras en materia de seguridad.

Aunque el protocolo Kerberos sea el único protocolo capaz de soportar la transitividad dentro del bosque y también entre dos bosques, los servidores que utilizan el protocolo NTLM (tales como los antiguos servidores Windows NT Server o Samba miembros de Dominio Windows Server 2003 o Windows Server 2008) pueden hacerse cargo de los controles de acceso provenientes de otro bosque. Esto es realizado por los controladores de dominio Windows Server que desempeñan el papel de pasarelas de autenticación entre los protocolos de Kerberos y NTLM. Observe que esta funcionalidad ya estaba presente en los controladores de dominio Windows 2000. De esta forma, un usuario autenticado empleando el protocolo Kerberos puede, sin ningún problema, controlarse mediante el Protocolo NTLM para acceder a un recurso gestionado por un servidor que utilice este protocolo.



Posibilidades, límites y marco de utilización de las confianzas de bosques

f. Encaminamiento de los sufijos de nombres y confianzas de los bosques

El enrutamiento de los sufijos de nombres permite gestionar la forma en que las peticiones de autenticación son transmitidas y despachadas entre bosques Windows Server con confianzas de bosque y utilizando los niveles funcionales Windows Server 2003 hasta Windows Server 2016.

En la medida en que la primera necesidad consiste en aprovechar la transitividad de las confianzas de bosque, todos los sufijos de nombres únicos serán encaminados por defecto. De esta manera, la administración de los dos bosques asociados puede ser simplificada en gran medida y todos los usuarios de un bosque dado pueden acceder a los recursos situados en cualquier dominio del otro bosque.

Esta configuración inicial podrá ser personalizada para permitir controlar las peticiones de autenticación aprobadas por uno de los bosques. En efecto, dos bosques pueden asociarse a través de una confianza de bosque, excluyendo algunos dominios.

Por definición, un bosque es un espacio de nombres únicos materializados por los sufijos de nombres únicos. Un sufijo de nombre solo es un nombre dentro de un bosque, tal como un UPN (*User Principal Name*) un SPN (*Service Principal Name*), o el nombre DNS del dominio raíz del bosque o de un árbol de dominio. Los nombres que figuran a continuación son ejemplos de sufijos de nombres únicos:

- Rootcorp.corporate.com ;
- Emea.rootcorp.corporate.com ;
- Partners.net ;
- BDurand@extranet.rootcorp.corporate.com ;
- Svc1$@rootcorp.corporate.com.

Desde un punto de vista del funcionamiento de la confianza de bosques, todos los hijos de todos los sufijos conocidos del bosque son de forma natural dirigidos hacia el otro bosque. Es por ello que la interfaz gráfica de la consola de gestión MMC **Dominios y confianzas de Active Directory** muestra todos los sufijos de nombres conocidos con el carácter asterisco (*).

Por ejemplo, si el bosque utiliza como sufijo de nombres **.rootcorp.corporate.com*, entonces todas las peticiones de autenticación en los dominios hijo *rootcorp.corporate.com* como **.emea.rootcorp.corporate.com*, serán encaminados a través de la confianza de bosque y la transitividad del protocolo Kerberos v5.

Observe: por lógica, cualquier sufijo de nombre hijo hereda la configuración de enrutamiento del sufijo de nombre único al que pertenece. Sin embargo, el enrutamiento de los nuevos sufijos surgido tras la creación de la confianza de los bosques será desactivada por defecto. Esta forma de proceder es la más segura. En efecto, no sería normal que un nuevo dominio dentro de un bosque sea aprobado de forma automática sin que ninguna validación se haya producido por parte del administrador. Podremos, por lo tanto, en segunda instancia, ver los nuevos sufijos de nombres de los nuevos dominios integrados tras la implementación de la aprobación de bosques y sólo entonces decidir activar o no el enrutamiento de autenticaciones.

Para ver o modificar el enrutamiento de los nombres de sufijos, podemos usar el cuadro de diálogo **Propiedades de confianza de bosque**. La selección de los sufijos de nombres específicos le permitirá activar o desactivar el enrutamiento de autenticaciones hacia el bosque asociado.

Detección de los sufijos duplicados, gestión de conflictos y desactivación automática

No es imposible que nombres de dominio idénticos puedan existir en dos bosques diferentes. Este podría, por ejemplo, ser el caso de dominios usando nombres genéricos como *partners.net* o *extranet.privnet.net*. Por esto la confianza de bosque puede gestionar esta excepción.

En el caso de que este problema se encuentre, el enrutamiento del sufijo de nombre más reciente es desactivado de forma automática. Observe que sólo los nombres que respeten el sistema de nombres DNS deben declararse. Por lo tanto, cualquier nombre incompatible supondrá su desactivación de forma automática.

Microsoft recomienda no añadir el carácter @ en el sufijo UPN declarado, ni como nombre de usuario. En efecto, el tratamiento de las peticiones de autenticación encaminadas hacia un bosque aprobado considera los caracteres situados a la izquierda del carácter @ como el nombre de usuario y los caracteres situados a la derecha del carácter @ como el nombre DNS del dominio. La Autoridad de seguridad local LSASS desactiva el enrutamiento de cualquier sufijo UPN que no respete el formato DNS, lo que sería el caso cuando un carácter @ está presente en el nombre.

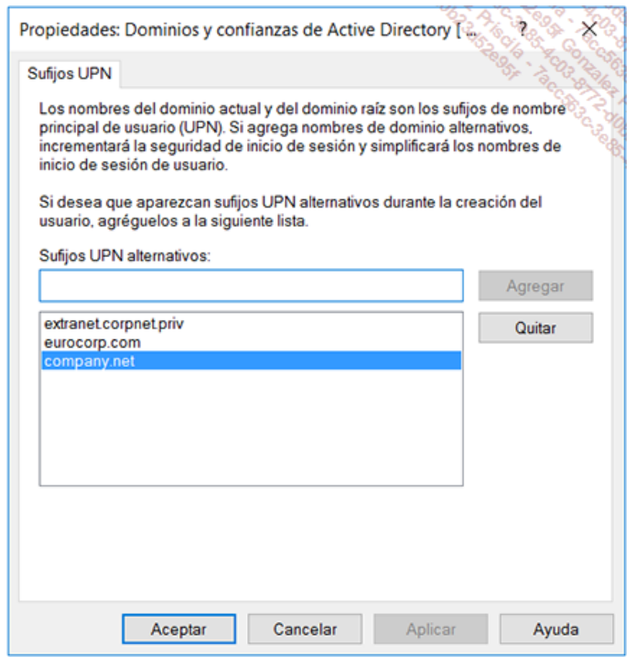
Las operaciones con conflictos propiamente dichos se denominan **colisiones**. Las colisiones pueden producirse cuando el mismo nombre DNS, el mismo nombre NetBIOS o cuando el SID de un dominio está en conflicto con otro SID de sufijo de nombre.

¡Estos puntos parecen evidentes! Sin embargo, conviene prestar especial atención a los problemas de nombres de dominio DNS. En efecto, como todo conflicto provoca la desactivación del nombre al nivel de la confianza del bosque, conviene anticipar al máximo los efectos de los errores de nombres.

Ejemplo de conflicto:

Sabemos que los dominios *corpnet.corporate.com* y *corporate.com* son dominios DNS distintos. Dentro del mismo bosque, estos dos dominios DNS forman un árbol de dominios dentro del bosque cuyo dominio raíz es *corporate.com*. Si consideramos que los dos dominios pertenecen a dos bosques distintos, no hay ningún problema hasta que no exista ninguna confianza o confianza de bosque. Esto significa que es perfectamente posible crear una confianza externa entre los dos dominios. Por el contrario, existirá conflicto si el bosque llamado *corporate.com*y el bosque llamado *corpnet.corporate.com* se vinculan empleando una confianza de bosques. En efecto, como estos dos dominios pertenecen al mismo espacio DNS, el enrutamiento entre estos dos sufijos de nombres será desactivado. Observe sin embargo que el enrutamiento seguirá funcionando para todos los otros sufijos de nombres únicos no conflictivos.

La pantalla siguiente muestra los sufijos de nombres UPN declarados en el bosque Active Directory.



La detección de conflictos de las confianzas de bosques se refiere también a los sufijos UPN

Cuando ocurre un conflicto, sea de la naturaleza que sea, y se detecta, los controles de acceso al dominio en cuestión serán rechazados desde el exterior del bosque. Sin embargo, el funcionamiento normal dentro del bosque se mantendrá, lo que es totalmente normal, ya que el conflicto no tiene significado más que entre los dos bosques y en modo alguno entre los dominios del bosque de pertenencia.

La pestaña **Enrutamiento de sufijo de nombre** disponible en la consola de administración MMC **Dominios y confianzas de Active Directory** en el nivel de las propiedades de las confianzas del bosque nos permitirá guardar un archivo de registro de los conflictos de los sufijos de nombres. Este archivo podrá crearse durante o después de la creación de la confianza del bosque.

Para más información sobre las confianzas y el funcionamiento de los bosques y dominios Active Directory, busque Domains and Forests Technical Reference en el sitio Microsoft Technet en la dirección https://technet.microsoft.com.

g. Uso del comando Netdom para crear y gestionar las confianzas

Por lo general, las confianzas internas, externas y de bosques son declaradas directamente empleando la consola de gestión MMC Dominios y confianzas de Active Directory. Sin embargo, podemos usar el comando **Netdom.exe** disponible por defecto en Windows Server 2008 y las versiones posteriores hasta Windows Server 2016 para crear, verificar, reiniciar y eliminar objetos de confianza.

Operaciones soportadas por Netdom relativas a las confianzas:

- Implementación de confianzas unidireccionales o bidireccionales entre los dominios Windows Server 2003 hasta Windows Server 2016.
- Implementación de confianzas unidireccionales o bidireccionales entre los dominios Windows Server 2003 hasta Windows Server 2016 situados en organizaciones diferentes.
- Implementación de confianzas de acceso directo entre los dominios Windows Server 2003 hasta Windows Server 2016 situados en la misma organización.
- Implantación de una confianza con un reino Kerberos no-Windows.
- Enumeración de las confianzas directas e indirectas.
- Visualización de parámetros y cambio de los parámetros de las confianzas.

Podremos por ejemplo usar el comando Netdom:

- Para verificar una confianza unidireccional entre el dominio DomA y el dominio DomB: `netdom trust /d:DomA DomB /verify`
- Para verificar una confianza bidireccional: `netdom trust /d:DomA DomB /verify /twoway`

La operación de verificación tiene por objeto controlar el buen funcionamiento de la confianza, así como las contraseñas declaradas entre los dos dominios durante la implementación de la confianza.

- Para comprobar que el protocolo Kerberos v5 está en pleno funcionamiento entre un equipo y su dominio de pertenencia*dom1.corporate.com*: `netdom trust /d:dom1. corporate.com /verify /KERBEROS`.

  El uso de los parámetros `/verify` y `/kerberos` requiere la obtención de un ticket de sesión para ponerse en contacto con el servicio de administración de Kerberos del controlador de dominio (servicio KDC) en el dominio objetivo. A partir del momento en que la operación tiene éxito, podemos considerar que todas las operaciones Kerberos pueden funcionar correctamente entre el equipo cliente y el dominio de destino.

Esta operación de verificación de las funciones Kerberos solo puede ejecutarse de forma local en el equipo a probar. Podremos en este caso utilizar las funciones de **Escritorio remoto**.

El comando Netdom permite gestionar las confianzas, pero también permite gestionar las operaciones siguientes:

- Insertar un equipo Windows en un dominio cualquiera que sea su tipo con la posibilidad de especificar la unidad organizativa y generar la contraseña de la cuenta de equipo de forma aleatoria.
- Gestionar las operaciones de administración de las cuentas de equipo como la adición, la eliminación, la consulta, el desplazamiento de las cuentas de equipo de un dominio a otro manteniendo el SID del equipo.
- Verificar los SC (*Secure Channel*) entre los puestos de trabajo, servidores, controladores de dominio Windows Server desde Windows Server 2008 hasta Windows -Server 2016.

Todas estas funciones son muy útiles en el marco del mantenimiento de cuentas de equipo, ya se trate de simples equipos de escritorio o de servidores miembro del dominio.

Tenga en cuenta que no es posible establecer relaciones de confianza entre los dominios Windows NT y dominios Windows Server 2008 R2 o

de un nivel posterior. Las modificaciones introducidas por Microsoft a partir de Windows Server 2008 R2 hacen imposible esta configuración. La modificación del parámetro de seguridad **Permitir algoritmos de criptografía compatibles con Windows NT 4.0** no funcionan en este caso concreto con controladores de dominio de un nivel inferior a Windows Server 2008.

Para más información, consulte el artículo 942564 de la base de conocimientos de Microsoft.

Éxito en el proceso de actualización de Active Directory a servicios de dominio de Active Directory Windows Server 2016

Windows Server 2016 es una versión mayor en más de un sentido. En consecuencia, se podría pensar que la instalación de nuevos controladores de dominio e incluso la actualización in situ de antiguos servidores Windows Server son tareas complejas que requieren una gran preparación.

En realidad, no es nada complicado, y veremos que con un mínimo de preparación para el despliegue de nuevos controladores de dominio Active Directory puede realizarse con mucha facilidad y con un mínimo de riesgos.

El proceso de migración a los servicios de dominio de Active Directory de Windows Server 2016 debe tener como objetivo -Plazo- el uso del nivel funcional más cercano a Windows Server 2016, sin olvidar por supuesto hacer lo mismo con el nivel funcional del bosque.

Verificaciones y gestión de riesgos

Antes de comenzar las operaciones propias de la integración de controladores de dominio Windows Server 2016, se recomienda realizar las operaciones siguientes:

- Realizar un inventario detallado de todos los controladores de dominio importantes, en especial su posicionamiento en los sitios Active Directory, así como los servicios que proveen (GC, servicios DNS, Servicios DHCP, KMS, Servicios de tiempo, …).
- Identificar los controladores de dominio que poseen los cinco roles FSMO.
- Comprobar las actualizaciones de los antiguos controladores de dominio que se conservarán.
- Hacer una copia de seguridad de tipo System State de uno o varios controladores de dominio operativos. Si se trata de VM, detener la VM a respaldar, efectuar clones y luego reiniciarlos.
- Determinar el mejor escenario de vuelta atrás, en previsión de una eventual catástrofe.

1. Preparación de la infraestructura de Active Directory para Windows Server 2016

Retirada de los antiguos controladores Windows Server 2003 en fin de vida

Con el fin de vida de Windows Server 2003, los controladores de dominio que utilizan esta versión del sistema operativo deben ser sustituidos por una versión más reciente del sistema operativo como Windows Server 2008 hasta Windows Server 2016.

Por lo tanto, todos los controladores de dominio Windows Server 2003 deberán eliminarse del dominio. Por lógica, una vez efectuada esta operación, el nivel funcional del domino -y raíz del bosque, deberán ser elevados como mínimo al nivel Windows Server 2008.

De esta forma, la empresa dispone de las funcionalidades aportadas por estos niveles de bosque o dominio, y no es posible añadir un controlador de dominio bajo Windows Server 2003.

Compatibilidad de los controladores de dominio Windows Server 2016 con el nivel funcional Windows Server 2003: Microsoft recomienda alcanzar el nivel funcional de dominio y bosque Windows Server 2008 como mínimo. Sin embargo, Microsoft especifica también que los niveles funcionales de dominio y bosque Windows Server 2003 seguirán siendo soportados en los dominios que supongan controladores Windows Server 2008 hasta Windows Server 2016, así como con los puestos de trabajo Windows 10.

Nivel funcional en Windows Server 2003 discontinuado: Microsoft también indica que los niveles funcionales Windows Server 2003 de bosques y dominio están discontinuados con Windows Server 2016 y que ya no serán soportados en las versiones futuras.

Migración de SYSVOL de NTFRS a DFSR

A partir del nivel funcional de dominio Windows Server 2008 y niveles superiores, el sistema de replicación DFSR puede utilizarse para replicar el volumen SYSVOL. En el caso de que un nuevo dominio de Active Directory se implemente, entonces la replicación DFSR será activada de forma automática para el volumen SYSVOL. En cambio, en el caso de una migración de dominio Active Directory, si la migración no ha sido ya realizada durante la implementación de los antiguos controladores de dominio Windows Server 2008 o posteriores, entonces será necesario migrar del antiguo motor de replicación NTFRS a DFSR.

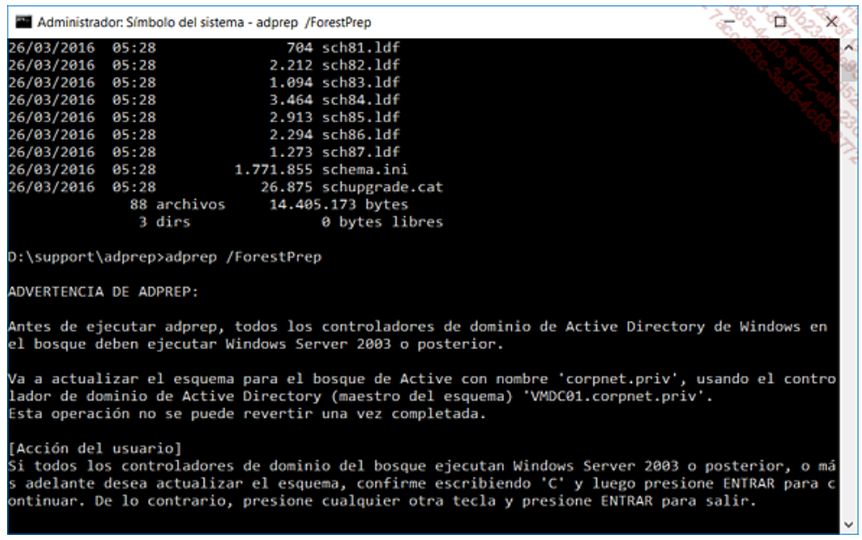
Los nuevos controladores de dominio Windows Server 2016 no soportan más la replicación NTFRS de SYSVOL.

Para más información sobre la migración del volumen de SYSVOL NTFRS a DFSR, busque SYSVOL Replication Migración Guide en el sitio Microsoft Technet en la dirección: http://technet.microsoft.com

Como ha ocurrido en el pasado en el momento de la migración de Dominio Windows NT 4.0 a los servicios de directorio Active Directory de Windows 2000 Server y luego a los servicios de directorio Active Directory de Windows Server 2003, la infraestructura de Active Directory debe estar preparada para acoger a los servidores Windows Server 2008 donde se alojarán los nuevos servicios AD DS. Las recomendaciones y operaciones siguientes deberán efectuarse:

- Asegurarse de poseer una cuenta de administración de dominio que forme parte de los grupos Administradores del dominio, Administradores de empresas, Administrador del esquema. Todas las operaciones que deban realizarse en un servidor que deban ser objeto de una promoción necesitarán también contar con privilegios de Administrador del equipo local.
- Efectuar la operación de actualización del esquema de Active Directory mediante el comando `adprep /forestprep`. Para lograrlo, ejecutamos el comando `adprep /forestprep` a partir de la línea de comandos en el contenido de la carpeta **\support\adprep** del medio de instalación de Windows Server 2016. Para tener éxito la actualización al ejecutar este comando, el administrador deberá pertenecer a los grupos Administrador del esquema, Administradores de empresas y Administradores del dominio.

Con Windows Server 2016, el comando adprep está contenida en la carpeta \support\adprep del medio de instalación de Windows Server 2016.



- Efectuamos la operación de preparación del dominio Active Directory a través del comando `adprep /domainprep /gpprep`. En el controlador de dominio que posea el rol de maestro de infraestructura, ejecutamos el comando `adprep /domainprep /gpprep`. Para ejecutar este comando, el administrador deberá formar parte del grupo administradores de dominio en el que la operación se realiza.
- ¡Observe! Después de haber realizado esta operación, espere con calma a instalar el primer controlador de dominio. Se recomienda esperar a que la nueva información se replique en el dominio. Por supuesto, podemos forzar las replicaciones utilizando las herramientas habituales **Replmon** o mediante el comando **Repadmin**.

Con respecto a los parámetros del comando Repadmin: podemos usar el comando Repadmin con los parámetros /A (de All partitions) P (modo Push) e (de Enterprise en inter-site) d (ver Distinguished Names) para forzar la replicación de todas las particiones del directorio de un controlador particular a los demás.`repadmin /syncall nombre_DNS_de_DC /APed`

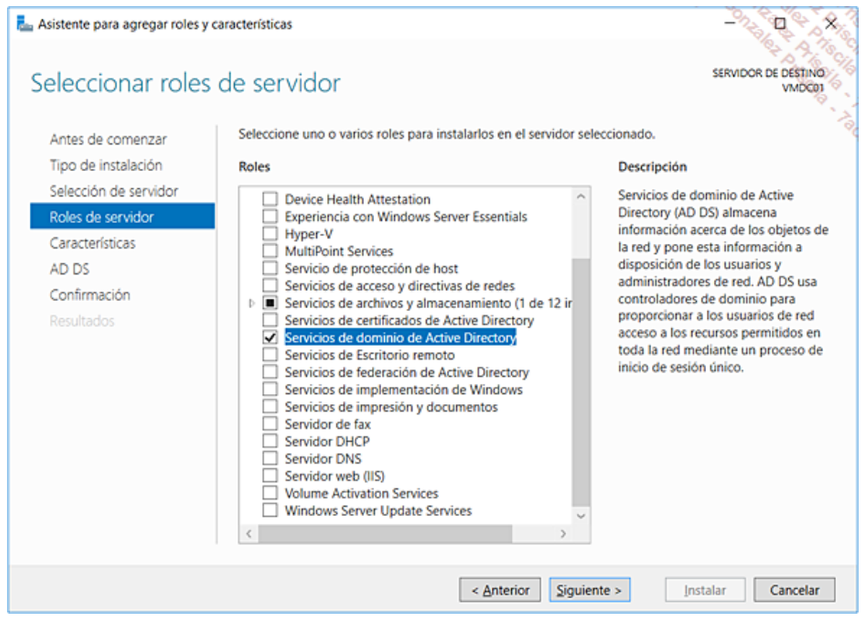
El parámetro que especifica el nombre DNS del controlador de dominio fuente no es obligatorio cuando el comando se ejecuta en este equipo.

2. Implementación de un nuevo controlador Windows Server 2016

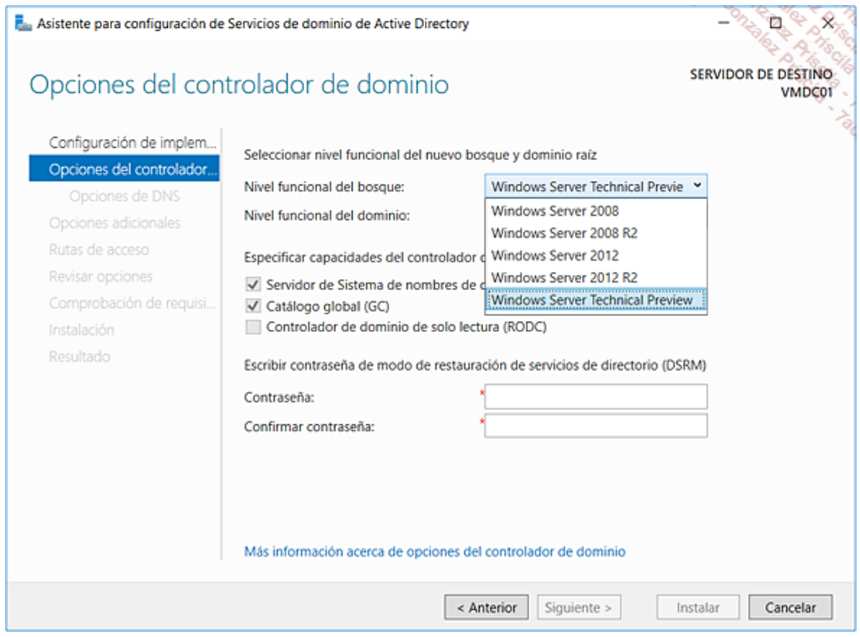
El entorno de producción que funciona con controladores de dominio Windows Server 2008 o versiones posteriores puede ser actualizado a Windows Server 2016 utilizando uno u otro de los escenarios siguientes:

Instalación de nuevos controladores Windows Server 2016

La primera solución consiste en insertar un nuevo servidor Windows Server 2016 en el dominio Active Directory de producción. Como hemos explicado antes, los antiguos controladores Windows Server 2003 se descontinúan y retiran del dominio. Proceda a la promoción del nuevo servidor al nuevo rol de controlador de dominio en el dominio existente. La operación de promoción podrá realizarse empleando la interfaz gráfica o a través de un archivo de comandos Windows PowerShell creado con antelación. La interfaz de Windows Server 2016 ofrece dos asistentes. El primero es accesible de forma directa a través del nuevo **Administrador de servidor - Administrar - Agregar roles y características**. El segundo será propuesto de forma automática al administrador una vez instalado el rol AD DS. Este asistente se llama Asistente de Configuración de los servicios de directorio Active Directory.



Añadir la función AD DS a través del administrador de servidor de Windows Server 2016



Asistente de configuración de los servicios de dominio de Active Directory

Actualización del sistema a Windows Server 2008 y Windows Server 2008 R2

Los supuestos siguientes son soportados por Microsoft:

- Windows Server 2008 R2 SP1 a Windows Server 2016.
- Windows Server 2012 a Windows Server 2016.
- Windows Server 2012 R2 a Windows Server 2016.

3. Reasignación de funciones FSMO

Una vez que el proceso de actualización del primer controlador termina, será necesario actualizar los elementos de infraestructura de Active Directory siguientes:

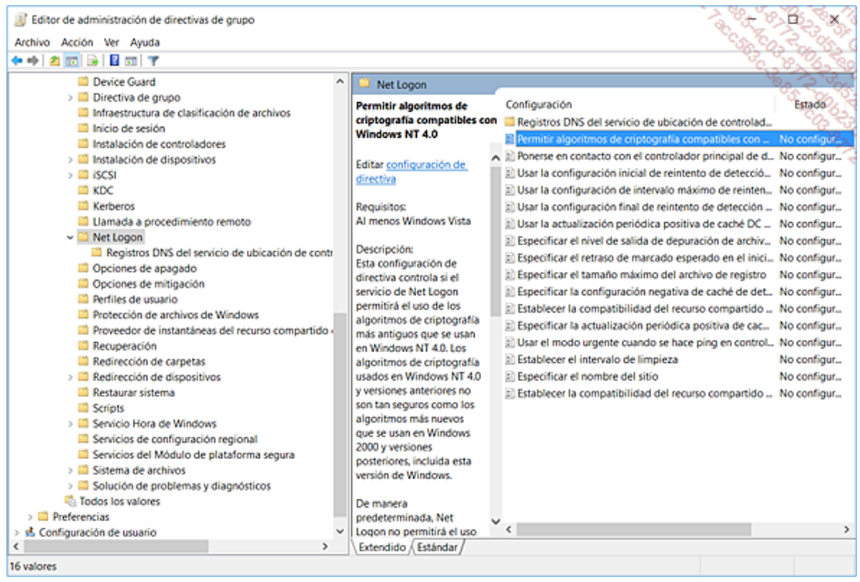
- Reasignación del rol de supervisor de operaciones de nombres de dominio a nivel del dominio raíz del bosque: esta operación no es obligatoria, pero se recomienda para garantizar la creación de particiones del directorio de aplicaciones utilizadas para las zonas DNS Active Directory, si es necesario. Si no deseamos actualizar el controlador de dominio que posee la función, basta con transferir el rol a un controlador de dominio ya actualizado a Windows Server 2016. Esta operación puede ser necesaria, ya que en el primer reinicio, el servicio servidor DNS intentará localizar las particiones necesarias para la actualización de las zonas. Además, si no las encuentra, tomará la iniciativa de crearlas. Para garantizar la correcta creación de estas particiones si se requiere, es obligatorio que el maestro de nombres de dominio se encuentre en un controlador de Dominio Windows Server 2016.
- Reasignación del rol supervisor de operaciones Emulador de controlador de dominio principal dentro del dominio raíz del bosque: esta operación garantiza que las nuevas cuentas adicionales de los dominios Windows Server 2016 serán creadas de forma correcta a nivel del dominio raíz del bosque.
- Reasignación del rol de supervisor de operaciones Emulador de controlador de dominio principal en otros dominios del bosque: esta operación garantiza que los nuevos grupos introducidos por Windows Server 2016, así como su contenido respectivo estarán bien creados en todos los dominios del bosque.
- A partir del momento en que el esquema Active Directory está actualizado mediante el comando `adprep /forestprep` y el dominio objetivo se ha preparado empleando el comando `adprep /domainprep`, se puede efectuar la inserción del primer nuevo controlador de dominio en el bosque Active Directory existente. A pesar de que sea posible instalar el nuevo Primer Controlador de Dominio Windows Server 2008 o Windows Server 2008 R2 en cualquier dominio del bosque, se recomienda colocar el primer Controlador de Dominio Windows Server 2016 en el dominio raíz del bosque. Por supuesto, este problema no se plantea en los entornos de bosque formados por un único dominio.

4. Operaciones de finalización Post Migración

a. Modificación de las directivas de seguridad de los controladores de dominio

Con el fin de aumentar el nivel de seguridad de las plataformas empresariales más importantes, los controladores de dominio Windows Server 2008 y posteriores hasta Windows Server 2016 exigen que, por defecto, las autenticaciones de cliente utilicen la firma de los paquetes SMB (*Server Message Block*), así como la firma del canal de autenticación seguro (*Secure Channel*).

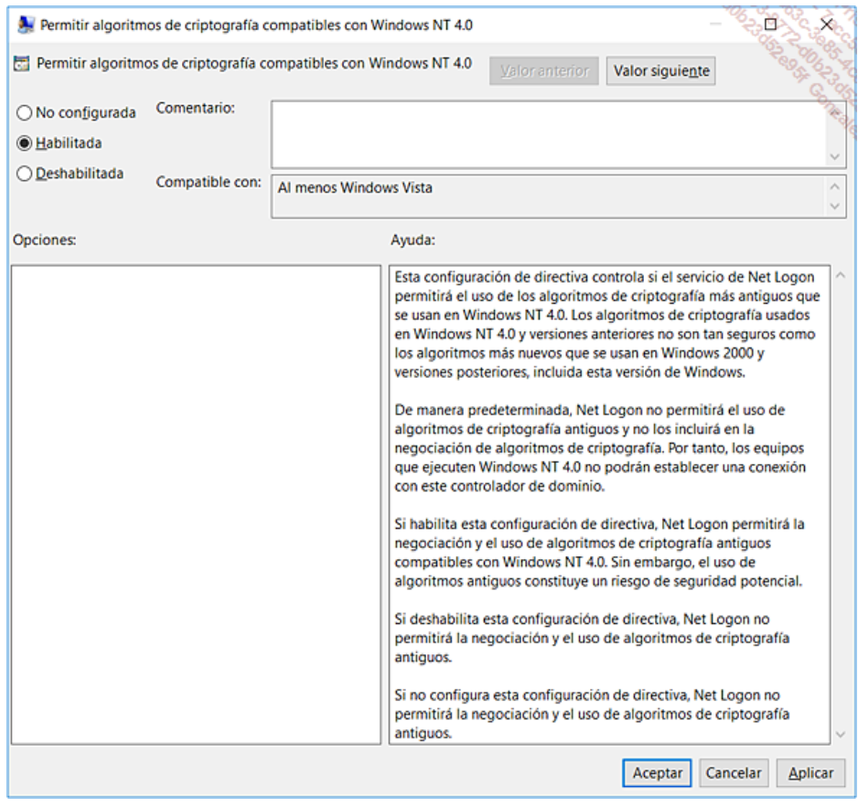
En el caso de que la red de la empresa incluya sistemas Windows NT 4.0 SP2 (no hay soporte para la firma de paquetes SMB) o incluso SP3 (no hay soporte para la firma del canal de autenticación segura), necesitará proceder a la modificación de la directiva de seguridad de los controladores de dominio.



Autorizar los algoritmos de cifrado compatibles NT

La buena práctica sería realizar una actualización de estos antiguos sistemas a una versión más moderna.

En el caso de que sea necesario modificar la directiva de los controladores de dominio, proceda a realizar antes de cualquier modificación una copia de seguridad de la directiva utilizando la función de respaldo disponible en la consola de gestión de directivas de grupo, GPMC.



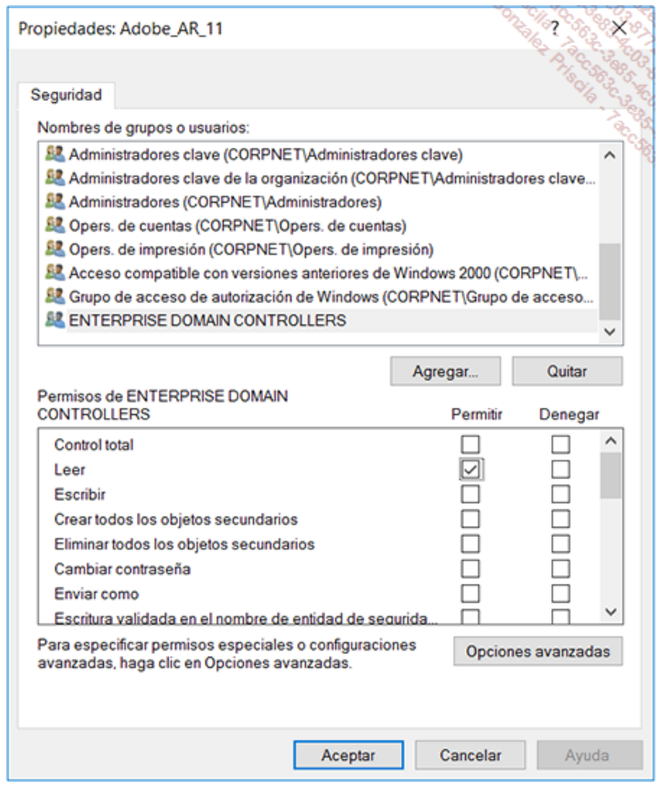
La sección Ayuda de la ventana de configuración del parámetro GPO expone los efectos relacionados con este parámetro, así como un enlace con el artículo de la base de conocimientos de Microsoft.

Para más información sobre la firma de los paquetes SMB y la firma del canal de autenticación segura, busque en el sitio de Microsoft Technet "Background Information for Upgrading Active Directory Domains to Windows Server 2008 AD DS Domains".

b. Actualización de los permisos de los objetos GPO para los antiguos dominios migrados a partir de Windows 2003

Cuando un dominio Windows Server 2003 es objeto de una migración a Windows Server 2008 o superior, el grupo ENTERPRISE DOMAIN CONTROLLERS no dispone de los permisos de lectura sobre los objetos de directivas de grupo disponibles en todos los dominios del bosque. Esta afirmación es verdadera para todos los objetos GPO que fueron creados antes de la actualización a Windows Server 2008 o un nivel superior.

Si ese es el caso, la función de "modelización" incluida en la consola de administración MMC para las directivas de grupo (GPMC), no funcionará. En efecto, cuando se invoca esta opción, un componente del controlador de dominio se solicita para leer y abrir los objetos GPO implicados en la simulación o que se encuentren en el bosque.



Verificación de permisos de lectura en un objeto GPO

Corrección de errores de permisos en el volumen SYSVOL: para corregir este problema de forma rápida, utilice el comando`adprep /GpPrep` luego compruebe el retorno de las operaciones realizadas en el registro del comando situado en la carpeta %System Root%\Debug\adprep\LOGS.

También podemos corregir este problema efectuando la actualización de las autorizaciones de todos los objetos de la directiva de grupo empleando el script **GrantPermissionOnAllGPOs.wsf**. Este script es parte de los ejemplos de scripts incluido antes con la consola de gestión de directivas de grupo disponibles para su descarga para Windows Server 2003. En efecto, en Windows Server 2008 hasta Windows Server 2016, estos scripts, considerados demasiado peligrosos, se han retirado del sistema operativo, y están disponibles mediante descarga desde el sitio de Microsoft.

Un paquete que contiene todos los scripts de automatización de las operaciones de mantenimiento de los objetos GPO está disponible en el sitio de Microsoft en la TechNet Code Gallery. Para descargar este paquete, regístrese en el sitio de Microsoft Technet Gallery a través de la dirección https://gallery.technet.microsoft.com/ luego busque Group Policy Management Console Scripting samples. Una vez instalados, los scripts se colocarán en la carpeta **%Program Files%\Microsoft Group Policy\GPMC Sample Scripts**, como ocurría en Windows Server 2003. Observe que la modificación de las autorizaciones de los objetos de directivas de grupo, que se almacenan en la partición de dominio y en la carpeta SYSVOL, requieren la pertenencia al grupo Admins del dominio.

Utilización de los grupos en entornos Active Directory

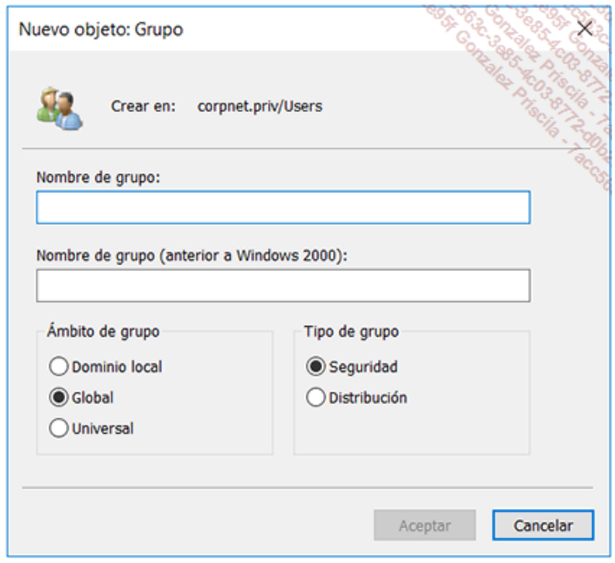
1. Los diferentes tipos de grupos Windows

La casi totalidad de los sistemas operativos implementa el concepto de grupo con el fin de simplificar la administración de sistemas, así como la gestión de acceso a recursos compartidos por los mismos sistemas. De esta forma, combinando las diferentes categorías de usuarios dentro de los grupos, resulta más fácil asignar los derechos, los permisos y luego garantizar su seguimiento.

En efecto, la gestión de las autorizaciones concedidas de manera específica a determinados usuarios debería seguir siendo una operación excepcional difícil de gestionar y supervisar, en el tiempo.

A partir de OS/2 LAN Manager y desde las primeras versiones de Windows NT, la noción de grupo se ha utilizado de forma amplia en el marco de la gestión de los privilegios de administración y acceso a recursos compartidos. Sin embargo, fuera del marco del dominio, cabe recordar que los grupos también están disponibles en todas los equipos Windows o Windows Server.

Hoy en día, los servicios de directorio Active Directory ofrecen muchos grupos predefinidos, así como diferentes tipos de grupos, todos destinados a diferentes tipos de uso. La pantalla siguiente ilustra este aspecto y demuestra que Active Directory ofrece dos grandes grupos: los**grupos de seguridad** y los **grupos de distribución**.



a. Los grupos de seguridad

Como su nombre indica, los grupos de seguridad se destinan a ser utilizados en el marco de las operaciones que requieren un control de acceso específico. Para que estas operaciones o solicitudes de acceso pueden ser controladas, los grupos de seguridad deberán disponer de un SID único (*Security Identifer Descriptor*), al igual que ocurre para los objetos de las clases **user**, **inetOrgPerson**, **computer**, o **domainDns**.

Por supuesto, cuando los usuarios son miembros de uno o varios grupos, heredan los permisos asignados a cada uno de los grupos a los que pertenecen.

Podemos verificar con facilidad este punto procediendo de la siguiente forma:

Abra una sesión con una cuenta de usuario de dominio.

Abra un símbolo de sistema y escriba el comando `whoami /all`.

Analicemos la información devuelta. Descubriremos, nuestro nombre de inicio de sesión, pertenencias a grupos, SID respectivos, así como la lista de nuestros privilegios en el equipo local.

En la medida en que la función principal del grupo consiste en consolidar usuarios y grupos inter-relacionados, los grupos de seguridad también pueden utilizarse para aplicaciones como listas de distribución. Esta función y este tipo de utilización de los grupos se tratará a continuación.

b. Los grupos de distribución

Las aplicaciones pueden requerir el uso de los servicios ofrecidos por la infraestructura de Active Directory. Por ejemplo, ya hemos estudiado los mecanismos de localización de los servicios de directorio Active Directory, disponibles para cualquier aplicación. Los grupos de distribución pueden también actuar en este sentido.

La correcta utilización de los grupos de distribución está directamente relacionada con las exigencias de una aplicación que puede utilizar para fines distintos la gestión de la seguridad y los controles de acceso de Windows. Por último, como su nombre indica, los grupos de distribución solo sirven para agrupar usuarios y otros grupos, sin que sea posible emplearlos nunca para fines de control de acceso.

Ventajas de los grupos de distribución

- Al no disponer de un SID, los grupos de distribución no se incluyen en el -token de acceso del usuario que no haya conseguido abrir una sesión. Este punto puede considerarse como una ventaja reduciendo al mínimo el tamaño de los tokens y así algunos flujos vinculados a las autenticaciones en la red.
- Por otro lado, se refuerza la seguridad. Al no emitirse un SID para el grupo, ningún acceso controlado puede ocurrir.

Inconvenientes de los grupos de distribución

- Como los grupos de distribución no cuentan con SID, estos no pueden ser utilizados para realizar controles de acceso, si no es de manera empírica, dentro de una aplicación que no utilice los servicios de seguridad de Active Directory.

Veremos más adelante que el tipo de un grupo puede ser cambiado entre seguridad y distribución y viceversa cuando el dominio funciona en el nivel funcional Windows 2000 nativo, Windows Server 2003 o posterior.

2. Alcance de los grupos

Los grupos disponibles en los entornos de dominio de Active Directory pueden adoptar diversas formas. Estos diferentes tipos de grupos nos

permitirán controlar el alcance de los grupos creados y repercuten en la naturaleza de objetos que podemos ubicar aquí.

a. Los grupos globales

Por definición, los grupos globales son interesantes para un uso global. Esto -significa que los grupos globales pueden ser utilizados de forma directa sobre cualquier otro equipo del dominio local y también en cualquier dominio del bosque. En sentido amplio, los grupos globales son utilizables en todos los dominios, ya se trate de los dominios Active Directory de un bosque determinado o dominios Active Directory situados en otro bosque.

Los grupos globales solo pueden contener cuentas del dominio local, ya se trate de cuentas de usuario o cuentas de equipo. En efecto, en la medida en que los grupos globales son utilizables en todos los dominios aprobados, si se pudieran establecer en los grupos globales de las cuentas procedentes de otro dominio, esto provocaría una transitividad no deseable.

Cuando el dominio Active Directory funciona en el nivel funcional Windows Server 2003 o posterior, entonces los grupos globales pueden también contener grupos globales del dominio local.

b. Los grupos locales de dominio

Por definición, los grupos locales solo pueden emplearse en el dominio local donde residen.

Cuando el nivel funcional del dominio es Windows Server 2003 o un nivel posterior, los miembros de los grupos de dominio local pueden contener cuentas y grupos globales de cualquier dominio, grupos universales de cualquier domino, así como grupos de domino local del mismo dominio.

También contamos con la posibilidad de añadir los grupos locales a otros grupos locales y asignarles solo los permisos de este dominio.

A diferencia de los grupos locales de los equipos Windows o Windows Server, los grupos locales de dominio Active Directory son utilizables en todo equipo miembro del dominio.

c. Los grupos universales

Por definición, los grupos universales pueden contener miembros procedentes de cualquier dominio del bosque. Pueden ser utilizados de la misma manera que los grupos globales en cualquier dominio del bosque y también entre diferentes bosques de Active Directory.

3. Reglas generales acerca de los objetos de grupo

Como para todos los objetos del directorio Active Directory, pueden realizarse muchas operaciones. Los puntos siguientes definen las operaciones y recomendaciones de uso destinadas a los administradores Active Directory.

a. Mejores prácticas para las cuentas de grupo

Debemos evitar asignar de forma directa permisos a las cuentas de usuario o de equipo. La utilización de los grupos de seguridad es mucho más flexible y mucho más fácil de gestionar. Para alcanzar este objetivo de simplificación y racionalización, debemos primero estudiar el mejor uso de los grupos en su empresa en función de su propia problemática de administración y delegación de la administración.

Debemos crear una convención de nombres para nuestros grupos de seguridad y distribución de tal manera que su papel y/o marco de uso sea fácil de identificar por los gestores de cuentas y de seguridad.

Tenga en cuenta que los grupos de entornos Active Directory pueden contener más que simples usuarios. En efecto, pueden contener cuentas de tipo usuario, grupo, contacto, inetOrgPerson y también objetos de tipo equipo.

En las redes "antiguas", no era habitual establecer grupos de equipos. Los sistemas que operan con Windows 2000, Windows XP Professional, Windows Vista, Windows 7, Windows Server 2008 y Windows Server 2008 R2 en un dominio Active Directory utilizan el protocolo Kerberos y mecanismos de delegación potentes al igual que la posibilidad de autorizar los servicios en base a los SPN. Por lo tanto, podemos ser llevados a crear grupos que contengan solo cuentas de equipo. Estos grupos podrán requerir su propia convención de nombres.

La posibilidad de insertar varios equipos en un grupo es una opción muy interesante para otorgar permisos a los grupos de equipos. Este podrá ser el caso de configuraciones en clúster o también cuando otras aplicaciones utilicen varios servidores o servicios.

Podremos crear grupos locales de dominio para controlar el acceso a los recursos o a las operaciones que deseemos controlar.

En los servidores miembros y otros puestos de red miembros de dominios Active Directory, contamos con la posibilidad de utilizar los grupos locales de equipos o bien los grupos locales de dominio. La regla decide que en un equipo local que deba controlar el acceso a sus propios recursos locales, la mejor práctica es utilizar una cuenta de grupo local del equipo. Sin embargo, este método crea una dependencia de las ACL con respecto al sistema operativo local. Este punto significa que la consolidación posterior de los datos con otro servidor provocará la pérdida de todos los permisos definidos con antelación en el mencionado equipo local. De hecho, cuando varios equipos son susceptibles de controlar los mismos discos o recursos, se recomienda sobre todo no utilizar grupos locales de equipo y favorecer el empleo de grupos locales de dominio.

Este caso es típico de los equipos que operan en un clúster, sabiendo que cada equipo miembro del clúster puede en potencia tener que controlar el acceso a los recursos que este contiene. Al utilizar los grupos locales de dominio, todos los equipos miembro del clúster pueden emplear el grupo presente en el dominio sin ninguna dependencia.

La fórmula mágica

En resumen, desde hace muchos años, conocemos la regla AGLP - *Accounts/Global groups/Local groups/Permissions*. Esta fórmula se adaptó a Active Directory bajo la forma AGUDLP, es decir *Accounts/Global groups/Universal groups/Domain Local groups/Permissions*. Hay que respetar el método siguiente:

- Ubique las cuentas de usuario en los grupos globales.
- Ubique los grupos globales en los grupos universales.
- Ubique los grupos universales en los grupos locales de dominio.
- Afine los permisos para los grupos locales de dominio.

La utilización de los grupos locales de equipo es en especial interesante para los aspectos de sistema relacionados con los permisos de grupos integrados. En todos los casos, la mejor práctica consiste en utilizar las cuentas de grupo procedentes del entorno de Active Directory.

b. Uso correcto de los grupos universales

Los grupos universales no deben ser utilizados para consolidar grupos que se extiendan a varios dominios. Si lo queremos, el método consiste en añadir las cuentas a los grupos globales y luego a incluir estos grupos globales dentro de los grupos universales. De esta forma,

una modificación de los miembros de un grupo global no tendrá ningún impacto directo sobre los objetos de grupos universales mismos.

- Con respecto a la replicación de los grupos: en el pasado, la pertenencia a un grupo universal debía abordarse con precaución. En efecto, cualquier modificación de un grupo universal provocaba la replicación de todos los elementos pertenecientes al grupo en todos los catálogos generales del bosque. En la medida en la que un grupo universal puede contener un número significativo de miembros, una sola modificación podría generar una utilización importante del ancho de banda de red, sobre todo entre sitios.

- Cuando el bosque Active Directory se encuentra operativo en el nivel funcional Windows Server 2003, la replicación LVR (*Listed Value Replication*) se activa de forma automática y permite obviar las observaciones siguientes. En efecto, la replicación de las listas de valores permite evitar la réplica completa del atributo con todos sus valores, y replicar cada valor del atributo modificado de forma independiente.

Definición de una estructura de unidades organizativas

1. Rol de los objetos unidades organizativas

Una unidad organizativa es un objeto del directorio Active Directory. Este tipo de objeto container (o contenedor), es un objeto fundamental en todos los sistemas de directorio. De hecho, es utilizado de forma regular como contenedor de la estructura lógica.

Podemos colocar aquí un número casi ilimitado de objetos de clase usuario, inetOrgPerson, grupos, equipos y también otras unidades organizativas.

Observe que las unidades organizativas no pueden, por definición, contener objetos de su propio dominio y de ninguna manera objetos provenientes de otros dominios Active Directory.

Además, como contenedor privilegiado, la unidad organizativa podrá ser usada con facilidad para asumir las operaciones listadas a continuación:

- Las unidades organizativas permiten la implementación de un modelo organizado.
- Las unidades organizativas pueden contener objetos que estarán sujetos a la política de delegación aplicada a la unidad organizativa, y también de manera específica a través de las distintas autorizaciones aplicables directamente sobre los objetos.
- Las unidades organizativas permiten definir un verdadero modelo de administración mediante la utilización de objetos directivas de grupo para configurar todos los tipos de equipos así como los entornos de los usuarios.

En la medida en que los servicios de delegación y el enlace de objetos de directiva de grupo son utilizables en una extensión de tipo sitio o dominio y unidad organizativa, parece que las unidades organizativas son los contenedores más pequeños utilizables.

Los contenedores Builtin, Computers, ForeignSecurityPrincipals, LostAndFound, NTDS Quotas, Program Data, Systems y Users no son contenedores de tipo Unidad organizativa, sino objetos contenedor pertenecientes a otras clases específicas. Por consiguiente, no es posible vincular una directiva de grupo a este tipo de objetos. Como ya hemos dicho, los objetos de la directiva de grupo no se aplican a los objetos equipos y usuarios ubicados en sitios, dominios y en unidades organizativas.

Podemos descubrir la naturaleza de las clases presentadas antes activando el modo **Características avanzadas** y consultando la pestaña**Objeto** de cada uno de estos contenedores.

En resumen, debemos considerar la función de las unidades organizativas de la siguiente forma:

- Las UO representan unidades de administración separadas para que podamos delegar las autorizaciones en las UO y los objetos contenidos.
- Las UO representan el conjunto de configuraciones para los usuarios y los equipos ya que podemos vincular aquí los objetos de directivas de grupo.
- Además de estos dos puntos fundamentales, las UO son un buen medio para implementar un modelo de organización ya que podemos emplearlas para buscar objetos dentro del entorno Active Directory.

2. Utilización de las unidades organizativas en relación con la organización de la empresa

La «ubicación» de las tecnologías del directorio dentro de las empresas en un tema importante. En efecto, el papel central de estas tecnologías tiende a complicar su implementación en el núcleo del sistema de información. Sin embargo, poco a poco, la necesidad de gestionar la información de una forma mejor impone su uso. Además, ciertas aplicaciones y ciertos servicios empresariales, tales como la mensajería electrónica, los servicios de certificados o la implementación de autenticaciones de bosques, requieren un directorio empresarial como Active Directory.

Es de esta forma que los servicios de directorio Active Directory y el empleo de unidades organizativas pueden tener lugar dentro de la empresa de dos formas principales:

- Para empezar, el directorio puede desempeñar un papel técnico. Este enfoque significa que los equipos, servidores, usuarios y otras aplicaciones Windows pertenecientes a la infraestructura de Active Directory pueden utilizar los servicios del mismo.
- Por último, el directorio puede desempeñar un papel más cercano a la organización. Este enfoque tiende a hacerlo por completo dependiente de las posibles evoluciones de la estructura de la empresa, con el riesgo de debilitar la explotación y limitar su correcta utilización.

De esta forma, si intentamos establecer una estructura de unidades organizativas que represente la estructura organizativa de la empresa, es muy probable que este modelo no permita aprovechar al máximo la delegación y un despliegue sencillo de las directivas de grupo.

De partida, las recomendaciones de Microsoft basadas en los primeros grandes despliegues de Active Directory tendían a reflejar el modelo organizativo de la empresa. Pero, los primeros retornos empezaron a poner de manifiesto que este método tiene como principal inconveniente ralentizar el proceso de definición de la organización del directorio y por lo tanto, su eficacia a corto y mediano plazo.

En efecto, un modelo basado en la organización de la empresa requiere de muchas reuniones y de interminables debates. Además, la organización de la empresa no hará aparecer por necesidad las disparidades a nivel de ésta, lo que conduce a dejar innumerables zonas oscuras.

Hoy en día, el enfoque de Microsoft ha cambiado y ya no se tiene en cuenta el modelo de organización o de funcionamiento interno de la empresa, salvo para determinar el número de bosques y dominios en función de las diferentes entidades legales y/o jurídicas.

Por último, debemos tener en cuenta que las unidades organizativas disponibles dentro de los servicios de dominio Active Directory deben simplificar las operaciones realizadas por los administradores, permitir la aplicación de políticas de seguridad adecuadas y no deben ser utilizadas desde un punto de vista de la organización de la empresa.

Para ilustrar este enfoque, podemos recordar que los usuarios de un puesto de trabajo Windows 2000 miembro de un dominio Active Directory podían directamente recorrer el directorio de Active Directory a través del Explorador de Windows. Los sistemas Windows XP profesional y versiones posteriores han perdido esta posibilidad.

Para más información sobre la delegación de la administración, consulte **Active Directory Planning and deployment**, en el sitio Web de Microsoft (http://www.microsoft.com/).

Delegación de la autoridad de administración y uso de las unidades organizativas

La delegación de la administración nos permitirá asignar una serie de tareas administrativas a los usuarios y grupos seleccionados de manera adecuada. De esta forma, algunas operaciones básicas o simples podrán ser realizadas por los usuarios o grupos que no tienen por supuesto los privilegios de tipo administrador.

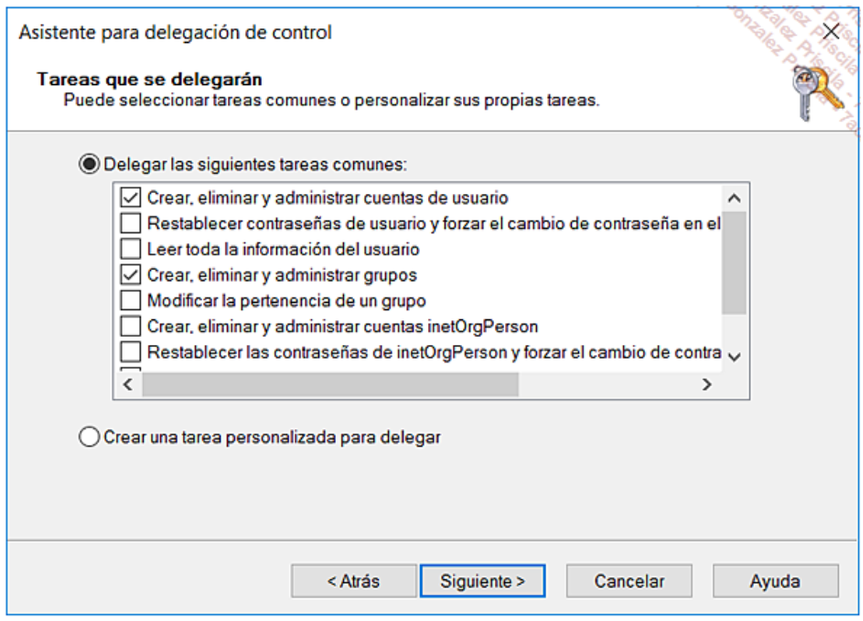
Procediendo de esta manera, los verdaderos administradores pueden dedicarse a la administración de los servicios de empresa incluidos en Active Directory o en la periferia de la infraestructura.

Otro aspecto importante es la "buena gestión" de los recursos. En efecto, ¿quién puede conoce mejor los permisos para conceder a los recursos que quien los ha creado de forma directa? El mismo usuario, ¡por supuesto!

Los servicios de delegación permiten al final liberar a los administradores de ciertas tareas que consumen un tiempo precioso a menudo y a las personas directamente responsables de ciertos recursos gestionar mejor los accesos. Por último, la delegación de la administración puede ser vista como una especie de "descentralización" del poder y puede beneficiar a un grupo mayor.

Entre las grandes operaciones que se refieren a la delegación de la autoridad ejecutiva sobre los objetos del directorio Active Directory, necesitaremos:

- Delegar el control administrativo dentro de un dominio de nuestro bosque mediante la creación de una jerarquía de unidades organizativas y delegando el control administrativo sobre algunas de estas unidades organizativas a los usuarios o grupos de usuarios de confianza.
- Tener en cuenta la estructura de su organización para decidir qué unidades organizativas y qué tipo de objetos deben o pueden ser delegados.
- Personalizar las consolas de gestión MMC para crear una versión personalizada y limitada de un componente como **Usuarios y equipos de Active Directory** o **Gestión del equipo**. La personalización de las consolas MMC se efectúa a través del **Asistente para nueva vista de cuadro de tareas...** el cual permite controlar las opciones ofrecidas a las personas para efectuar una delegación de la administración.
- Documentar las delegaciones efectuadas y asegurarse de que los usuarios a los que va a ser asignado el control sobre los objetos tienen el mínimo de conocimientos para realizar dichas operaciones.



Ejemplo de delegación simple sobre los objetos usuarios y grupos de usuarios

1. Estructura basada en la naturaleza de los objetos administrados

Una estructura basada en los diferentes tipos de objetos es en especial adecuada cuando se requiere delegar tareas administrativas en función de los tipos de objetos, lo que sucede a menudo. Por ejemplo, podemos proceder paso a paso de la siguiente manera:

- Creamos uno o varios grupos de seguridad para incluir a los usuarios o grupos que serán objeto de la delegación.
- Creamos una jerarquía de unidades organizativas adaptada a nuestra jerarquía de administración.
- En cada unidad de organizativa, insertamos los diferentes tipos de objetos a delegar.
- Delegamos las diferentes tareas de administración en las diferentes unidades organizativas de los grupos que deban disponer de dichas autorizaciones.

2. Estructura basada en las tareas de administración

Una estructura basada en las tareas delegadas a realizar se define en función de las diferentes tareas de administración. En este modelo, podemos proceder de la siguiente manera:

- Creamos uno o varios grupos de seguridad para incluir a los usuarios o grupos que serán objeto de la delegación.
- Creamos una jerarquía de unidades organizativas adaptada a nuestra jerarquía de administración. En este modelo, la jerarquía de unidades organizativas no será afectada por las tareas de administración. Sin embargo, este punto no es obligatorio y la estructura puede considerar otros criterios, tales como la organización de los objetos, las ubicaciones geográficas, la organización de la empresa, los tipos de objetos y los tipos de tareas de administración.
- En cada unidad organizativa, insertamos los diferentes tipos de objetos a delegar.
- Delegamos las tareas de administración sobre las diferentes unidades organizativas en los grupos que tendrán la delegación en función de la naturaleza de los objetos y las tareas asociadas a estos tipos de objetos. Para lograr una delegación de este tipo, podemos proceder de la siguiente manera:

En el **Asistente para delegación de control**, durante el paso **Tareas que se delegarán**, seleccione la opción **Crear una tarea personalizada para delegar**.

En la pantalla **Tipo de objeto de Active Directory**, seleccione la opción **Sólo los siguientes objetos en la carpeta**, y seleccione las categorías deseadas.

Por último, en la pantalla **Permisos**, seleccione los permisos solicitados.

3. Factores que deben integrarse en la definición de una jerarquía de unidades organizativas

Antes de definir con precisión la estructura de una jerarquía de unidades organizativas, es interesante hacer un balance de los contenedores por defecto. A continuación, identificaremos los factores de estructura más acertados que nos permitirán estudiar una estructura de unidades organizativas basada en diferentes modelos.

a. Con respecto a los contenedores por defecto

Todo dominio Active Directory contiene un conjunto genérico de objetos unidades organizativas y otros contenedores. De esta forma, en cada dominio Active Directory, encontraremos los siguientes elementos:

Builtin: el contenedor tiene los objetos que definen los grupos y cuentas de administración predefinidos por defecto. Encontraremos, por ejemplo, los grupos **Administradores**, **Opers. de cuenta**, **Opers. de impresión** o el grupo **Acceso compatible con versiones anteriores de Windows 2000**. La lista siguiente detalla todos los grupos propuestos por defecto con Windows Server 2016, su naturaleza y marco de utilización en un dominio bajo el nivel funcional Windows Server 2012 R2:

- Acceso compatible con versiones anteriores de Windows 2000 / Grupo de seguridad - Dominio local: un grupo de compatibilidad descendente que permite un acceso de lectura a todos los usuarios y grupos en el dominio.
- Acceso DCOM a Serv. de certif. / Grupo de seguridad - Dominio local: los miembros de este grupo están autorizados para conectarse a las autoridades de certificación de empresa.
- Administradores / Grupo de seguridad - Dominio local: los miembros del grupo Administradores disponen de un acceso completo e ilimitado al equipo y al dominio.
- Administradores de Hyper-V / Grupo de seguridad - Dominio local: los miembros de este grupo disponen de un acceso completo e ilimitado a todas las funcionalidades Hyper-V.
- Duplicadores / Grupo de seguridad - Dominio local: soportan la replicación de archivos en el dominio.
- Creadores de confianza de bosque de entrada / Grupo de seguridad - Dominio local: los miembros de este grupo pueden crear aprobaciones de en sentido de entrada para este bosque.
- Grupo de acceso de autorización de Windows / Grupo de seguridad - Dominio local: los miembros de este grupo tienen acceso al atributo tokenGroupsGlobalAndUniversal para los objetos Usuario.
- IIS_IUSRS / Grupo de seguridad - Dominio local: grupo integrado empleado por los servicios Internet (IIS).
- Invitados / Grupo de seguridad - Dominio local: los miembros del grupo Invitados disponen por defecto del mismo acceso que los miembros del grupo Usuarios, con la excepción de la cuenta Invitado que dispone de permisos restringidos.
- Lectores del registro de eventos / Grupo de seguridad - Dominio local: los miembros de este grupo pueden leer los registros de eventos a partir del equipo local.
- Operadores de asistencia de control de acceso / Grupo de seguridad - Dominio local: los miembros de este grupo pueden consultar de forma remota los atributos de autorización y los permisos de los recursos de este equipo.
- Opers. de impresión / Grupo de seguridad - Dominio local: los miembros pueden administrar las impresoras instaladas en los controladores de dominio.
- Operadores criptográficos / Grupo de seguridad - Dominio local: los miembros están autorizados para efectuar operaciones de cifrado.
- Opers. de cuentas / Grupo de seguridad - Dominio local: los miembros pueden administrar las cuentas de usuario y los grupos de dominio.
- Operadores de configuración de red / Grupo de seguridad - Dominio local: los miembros de este grupo pueden disponer de algunas autorizaciones de administración para la configuración de las funciones de red.
- Operadores de copia de seguridad / Grupo de seguridad - Dominio local: los miembros del grupo Operadores de copia de seguridad solo pueden evitar las restricciones de seguridad en con el objeto de efectuar la copia de seguridad y restauración de los archivos.
- Opers. de servidores / Grupo de seguridad - Dominio local: los miembros pueden administrar los servidores de dominio.
- Servidores de acceso remoto RDS / Grupo de seguridad - Dominio local: los servidores de este grupo permiten a los usuarios de los programas RemoteApp y de escritorio remoto virtuales acceder a los recursos. En los despliegues con acceso a través de Internet, estos servidores se despliegan por lo general en una red perimetral. Este grupo debe ser introducido en los servidores que ejecutan el servicio Broker para las conexiones de escritorio remoto. Los servidores de pasarela para los servicios de Escritorio remoto y los servidores de Acceso al escritorio remoto empleando la Web empleados en el despliegue deben formar parte de este grupo.
- Servidores de licencias de Terminal Server / Grupo de seguridad - Dominio local: los miembros de este grupo pueden actualizar las cuentas de los usuarios en Active Directory con información de la emisión de licencias, con el fin de seguir y de generar informes de utilización de licencias de acceso de clientes Terminal Server por usuario.
- Servidores de administración RDS / Grupo de seguridad - Dominio local: los servidores de este grupo pueden efectuar las acciones administrativas rutinarias en los servidores que ejecutan los Servicios de Escritorio remoto. Este grupo debe incluirse en todos los servidores de tipo Servicio de Escritorio remoto. Se debe incluir a los servidores que ejecutan RDS Central Management en este grupo.
- Servidores de extremo RDS / Grupo de seguridad - Dominio local: los servidores de este grupo ejecutan equipos virtuales y albergan las sesiones donde se ejecutan los usuarios, los programas RemoteApp y los escritorios virtuales personales. Este grupo debe ser introducido en los servidores Broker para las conexiones de escritorio remoto. Los servidores host de los servicios de Escritorio remoto y los servidores host de virtualización de los servicios de escritorio remoto empleados en el despliegue deben formar parte de este grupo.
- Storage Replica Administrators / Grupo de seguridad - Dominio local: los miembros de este grupo se benefician de un acceso total e ilimitado a todas las funcionalidades de Storage Replica.
- System Managed Accounts Group / Grupo de seguridad - Dominio local: los miembros de este grupo son administrados por el sistema.
- Usuarios / Grupo de seguridad - Dominio local: los usuarios no pueden hacer cambios accidentales o intencionales en todo el sistema. Por otra parte, pueden ejecutar la mayoría de las aplicaciones.
- Usuarios de administración remota / Grupo de seguridad - Dominio local: los miembros de este grupo tienen acceso a recursos WMI a través de los protocolos de gestión (tales como WS-Management a través del servicio Gestión remota de Windows). Esto no se aplica a los espacios de nombres de WMI que dan acceso al usuario.
- Usuarios del registro de rendimiento / Grupo de seguridad - Dominio local: los miembros de este grupo pueden acceder a los datos de los contadores de rendimiento a nivel local y de forma remota.
- Usuarios de escritorio remoto / Grupo de seguridad - Dominio local: los miembros de este grupo cuentan con los derechos necesarios para abrir una sesión remota
- Usuarios del registro de rendimiento / Grupo de seguridad - Dominio local. Los miembros de este grupo pueden planificar la grabación de los contadores de rendimiento, activar los proveedores de la ruta y recopilar los datos de eventos tanto a nivel local como a través de un acceso remoto al equipo.
- Usuarios COM distribuidos / Grupo de seguridad - Dominio local: los miembros están autorizados a ejecutar, activar y utilizar en este equipo los objetos COM distribuidos.

Computers: el contenedor incluye los objetos de equipo Windows, al igual que las cuentas de equipo creadas de forma original por las antiguas API NT que no funcionaban con Active Directory. Observe que el contenedor también se utiliza cuando los dominios Windows NT se

actualizan a Windows 2000 o Windows Server 2003. Al término de la migración de un dominio NT a Active Directory, todos los equipos miembro del dominio se encontraban almacenados en este contenedor. Observe a su vez que este contenedor no puede ser -renombrado o eliminado.

Domain Controllers: esta unidad organizativa contiene los objetos de equipo destinados a desempeñar el papel de controladores de dominio Windows Server. Las cuentas de equipo de los antiguos controladores de dominio Windows NT aparecen también en esta ubicación.

Users: este contenedor contiene las cuentas de usuarios y grupos creados de partida por las antiguas API Windows NT que no reconocían los servicios de dominio de Active Directory. Este contenedor se emplea a su vez cuando los dominios Windows NT se actualizan a Windows 2000 o Windows Server 2003. Al concluir la migración de un dominio NT a Active Directory, todos los usuarios miembro del dominio se encontrarán almacenados en este contenedor. Este contenedor no puede ser renombrado o eliminado.

LostAndFound: este objeto contenedor de la clase **LostAndFound** contiene los objetos donde los contenedores han sido eliminados en el momento en que un objeto hijo se ha creado. Cuando un objeto se crea en un lugar determinado o se traslada a éste y faltara en la replicación; el objeto perdido se añadirá al contenedor **LostAndFound**. El contenedor **LostAndFoundConfig** ubicado en la partición del directorio de configuración cumple el mismo rol para los objetos del bosque.

System: la carpeta **System** es un contenedor que contiene información crítica para todo el dominio Active Directory. Por ejemplo: este contenedor contiene los datos que conciernen a las directivas locales de seguridad, los -objetos TDO que representan las confianzas inter-dominio al igual que los puntos de conexión TCP y Windows Sockets. Aqui encontraremos los siguientes subcontenedores: AdminSDHolder, Default Domain Policy, Dfs Configuration, File Replication Service, FileLinks, IP Security, Meetings, MicrosoftDNS, Policies, RpcServices, WinsockServices,...

Ahora que tenemos una buena visión de los objetos a gestionar dentro de un entorno Active Directory, podemos abordar la continuación de este capítulo, siendo el objetivo definir una estructura de unidades organizativas óptima para minimizar las tareas de administración.

b. Criterios de ubicación, de operaciones y de tipos de objetos

Hemos visto antes que el mejor enfoque para la definición de una buena jerarquía de unidades organizativas depende en gran parte de la relación que debe existir entre el modelo a definir y la organización de la empresa, puntualizando que, precisamente, es muy recomendable desprenderse de este tipo de limitación para poder disfrutar plenamente de los servicios de seguridad, de delegación y de gestión ofrecidos a través de los servicios de dominio de Active Directory.

Una jerarquía de unidades organizativas bien construida debe permitir a los administradores construir un plan de delegación de la autoridad más sencillo de implementar. Para lograrlo, necesita en principio tener una buena percepción de las operaciones que se desea delegar y también a quién y qué objetos y/o tipos de objetos.

Por regla general, debemos garantizar un buen nivel de estabilidad de los primeros niveles de la jerarquía de unidades organizativas. Para lograrlo, definamos estos niveles en base a criterios fiables, estáticos y si es posible independientes de los parámetros de la empresa. Respetando al máximo estas pocas limitaciones, podemos protegernos de los efectos negativos generados por una reorganización interna de la empresa.

Podemos considerar los criterios más adelante como criterios estables utilizables para construir los primeros niveles de nuestra jerarquía de unidades organizativas:

- Consideremos las ubicaciones geográficas, edificios, pisos o zonas especiales de la red respetando la planificación de nombres ya establecidos y por lo tanto, bien conocidos por todos. El hecho de construir la jerarquía de unidades organizativas en función de las distintas ubicaciones vuelve a utilizar un modelo basado en las tareas de administración en función de las ubicaciones.
- Considere la naturaleza de las operaciones a delegar, tales como, por ejemplo, la creación, eliminación o modificación de las cuentas de usuario, el control de los miembros de grupo, o las cuentas de equipo. Puede tratarse también de tareas tales como la creación de objetos de directiva de grupo, filtros WMI, o solo los vínculos de directivas de grupo. Este tipo de modelo es muy interesante en la medida en que es independiente de la organización de la empresa donde las tareas genéricas serán casi siempre las mismas.
- Considerar la naturaleza de los objetos. Este tipo de enfoque se parece al modelo anterior basado en los tipos de operaciones de delegación.

Estas tres grandes familias de criterios nos permitirán definir los primeros niveles de una jerarquía de unidades organizativas. Ademas de estos criterios de estructura, podemos respetar los siguientes consejos:

- Si nuestra empresa se compone de varios dominios Active Directory, debemos asegurarnos de que los primeros niveles definidos para la definición del modelo de unidades organizativas sea lo más reutilizable posible. De esta forma, garantizamos una buena coherencia administrativa de los objetos dentro de los diferentes dominios.
- Por debajo de los primeros niveles que deben ser lo más genérico posible, las unidades organizativas de los niveles siguientes deben representar los niveles precisos en relación con las operaciones delegadas. Estas unidades organizativas también podrán utilizarse para ocultar objetos o para aplicar directivas de grupo.
- Para aprovechar de forma eficaz los servicios de delegación, no debemos complicar la estructura en demasía. Podremos controlar mejor los mecanismos de herencia en una jerarquía simple que no contenga más de una decena de niveles.

Para poner en práctica estos principios, podemos imaginar la estructura de unidades organizativas de la empresa *corpnet.priv*, como especificamos a continuación:

@Corporate: esta unidad organizativa contiene una jerarquía adaptada a las necesidades de la empresa.

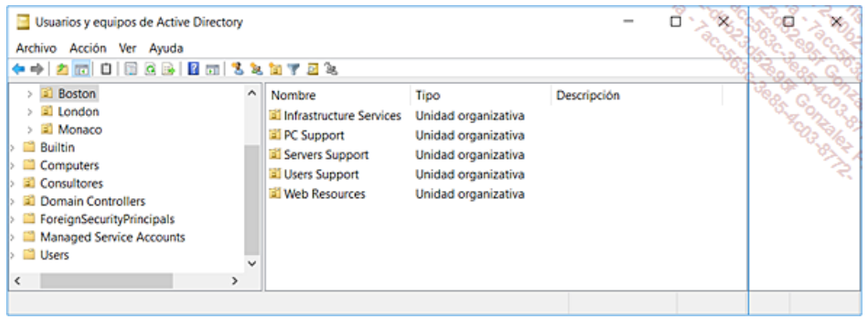
@Extranet Network: esta unidad organizativa contiene una jerarquía adaptada a las necesidades de la red Extranet. En el caso de una externalización de estos servicios, la gestión de la Extranet de la empresa puede delegarse en un proveedor de servicio "aprobado" y que cuenta con una delegación de la administración.

@Groups: esta unidad organizativa contiene todos los grupos que estaremos obligados a crear. El hecho de clasificar todos los grupos en este contenedor permite localizarlos de forma sencilla y tener así una visibilidad total de estos objetos sensibles usados para la asignación de las autorizaciones y permisos. Además, como los objetos de la directiva de grupo solo se aplican a objetos equipos y usuarios situados dentro de un ámbito extensión de la administración de tipo "Sitios / Dominios / UO ", el hecho de clasificar todos los grupos creados en una UO especial no tiene ningún efecto negativo en relación con la aplicación de las GPO.

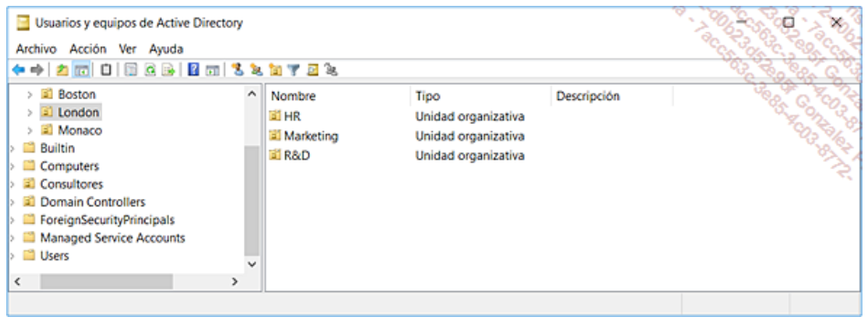
Managers & External Services: esta unidad organizativa contiene sólo las cuentas de servicio utilizadas por las aplicaciones así como las cuentas temporales que disponen de delegaciones. Este enfoque permite localizar de forma sencilla las cuentas utilizadas por las aplicaciones así como las cuentas externas que disponen de autorizaciones de forma temporal obtenidas a través de una delegación de la administración.

Subsidiary: esta unidad organizativa contiene los puntos de partida de las jerarquías que se dedicarán a las diferentes filiales de la empresa, si es necesario. Este enfoque se explica más adelante.

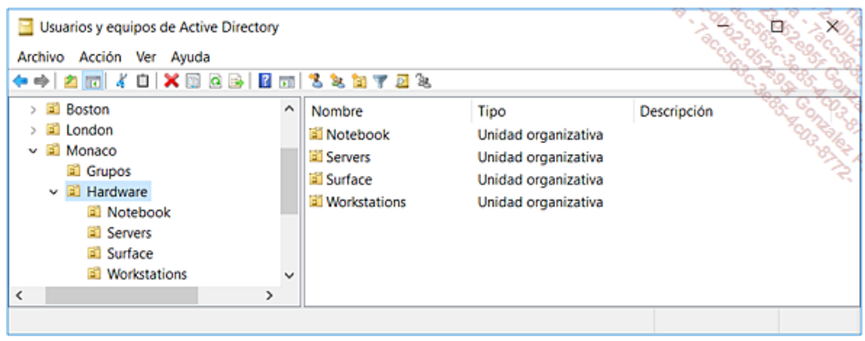
En cuanto a "The Boston Company": la unidad organizativa Boston contiene una jerarquía adaptada a las necesidades de la filial de Boston. Esta parte del dominio de Active Directory utiliza un modelo basado en la naturaleza de las tareas de administración delegadas. De hecho, un modelo que agrupa los objetos por su naturaleza se adapta de forma óptima.



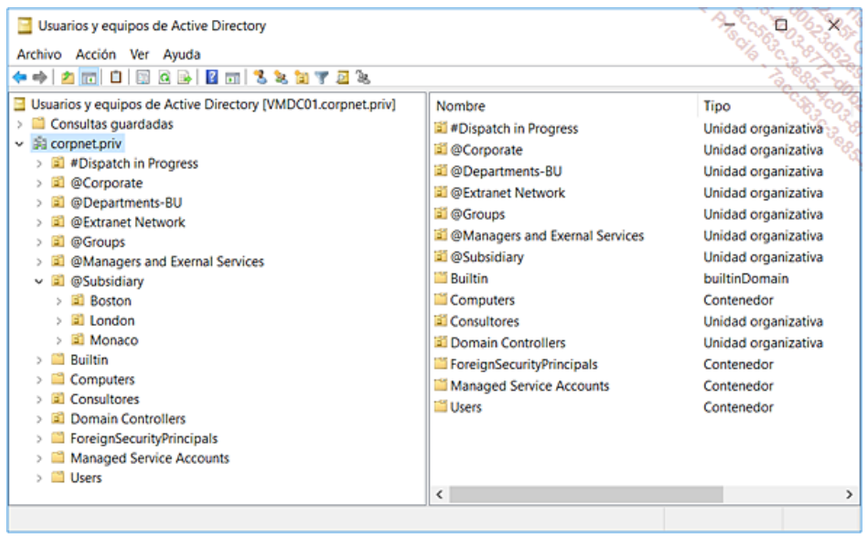
En cuanto a "The London Company": la unidad organizativa London contiene una jerarquía adaptada a las necesidades de la filial de Londres. Esta parte del dominio Active Directory utiliza un modelo basado en la organización de la empresa y luego en los tipos de objeto. Un modelo de este tipo permite referenciar a los departamentos de la empresa, utilizando los servicios de delegación en función de los diferentes tipos de objetos.



En cuanto a "The Monaco Company": la unidad organizativa Monaco contiene una jerarquía adaptada a las necesidades de la filial de Monaco. Esta parte del dominio Active Directory utiliza un modelo basado en las ubicaciones y luego en los tipos de objeto. Un modelo de este tipo permite hacer aparecer de forma clara las distintas ubicaciones geográficas, así como las categorías de objeto que utilice la delegación y quizá también las directivas de grupo.



La siguiente pantalla muestra una estructura de unidades organizativas que respeta estos principios fundamentales.



Jerarquía de unidades organizativas organización basada en diferentes criterios y modelos

En cuanto a "Dispatch In Progress": esta unidad organizativa desempeña el papel de zona temporal cuando los objetos deben ser creados de forma urgente, y la unidad organizativa que las acogerá no está todavía definida. Podemos en segunda instancia desplazar el equipo, el usuario o el grupo deseado a la unidad organizativa adecuada.

Uso de las unidades organizativas para las directivas de grupo

Más adelante estudiaremos en detalle el funcionamiento de las directivas de grupo. Sin embargo, la relación que existe entre los contenedores de tipo unidad organizativa y los objetos de la directiva de grupo es tal que no es posible olvidar las mejores prácticas que deben respetarse para la definición de una jerarquía de unidades organizativas y el correcto uso de las directivas de grupo dentro de la misma jerarquía.

Los objetos de la directiva de grupo son objetos de directorio Active Directory que permiten el despliegue de conjuntos de parámetros para los equipos y los usuarios. Gracias a estos objetos, podemos soportar mediante Active Directory todos los parámetros de registro, parámetros de seguridad, los scripts de inicio y cierre de sesión, la instalación y gestión de aplicaciones, la redirección de los directorios, la administración de cuotas de disco, la gestión de los parámetros de redes Wifi , las directivas de restricción de software, los parámetros AppLocker, los parámetros de claves públicas, los parámetros de directivas IPSec, los parámetros de Internet Explorer, los parámetros de QoS (*Quality of Services*), a los que habrá que añadir incontables parámetros ofrecidos a través de las extensiones de tipo GPP - *Group Policy Preferences*.

Sabemos que, por concepto, las directivas de grupo se aplican según el esquema L,S,D,UO. Este esquema significa que en primera instancia los parámetros locales del equipo se aplican (L para local), seguidos por los parámetros de las directivas de grupo del sitio (S para sitio), seguidos de los parámetros de las directivas de grupo del dominio (D para dominio), y por último los parámetros de las directivas de grupo de la jerarquía de unidades organizativas (UO para unidades organizativas).

Este principio exagerado de funcionamiento demuestra hasta qué punto es importante la estructura de unidades organizativas. Las directivas de grupo se aplican de arriba abajo y descienden la jerarquía gracias a las posibilidades de herencia, y de bloqueo de los mecanismos de herencia, de los servicios de directorio Active Directory.

Para más detalles sobre el funcionamiento y la delegación de las directivas de grupo o las operaciones correspondientes, consulte el capítulo Componentes de la estructura lógica que trata acerca de las directivas de grupo.

Reglas generales y mejores prácticas

Emplear al máximo las funcionalidades de herencia del directorio Active Directory y bloquear la herencia a nivel de un contenedor solo cuando sea necesario.

Utilizaremos un modelo basado en la organización si deseamos que los primeros niveles representen las distintas entidades, direcciones o centros de coste de la empresa. Cuando la empresa tiene una estructura complicada, este modelo permite construir de forma simple un plan de delegación de la administración que refleja con precisión la organización de la empresa. Sin embargo, este modelo puede presentar el siguiente inconveniente:

- Esta técnica depende de la organización y se ve afectada cuando la empresa está sujeta a una reorganización interna.
- Por otra parte esta estructura ya es conocida, y será por lo general aprobada por todos. Este punto no es un inconveniente y puede incluso considerarse como un certero beneficio.

Utilizar un modelo basado en las diferentes actividades de la empresa cuando una actividad se basta por sí misma y por tanto tiene una gran autonomía. Si la empresa parece estar compuesta por varias entidades muy autónomas, e incluso independientes, un modelo de este tipo suele resistir todas las reorganizaciones.

Verifique que los primeros niveles de la jerarquía no estén sujetos a cambios frecuentes. La idea es que en un bosque compuesto de varios dominios, siendo dos o tres de sus primeros niveles genéricos, respetarán las mismas normas de estructura. De esta forma, será fácil crear la misma estructura de partida en todos los dominios.

Utilizaremos los objetos unidad organizativa con moderación. Es una buena idea crear una unidad organizativa cuando se presenta uno de los tres casos siguientes:

- Es necesario establecer una delegación de administración.
- Queremos ocultar determinados objetos.
- Deseamos controlar la aplicación de las directivas de grupo empleando la fórmula L,S,D,UO.

Para más información sobre la delegación de la administración, consulte el documento **Active Directory Planning and deployment**, disponible en el sitio Web de Microsoft. También puede conectarse al sitio web de Microsoft Active Directory en la dirección http://www.microsoft.com/adds o buscar en el sitio Microsoft Technet « Understanding AD DS Design ».

Tecnología IntelliMirror

1. Introducción

La tecnología de gestión y administración IntelliMirror es un conjunto de potentes funciones desarrolladas para incrementar la disponibilidad de los sistemas y reducir el coste total de propiedad de los equipos que funcionan bajo Windows.

IntelliMirror llama a «directivas» para implementar los mecanismos de gestión de las modificaciones y de los cambios de configuración. De esta forma, la tecnología permite a los usuarios interactuar con una red mucho más dinámica. Los usuarios pueden de forma sencilla recuperar sus datos, su software y sus parámetros dentro de un entorno informático distribuido, estén conectados o no. La tecnología IntelliMirror se encuentra integrada de forma directa en el núcleo de los sistemas Windows y apareció con la primera versión de Active Directory con Windows 2000 Server y Windows 2000 Profesional.

Para beneficiarse de las nuevas características ofrecidas por la tecnología IntelliMirror, es obligatorio disponer de un entorno de dominio Active Directory y de puestos de trabajo funcionando con un sistema operativo cliente Microsoft Windows -sea cual sea la versión desde Windows 2000 Profesional hasta Windows 10 y futuras versiones. Los sistemas operativos antiguos tales como Windows NT, Windows 9x o incluso las versiones más recientes de Unix, Linux o los equipos Apple que funcionan bajo Mac OS no soportan las tecnologías Microsoft IntelliMirror, incluso si podemos utilizar los componentes cliente Samba para conectar estos sistemas a Active Directory.

Observación: hablaremos con frecuencia en este capítulo de equipos de tipo Windows o clientes Windows. Esta denominación se refiere a los equipos Windows 7, Windows 8, Windows 8.1, Windows 10, así como los sistemas operativos Windows Server asociados tales como Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016. Cuando sea necesario se especificarán las versiones para ofrecer mayor claridad.

IntelliMirror se articula en torno a tres funciones principales:

- La gestión de los datos de los usuarios.
- La gestión de los parámetros de los usuarios y equipos.
- La instalación y mantenimiento del software para los usuarios y también para los equipos.

Por supuesto, podemos utilizar todos o parte de estos servicios en función de las necesidades de los diferentes grupos de la empresa.

2. Aportaciones a la empresa

Como las funciones IntelliMirror se implementan a través de los componentes integrados en el sistema operativo Windows y en el núcleo de los servicios de dominio Active Directory, la tecnología puede utilizarse de forma independiente del tamaño de las redes. De esta forma, si los métodos de administración y gestión de los cambios de configuración evolucionan, entonces será posible disponer de un entorno a la vez seguro y controlado.

En efecto, a partir del momento en que los parámetros de gestión y configuración ya no se encuentran definidos de forma directa en los equipos cliente de la red, sino en las "directivas" facilitadas por el directorio Active Directory, entonces el puesto de trabajo "pesado" se convierte en un puesto de trabajo "controlado", e inteligente.

La tecnología IntelliMirror es una solución distribuida donde los clientes inteligentes de la red interactúan con los servicios de infraestructura de Active Directory puestos a su disposición. Aunque es posible integrar en Active Directory los terminales de tipo Windows Embedded, debemos tener en cuenta que estos clientes disponen de funcionalidades IntelliMirror limitadas.

IntelliMirror permite una gestión de los cambios y modificaciones de configuración basada en dos grandes tipos de directivas:

- Las directivas locales: todos los equipos que funcionan con Windows tienen una directiva local, ya se trate de equipos miembro de un dominio o de equipos autónomos. Descubriremos más adelante que cuando un equipo es miembro de un dominio Active Directory, entonces las directivas derivadas del dominio prevalecen sobre la directiva local.

En sistemas Windows Cliente y Windows, la directiva local se almacena de forma local en el equipo en el directorio %Systemroot%\system32\GroupPolicy.

- Las directivas de grupo: una directiva de grupo permite aplicar de forma centralizada y uniforme a los grupos de usuarios y/o grupos de equipos las limitaciones de gestión y las normas vigentes en la empresa. Un grupo corresponde a un conjunto de objetos almacenados en el directorio Active Directory. La gestión centralizada de varios usuarios y equipos permite reducir de forma considerable el tiempo y esfuerzo de gestión de un administrador. Una vez implementada una directiva de grupo, el sistema puede aplicarse de manera cíclica y casi por completo dinámica, sin que sea necesaria ninguna intervención posterior.

¿Directivas locales o directivas de grupo? La tecnología de gestión y de cambio de configuraciones tiene por objeto gestionar el ciclo de vida de los equipos y usuarios. Dicha gestión podrá en función de las necesidades usar a veces directivas locales, a veces directivas de grupo. También podemos utilizar una mezcla de ambos tipos de directivas y así definir los parámetros y las posibilidades que se destinarán a los usuarios o a los equipos. Las directivas locales se definen en un equipo local, mientras que las directivas de grupo se configuran y aplican a conjuntos de usuarios o de equipos, a través de los servicios de dominio de Active Directory. Las directivas de grupo permiten a IntelliMirror centralizar y simplificar la gestión de los cambios y la configuración.

Las directivas de grupo se denominan en inglés "GPO de *Group Policy Object*". Tenga en cuenta que este término se usa de forma regular en la literatura de Active Directory.

Podemos utilizar un equipo en modo no conectado o en modo conectado. Será por supuesto el caso de utilización de ordenadores portátiles. Los usuarios podrán, en función de sus actividades, pasar regularmente de un modo a otro en el transcurso del día.

Beneficios para la empresa

Uno de los principales beneficios para la empresa es una mejora de productividad de los usuarios. La idea es que el equipo se encuentre disponible la mayor parte del tiempo, más eficaz, y también lo más autónomo posible dentro de la infraestructura de la que forma parte. Con la iniciativa ZAW (*Zero Administration for Windows*) lanzada por Microsoft en 1996 con NT 4.0 y el Zero Administración Kit -llamado Zak, que era un conjunto de herramientas de gestión y procedimientos- desde la primera versión de Active Directory en Windows 2000 Server y los primeros puestos de trabajo bajo Windows 2000 Profesional. IntelliMirror permitió y todavía permite con Windows 10, una gestión completa de la administración y de la seguridad dentro de la infraestructura de Windows.

Beneficios para los usuarios

El usuario puede aprovechar la mejor parte de su equipo. Este se encuentra tanto disponible como fiable, tanto desde el punto de vista del

hardware como el software que lo soporta. Los parámetros del equipo y los datos de usuario se mantienen siempre, ya sea en modo conectado o no. Estas pequeñas mejoras proporcionan grandes servicios mejorando la disponibilidad de datos y entorno de trabajo. Además, como esas funciones son sencillas de usar, son transparentes para los usuarios. Los usuarios pueden abrir una sesión en cualquier equipo y acceder a sus propios datos y aplicaciones sin necesidad de saber donde se encuentran estos datos de forma física (uso del servicio DFS-N, replicación DFS-R, acceso a directorios sin conexión, uso de perfiles de usuario, instalación y mantenimiento de software a través de los servicios de gestión de software, instalación de actualizaciones y parches de Windows a través de los servicios WSUS - *Windows Server Update Services*).

3. Evoluciones aportadas a las GPO para los clientes Windows 7

Los sistemas operativos Windows Cliente tales como Windows 7, Windows 8.x y Windows 10 incorporan nuevas funcionalidades que hacen avanzar los mecanismos relacionados con la infraestructura de las directivas de grupo, mejoran la detección de red y ofrecen una mayor capacidad de gestión para los administradores.

Desde fuera, los grandes principios introducidos por Active Directory y Windows 2000 siguen siendo válidos, pero con Windows 7 y las versiones posteriores, Microsoft proporciona una importante evolución de la infraestructura de las directivas de grupo. En Windows Server 2003 y Windows XP Profesional, el tratamiento de las directivas de grupo se desarrolla mediante el proceso Winlogon.

En estas plataformas, Winlogon es un componente a cargo de muchas funciones tales como el inicio de la sesión local y las operaciones relativas a las directivas de grupo. Con Windows 7 y versiones posteriores, las directivas de grupo disponen de un servicio de tratamiento dedicado. Además, el tratamiento y la aplicación de las directivas se ve reforzado de tal manera que es imposible detenerlo o que un administrador pueda tomar posesión de los permisos establecidos en la directivas de grupo para desactivarlo. Todos estos cambios mejoran la fiabilidad global del motor de la directiva de grupo reforzando la infraestructura de seguridad en su conjunto.

a. Mejora de la detección de red (Network Location Awareness)

Con los puestos de trabajo Windows 7 hasta Windows 10, los mecanismos de gestión de las directivas de grupo determinan la naturaleza del vínculo de red (vinculo lento o vinculo rápido). En función del vínculo, esta información se emplea para seleccionar los parámetros de la directiva a aplicar. Este método todavía se encuentra vigente, sin embargo, el método de cálculo para determinar el ancho de banda se ha modificado de forma radical. En las antiguas plataformas, la determinación de la velocidad utilizaba el envío de paquetes ICMP (*Internet Control Message Protocol*) a los controladores de dominio. Si la idea es buena de partida, en la práctica varios problemas surgen a lo largo del tiempo y de hecho hoy en día, es cada vez más frecuente, que el soporte de los mensajes ICMP esté desactivado en los controladores de dominio para detener las respuestas ICMP. Luego, cuando la conexión se establece a través de enlaces de alta latencia, como los enlaces vía satélite, los cálculos pueden ser erróneos. En estas situaciones, no es posible garantizar que el vínculo sea lo bastante rápido.

Otro problema de los sistemas que operan con versiones antiguas de Windows como Windows XP Profesional atañe a la falta de capacidad de dichos sistemas para reconocer el modo suspensión o hibernación. Es por esto necesario la posibilidad de actualizar las directivas de grupo antes de la salida del estado de suspensión o hibernación, o simplemente cuando el equipo se conecta después de una ausencia prolongada.

Los sistemas que trabajan con Windows 7 hasta Windows 10 actualizan los parámetros de conectividad de red en tiempo real. La principal modificación se refiere al motor de las directivas de grupo, que ahora usa el gestor NLA (*Network Location Awareness*). Los componentes del servicio NLA alertan al motor de las directivas tan pronto como un controlador de dominio está disponible y desencadenan, si es necesario, un refresco de las directivas de grupo.

b. Directivas locals múltiples (LGPO)

Por norma, las directivas locales se utilizan para permitir a los administradores de los equipos Windows configurar los parámetros de seguridad o de registro en estos equipos, cuando una infraestructura de GPO no está disponible. En general, este caso se produce en las equipos de tipo "quiosco" (equipos de autoservicio), equipos situados en entornos públicos o incluso equipos de prueba o demostración que no forman parte de un dominio Active Directory.

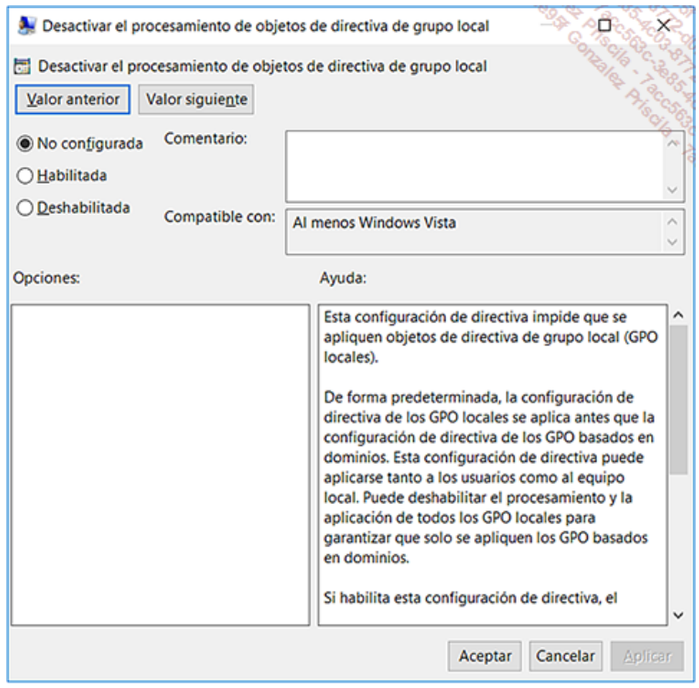
El límite de las directivas locales reside en el hecho de que las plataformas basadas en Windows 2000 como Windows XP y Windows Server 2003 solo soportan una directiva local, este punto es especialmente problemático cuando es necesario administrar parámetros diferentes para diferentes usuarios.

Las versiones siguientes del sistema operativo Windows corrigen esta limitación, permitiendo la creación de varias directivas de grupo locales, LGPO, *Local Group Policies Objects*, aplicables a las entidades siguientes:

- Cualquier usuario local del equipo, especificado por su nombre.
- Los usuarios miembros del Grupo Administradores del equipo local.
- Los usuarios no miembros del Grupo Administradores del equipo local.

¡Observe! Un usuario dado solo se ve afectado por una de las directivas locales presentadas antes, en función de la declaración hecha. Además, conviene precisar que cuando el equipo Windows forma parte de un dominio Active Directory, las directivas de grupo se aplicarán, respetando el orden Sitio / Dominio / UO, y siguen siendo prioritarias sobre los parámetros declarados de forma local.

Tenga en cuenta que en el caso de que sea conveniente impedir el uso de esta nueva funcionalidad, los administradores tienen la posibilidad de desactivar el funcionamiento de los LGPO en equipos Windows Vista, como mínimo.



Activación / desactivación de los objetos de directivas de grupo locales

La imagen anterior muestra la posibilidad de desactivar esta nueva funcionalidad cuando se espera que no pueda ser utilizada.

c. Mejor gestión de los mensajes de eventos

Los clientes Windows están equipados con un sistema de registro de eventos. El motor de directivas de grupo opera este sistema de registros Windows Eventing fraccionando los eventos en dos partes. La parte utilizada por el registro del sistema incluirá los problemas de directivas de grupo, mientras que la parte que utiliza el diario de aplicaciones es específica de las diferentes directivas de grupo, y almacenará los eventos operacionales. Este nuevo sistema sustituye el voluminoso archivo de solución de problemas userenv.log.

d. Antiguos ADM y nuevos ADMX

En las versiones de Windows anteriores a Windows 7, la creación de un nuevo objeto GPO genera un conjunto de archivos ADM que representan alrededor de 5 MB. En consecuencia un importante número de objetos GPO supondrá la creación de un gran número de archivos idénticos en el SYSVOL, los cuales serán replicados por necesidad en los diferentes controladores de dominio del dominio.

Las directivas de grupo introducidas con Windows 7 y Windows Server 2008 aportan una respuesta a esta problemática introduciendo un nuevo formato basado en XML para los archivos de definición de directivas: los archivos ADMX. Cabe señalar también que los archivos ADMX (nuevo formato de archivos para las plantillas administrativas a partir de Windows 7) ya no dependen del idioma y van acompañados de un archivo ADML (archivo que contiene datos específicos de los idiomas utilizados por la consola de gestión de directivas de grupo de Windows 7 o versiones posteriores).

Además del cambio de estructura de archivos, el nuevo formato ADMX soporta el almacén central. Este nuevo espacio de almacenamiento de objetos GPO evita la replicación de información duplicada y facilita la actualización de un archivo ADMX dado en un solo punto. Los administradores que definen las directivas de grupo a partir de un puesto de administración Windows tienen acceso de forma automática a los nuevos archivos ADMX actualizados en el almacén central replicado en los controladores de dominio.

A modo de ejemplo, Windows 7 y Windows 10 disponen de forma respectiva de 130 y 191 archivos ADMX para reemplazar a los seis u ocho archivos ADM proporcionados en las versiones anteriores de Windows.

Estos archivos se almacenan en el directorio C:\Windows\PolicyDefinitions, mientras que los archivos de lenguaje ADML se almacenan en un subdirectorio específico del idioma (por ejemplo es-ES para España y en-US para el idioma inglés/Estados Unidos).

Es importante tener en cuenta que los sistemas Windows 7 y versiones posteriores de Windows almacenan los parámetros de las directivas de grupo de manera diferente. Los nuevos archivos ADMX reemplazan a los antiguos archivos ADM ofreciendo muchas nuevas posibilidades, tales como la carga dinámica, el soporte de varios idiomas, así como la posibilidad de centralizar los modelos en los controladores de dominio.

¡IMPORTANTE! Las plataformas Windows Client y Windows Server siguen soportando los antiguos formatos de modelos basados en los archivos ADM. Sin embargo, Microsoft promueve la conversión de archivos ADM al nuevo formato ADMX empleando la herramienta **ADMX Migrator** disponible de forma gratuita en el sitio de Microsoft. Esta herramienta funciona en todas los equipos Windows Cliente y Windows Server y requiere la consola MMC 3.0 y la instalación previa de Microsoft .NET 2.0.

e. Windows 10 soporta muchas nuevas categorías

En comparación con Windows 7 Profesional, Windows 10 añade alrededor de cien parámetros de directivas de grupo. Entre estas evoluciones, las más interesantes se centran en los parámetros de redes cableadas e inalámbricas, los parámetros del firewall de Windows en modo avanzado, los parámetros IPSec, los parámetros de Gestión de impresoras al igual que los de Desktop Shell, la asistencia remota y otras funciones Tablet PC. Cabe destacar también, la gestión de las unidades de almacenamiento extraíbles, la gestión de la energía, el control de las cuentas de usuario, la gestión de los informes de errores de Windows, la protección acceso a la red y los parámetros de Windows Defender.

¡Observe! Para crear o modificar los GPO que utilizan los parámetros de Windows 10, debemos usar por fuerza un equipo con Windows 10, o un servidor Windows Server 2016. De hecho, algunas funcionalidades soportadas por las versiones de Windows Cliente requieren el uso de un puesto que funciona sobre la versión equivalente o la más moderna de Windows Client. Esto es especialmente cierto con respecto a las preferencias de las directivas de grupo - en inglés GPP para *Group Policy Preferences*. Por ejemplo, para modificar los parámetros de GPP para IE 10 o IE 11, es necesario realizar las operaciones en un sistema operativo cliente que funcione como mínimo con Windows 8.1 Professional - y esto, a pesar de la adición de las plantillas de administración ADMX para Windows 10.

Como podemos ver, Windows Vista modernizó de manera importante los objetos GPO y la manera de gestionarlos. Incluyen un mayor número de parámetros configurables para aumentar el control y la seguridad de los sistemas.

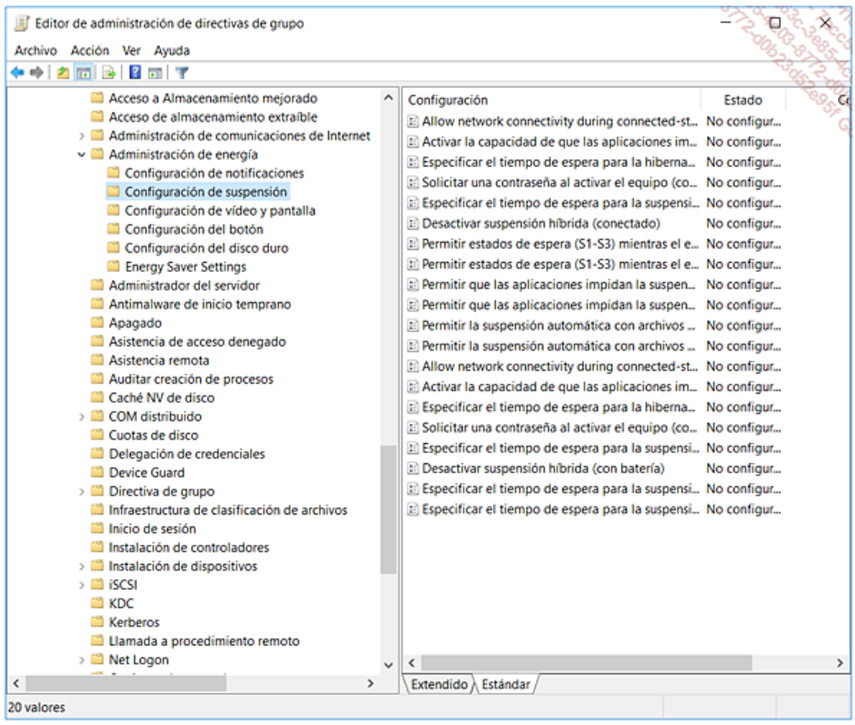
4. Novedades introducidas en los puestos cliente mediante la evolución de las directivas de grupo de Windows Server 2016

Como es costumbre, las últimas versiones de los sistemas operativos de la familia Windows Server aportan componentes y archivos de configuración necesarios para la administración de los clientes del mismo nivel. De esta forma, Windows Server 2016 permite un manejo más rico de los puestos de trabajo Windows 10. Nuevas categorías están surgiendo, las cuales nos permitirán aprovechar mejor los avances y progresos realizados.

Entre éstas, podemos señalar los puntos siguientes:

a. Gestión centralizada de los parámetros de administración de energía

Esta funcionalidad permitirá, sin lugar a dudas, ahorros considerables en las redes de todos los tamaños.

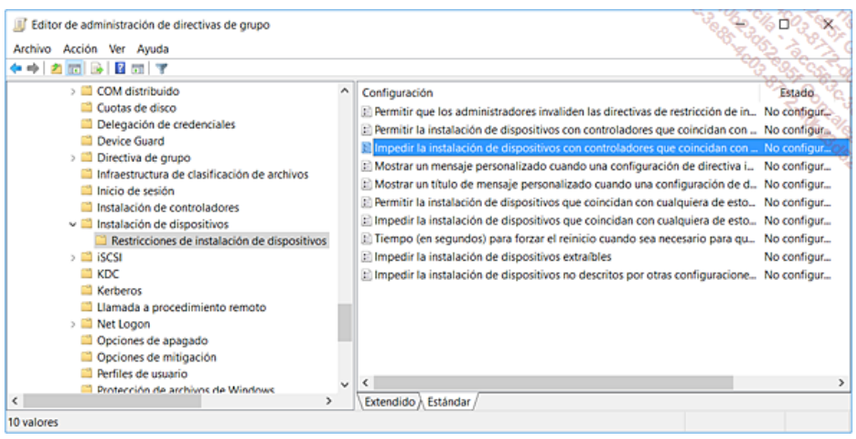


Los parámetros de administración de energía se soportan empleando las directivas de grupo de Windows Server 2008 R2

Varias decenas de parámetros permiten una administración totalmente centralizada, gracias a las directivas de grupo. Estos parámetros se gestionan empleando la Consola GPMC y situados en un objeto GPO en la siguiente ubicación: **Configuración del equipo - Directivas - Plantillas administrativas - Sistema - Administración de energía**.

¡Observe! Estos parámetros solo se refieren a los puestos de trabajo Windows 7 y versiones posteriores y no a los sistemas Windows XP Professional.

b. Posibilidad de gestionar las instalaciones de dispositivos USB no autorizadas, así como la delegación de la instalación del controlador de impresión a algunos usuarios



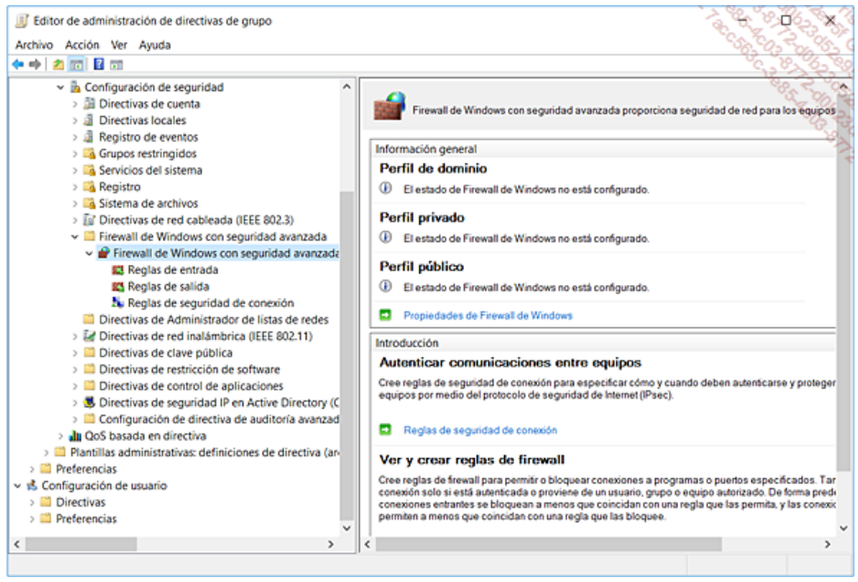
Restricción de instalación de dispositivos

La gestión centralizada de las restricciones de funcionamiento de los dispositivos USB nos permite crear políticas adecuadas para los distintos tipos de dispositivos tales como discos y llaves USB, lectores y grabadoras de CD y DVD-RW. Estos parámetros están en la siguiente ubicación:**Configuración del equipo - Directivas - Plantillas administrativas - Sistema - Instalación de dispositivos - Restricciones de instalación de dispositivos**.

¡Observe! Estos parámetros solo se refieren a los puestos de trabajo Windows 7 y versiones posteriores y no a los sistemas Windows XP Professional.

c. Mejoras en los parámetros de seguridad

Las directivas de seguridad reúnen a partir de ahora todos los parámetros IPSec y del cortafuegos. Esta racionalización de la interfaz es más coherente con los escenarios de despliegue.



Integración del Firewall de Windows con funciones avanzadas de seguridad

Además los nuevos asistentes permiten una aplicación más rápida de las configuraciones de tipo aislamiento dentro de un dominio Active Directory.

d. Mejor gestión de los parámetros relacionados con Internet Explorer

En las plataformas antiguas que funcionaban con Windows XP, podía darse el caso de que los parámetros utilizados en el equipo local tuvieran prioridad sobre los parámetros contenidos en un objeto GPO. Este tipo de incidente podía en particular darse en la edición de los parámetros de Internet Explorer contenidos en un objeto GPO. En adelante, Windows 7 y versiones posteriores como, por ejemplo, Windows 10, no permiten este tipo de alteración de parámetros.

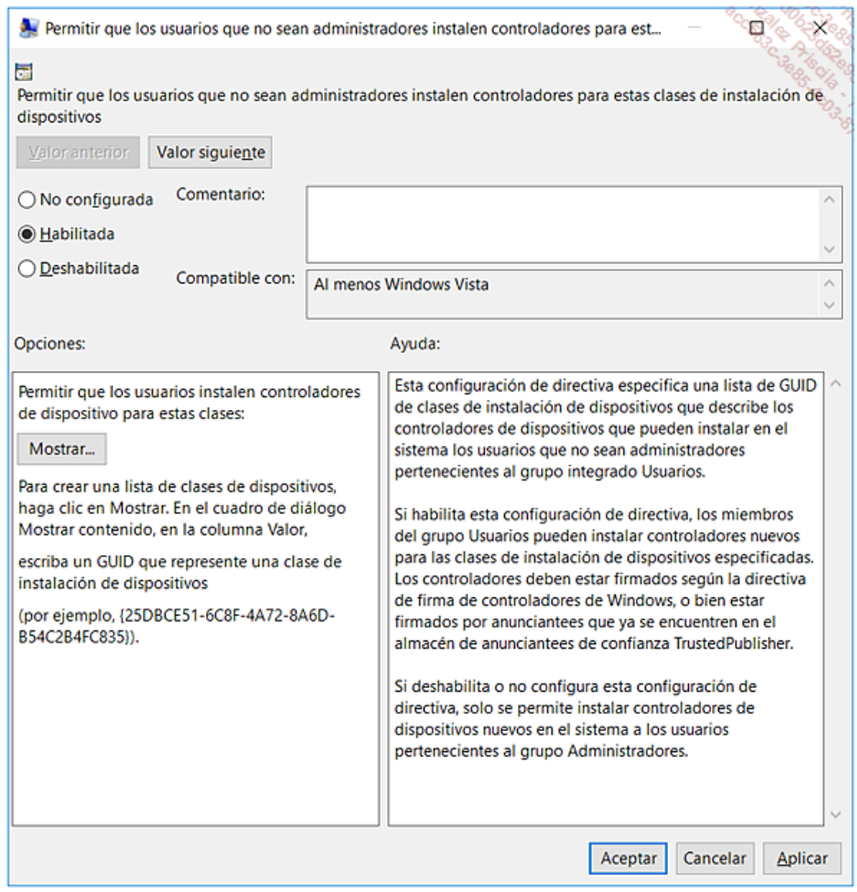
e. Asignación de impresoras en función del sitio Active Directory

Las directivas de grupo permiten hacerse cargo de la problemática de las conexiones a las impresoras en los entornos a los que los usuarios se desplazan. Prestar atención al hecho de que el nuevo emplazamiento no se conocerá hasta que se haya completado el ciclo de refresco del objeto directiva de grupo.

Estos parámetros están disponibles como parámetros de equipo y de usuario. Estos parámetros están en la siguiente ubicación: **... / Directivas / Plantillas administrativas / Impresoras**.

f. Delegación de la instalación del controlador de impresión a través de los GPO

Los administradores pueden delegar en los usuarios la posibilidad de instalar controladores de impresión. Esta característica reduce la necesidad de proporcionar a los usuarios privilegios de tipo "administrador". No obstante, conviene señalar que esta característica solo está soportada a partir de Windows 7 y versiones posteriores.



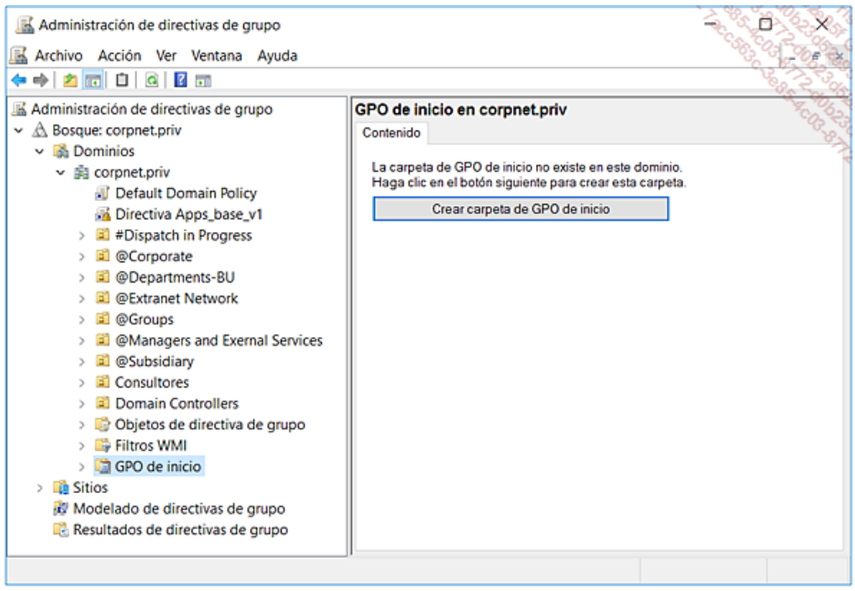
Instalación de nuevos controladores para las clases de dispositivos especificados

¡Observe! Esta directiva requiere que los controladores de dispositivos estén firmados. Los controladores no firmados no se ven afectados

por este parámetro y deberán ser instalados, como de costumbre, por los administradores. Estos parámetros están en la siguiente ubicación: **Configuration del equipo - Directivas - Plantillas administrativas - Sistema - Instalación de controladores**.

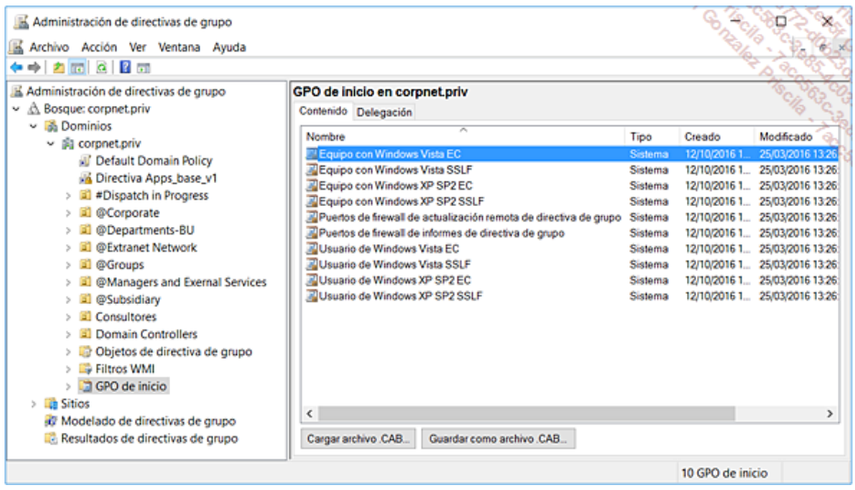
g. Nuevos objetos GPO Starter

Con Windows Server 2008 R2, Windows 7 y versiones posteriores, la gestión de los objetos de directivas de grupo es mucho mejor para la creación de plantillas de directivas de grupo llamados GPO Starter. Así, podemos crear una biblioteca de GPO, los cuales se utilizarán luego como plantillas o como punto de partida.



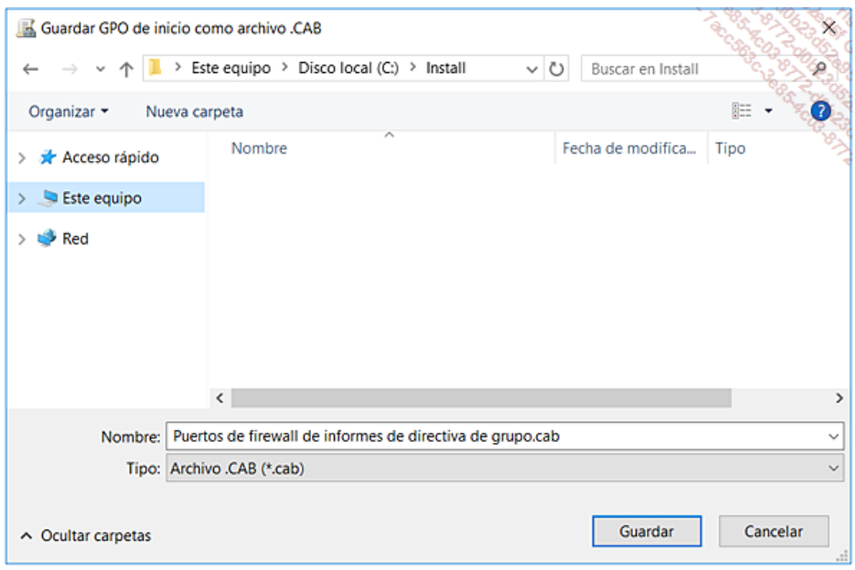
Creación de la carpeta de los objetos GPO Starter

Una vez creado el almacenamiento, entonces será posible crear nuevos objetos GPO Starter, sabiendo que su único objetivo es servir de plantilla para las directivas de grupo.



Lista de objetos GPO Starter por defecto

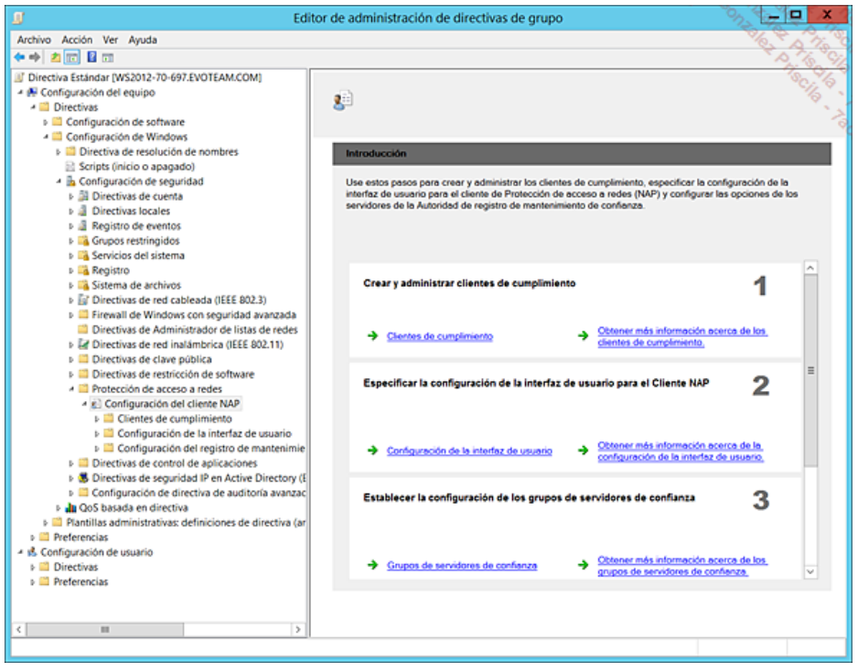
Una vez creada nuestra colección de plantillas en función de nuestras necesidades, no queda más que crear objetos de directiva de grupo basados en estas plantillas empleando la opción **objeto Starter GPO source**. Por último, cabe señalar que es posible utilizar la opción**Guardar como archivo CAB...** para transportar un objeto GPO Starter a otro entorno de Active Directory. La importación/exportación se facilita al incluir en un único archivo .cab, todos los archivos que constituyen el objeto directiva de grupo.



Export de un GPO Starter para importar en otro dominio

h. Parámetros del Protocolo NAP - Network Access Protection

El protocolo NAP es una tecnología que permite a los administradores determinar bajo qué condiciones algunos equipos obtendrán acceso a la red de la empresa. Podrá, por ejemplo, ser el caso en que un ordenador portátil con anti-virus, anti-spyware o firewall presenta errores de configuración que se consideran peligrosos. En base a los defectos de configuración detectados por el cliente NAP, éste podrá tomar la iniciativa de corregir el problema permitiendo al equipo ponerse en contacto con un servidor de "remediation". Las directivas de grupo de Windows 7 hasta Windows 8.1 integran el conjunto de parámetros de configuración NAP del puesto de trabajo, ya que permiten especificar los diferentes parámetros de cifrado a los servidores de tipo *"Health Registration Authority"*.



Configuración del cliente NAP con Windows 7, 8 y 8.1

¡Observe! Los componentes NAP se implementan en los puestos Windows Cliente de Windows XP hasta Windows 8.1 a través de un servicio y parámetros controlados por GPO. La parte servidor se implementa en los servidores Radius NPS Windows Server 2008 R2, 2012 y 2012 R2 pero no en los servidores que utilizan Windows Server 2016, ya que la funcionalidad NAP se retiró de la misma manera que en Windows 10. Este anuncio forma parte de una estrategia a largo plazo donde otras tecnologías están en fase de desarrollo y se integrarán en las próximas versiones de Windows Client y Windows Server.

5. Preferencias de las directivas de grupo de Windows Server 2016

Con los servidores Windows Server 2008 y Windows Server 2008 R2 apareció un nuevo espacio de gestión dentro de las directivas de grupo. Este nuevo espacio denominado "Preferencias" -en inglés GPP para *Group Policy Preferences*- permite a los administradores configurar, instalar, administrar y gestionar todos los parámetros del sistema y aplicaciones que no eran capaz de gestionar utilizando las directivas de grupo. Antes de la disponibilidad de los objetos GPP, el Administrador debía complementar los parámetros distribuidos a través del GPO creando scripts de arranque o inicio de sesión. A partir de Windows 7 y gracias a las nuevas Preferencias de las directivas de grupo, no es necesario desarrollar scripts complejos para realizar funciones sencillas y básicas, como las conexiones de red o impresoras, la planificación de las tareas de mantenimiento o incluso configurar los detalles o el contenido del menú **Inicio** al igual que cualquier otro parámetro de entorno como Internet Explorer, los parámetros regionales o incluso cualquier clave de registro o archivo de configuración.

En vez de integrar los parámetros directamente en la imagen de referencia o de su creación a través de un script, no siempre fácil de mantener en función de la evolución de los sistemas, el entorno de usuario y aplicaciones, Microsoft recomienda utilizar las nuevas "Preferencias". Los scripts serán utilizados como último recurso, cuando no sea posible realizar una operación de configuración especial, ni por las directivas de grupo, ni por las opciones de Preferencias.

a. ¿Preferencias o directivas de grupo?

Las preferencias de directivas de grupo son complementarias a las directivas de grupo. Para poder beneficiarnos de las preferencias de directivas de grupo es crucial comprender el concepto de complemento entre ambas. El cuadro siguiente ubica las dos tecnologías lado a lado.

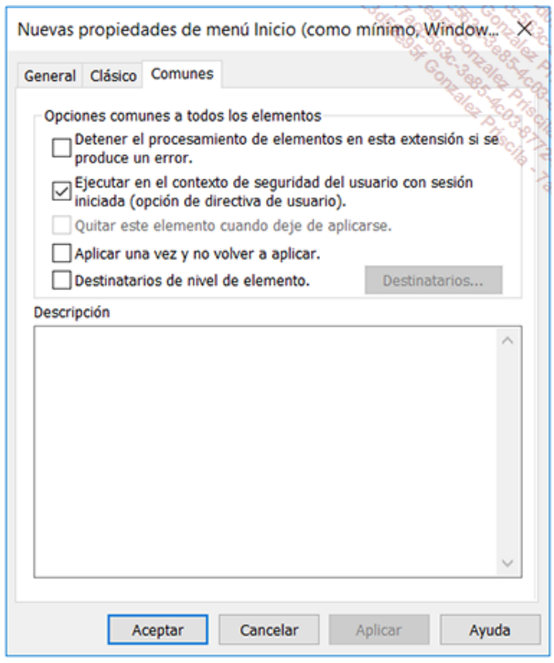
	Preferencias de directivas de grupo	**Objetos de directiva de grupo**
Método de aplicación y refresco	Se aplican, ver reaplicar. No desactivan la interfaz. Pueden aplicarse una sola vez o reaplicadas mediante refresco.	Se aplican, ver reaplicar. Desactivan la interfaz. Mediante refresco.
Flexibilidad	Creación simple de ítems: conexiones, iconos y carpetas, archivos... Importación de claves y ramas para el registro. Actualización de los archivos de configuración. Importación de parámetros de registro en local o de forma remota.	La adición de parámetros requiere que la aplicación utilice el Registro, además de la creación de plantillas de administración. No pueden gestionar el contenido de los archivos, carpetas...
Directiva local	Ninguna preferencia con las directivas locales.	Soportados a través de una directiva local (Local GPO).
Dependencias	Soporta aplicaciones no diseñadas para utilizar las GPO.	Requiere aplicaciones que soportan las GPO.
Almacenamiento	Borrado de los parámetros originales. No restauración de los parámetros en caso de eliminación de las preferencias.	Los parámetros originales no son alterados. Los parámetros están bajo la clave \Policy. La supresión de una directiva de grupo restaura los parámetros originales.

Selección y Filtrado	La selección es muy fina en función de los criterios que podemos elegir a través de una interfaz gráfica. La selección puede efectuarse a nivel de cada ítem administrado por las preferencias.	El filtro se basa en las peticiones WMI que habrá que escribir, y luego asociar al objeto GPO. El filtro se aplica a nivel de cada GPO.
Interfaz de usuario	La interfaz permite definir todos los parámetros de forma muy intuitiva.	La interfaz permite controlar los parámetros más importantes.

Para responder a la pregunta "¿Cómo elegir entre realizar un parámetro de configuración a través de un objeto GPO o a través del uso de las preferencias de GPO ?", podremos basarnos en la lógica siguiente:

- ¿Queremos forzar el parámetro? En caso afirmativo, utilizaremos un objeto GPO. Si no, usaremos las preferencias.
- ¿Soportan los parámetros de la aplicación o del componente a configurar una gestión de tipo GPO y deseamos forzar su aplicación? En caso afirmativo, utilizaremos un objeto GPO. Si no, usamos las preferencias y desactivamos la opción **Aplicar una vez y no volver a aplicar**.

¡Observe! Cuando un parámetro determinado es declarado en un objeto GPO y también como elemento de tipo preferencia, el parámetro declarado en el objeto GPO tendrá preferencia. Los objetos GPO son tratados de manera prioritaria en relación a las preferencias de la directivas de grupo.



Opciones de tratamiento de las preferencias en un elemento

Los parámetros de los elementos contenidos en las preferencias se aplican de forma "normal" durante el refresco de los objetos de directivas de grupo. Por defecto, las preferencias son reaplicadas, es decir reescritas, durante el arranque del equipo o durante el inicio de sesión. Este modo de funcionamiento garantiza que los elementos soportados a través de las preferencias están en un estado conocido, de la misma manera que ocurre con los parámetros declarados habitualmente en los objetos directivas de grupo.

¡Observe! Si la opción **Aplicar una vez y no volver a aplicar** es seleccionada, entonces las preferencias se aplican en el equipo o el usuario solo la primera vez. Este modo de funcionamiento interesará a los administradores que deseen ofrecer a los usuarios un entorno de partida que esos mismos usuarios podrán modificar si fuera necesario.

Este modo de funcionamiento puede también ayudar a personalizar el entorno por defecto de los usuarios, sin modificar el perfil por defecto usado para crear el perfil del usuario en su primer inicio de sesión.

b. Despliegue y manejo de las preferencias de directivas de grupo

La implementación de las preferencias de directivas de grupo es el resultado de la compra del producto PolicyMaker de la empresa Desktop Standard. Microsoft también compró el producto GPOVault que ha sido adaptado para convertirse en *Advanced Group Policy Management*(AGPM), y distribuido como elemento de *Microsoft Desktop Optimization Pack for Software Assurance* - también llamado MDO.

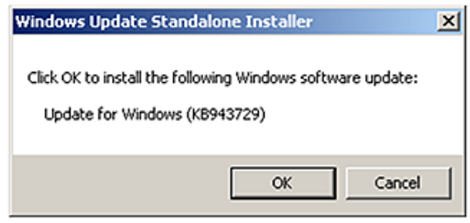
De esta forma, hoy en día las preferencias de los GPO están disponibles de dos maneras:

- Empleando las nuevas herramientas de administración integradas en Windows Server.
- Empleando RSAT (*Remote Server Administration Tools for Windows 10*), el cual está disponible en forma de descarga desde el sitio de Microsoft. Esta segunda opción permite a los entornos de dominio basados en Windows Server 2008 R2 o una versión posterior, tal como Windows Server 2012 R2 gestionar las nuevas preferencias de las directivas de grupo con la consola MMC GPMC de gestión de directivas de grupo, el último nivel de gestión de las preferencias y los modelos ADMX / ADML adaptados a Windows 10 y las versiones anteriores.

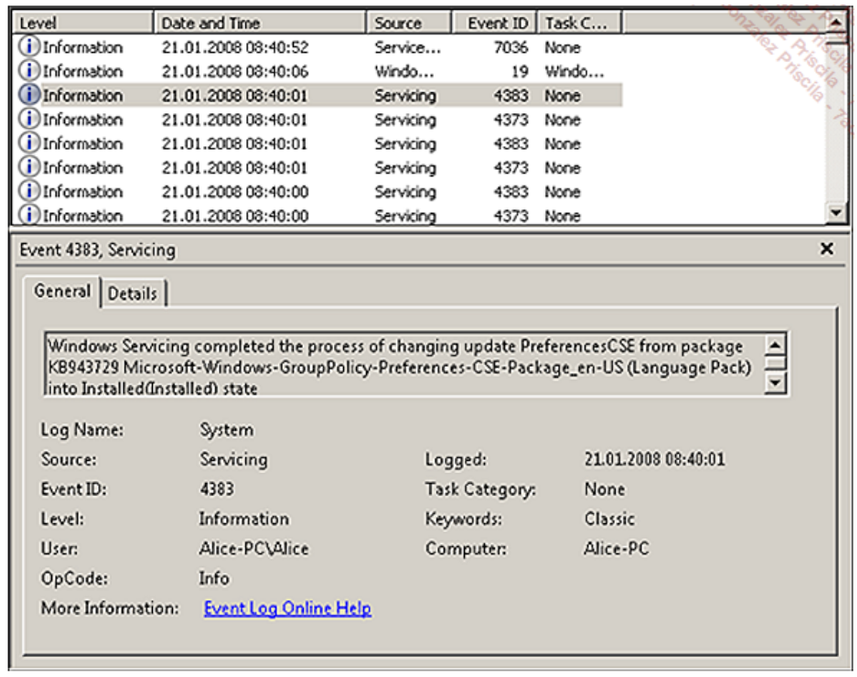
Desde el punto de vista de los puestos de trabajo cliente, el soporte de las opciones y parámetros establecidos en las preferencias se realiza sobre los sistemas siguientes:

- Windows 10/Windows Server 2016
- Windows 8.1/Windows Server 2012 R2
- Windows 8/Windows Server 2012
- Windows 7/Windows Server 2008 R2
- Windows Vista o posterior/Windows Server 2008 SP1 o posterior
- Windows XP SP2 o posterior/Windows Server 2003 SP1 o posterior

¡Observe! El soporte de las preferencias de los GPO requiere para los puestos Windows XP, la instalación de las CSE (*Client-Side Extensions*) necesarias a través de la KB943729. Observe que el uso de las nuevas funcionalidades ofrecidas por las preferencias no requiere ninguna licencia adicional. La imagen siguiente ilustra la aplicación de esta actualización en el caso de Windows XP SP3.

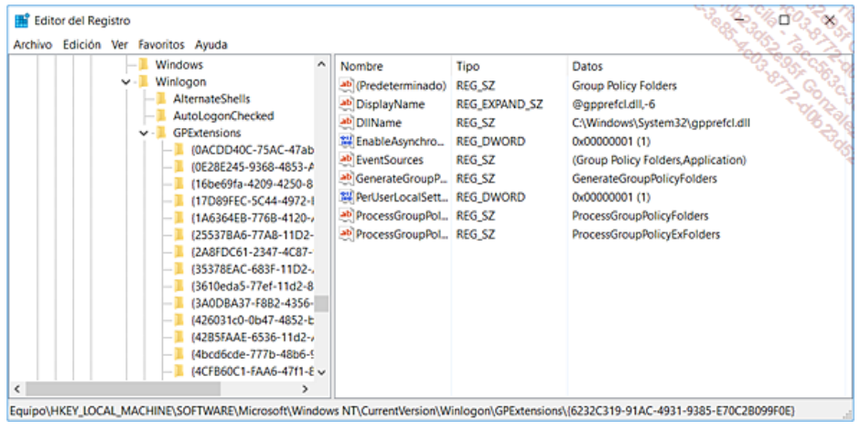


Instalación del paquete de actualización "Windows6.0-KB943729-x86" para un equipo Windows Vista US 32 bits.



Instalación del módulo "PreferencesCSE" a partir del paquete KB943729

La instalación del componente se encarga del soporte de las distintas operaciones realizadas por las preferencias en forma de varios DLL (*Dynamic Link Library*) integradas como componentes de tipo GPE (*Group Policy Extensions*).



Lista de componentes CSE para el tratamiento de las preferencias

c. Familias de parámetros que soportados por las preferencias de directivas de grupo

Mediante la utilización de las Preferencias de directivas de grupo, podemos soportar las familias de parámetros siguientes:

Configuración de Windows:

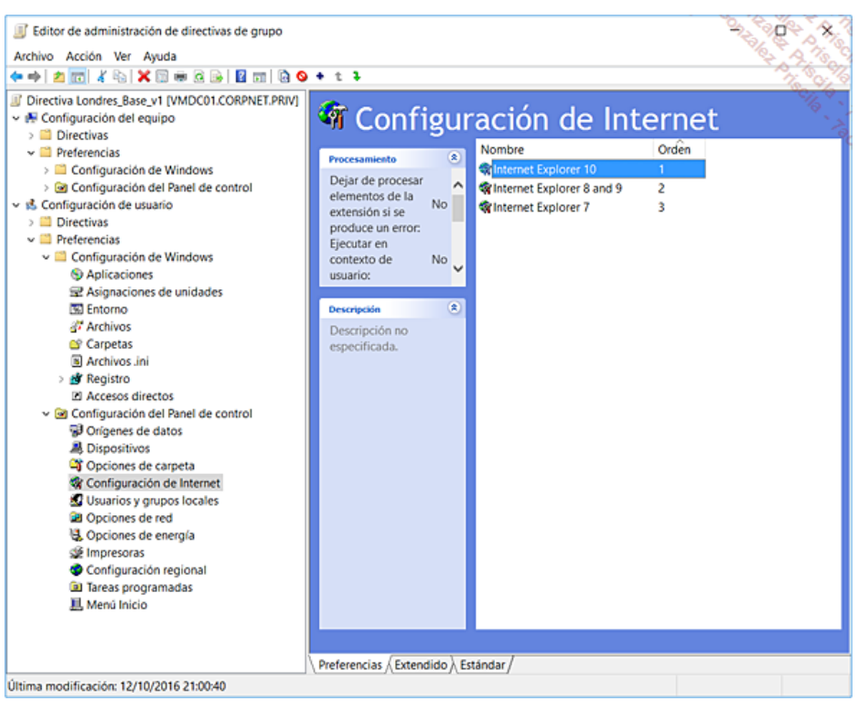
- **Aplicaciones**: este nodo de configuración permite a los desarrolladores insertar conjuntos de parámetros adaptados a sus aplicaciones. Este nodo puede recibir componentes (plug-in) de aplicación. Para más información sobre esta característica poco habitual en la actualidad, busque "Extending the Applications Snap-in" en el sitio Microsoft MSDN en la direcciónhttps://msdn.microsoft.com/.
- **Asignaciones de unidades**: este nodo de configuración permite a los administradores crear, modificar o eliminar conexiones de red. También podemos gestionar la visibilidad de cada unidad. Esta nueva extensión permite gestionar todas las conexiones de red sin implementar scripts. Podemos declarar muchos elementos de tipo "Asignación de unidades" en función de varias condiciones como la pertenencia a grupos, consultas LDAP a cualquier atributo disponible en los servicios de dominio Active Directory o incluso la información relacionada con el equipo.
- **Entorno**: este nodo de configuración permite a los administradores crear, modificar o suprimir las variables de entorno del usuario o el sistema. Esta nueva extensión es muy interesante para gestionar de manera centralizada todas las variables de entorno a utilizar.
- **Archivos**: este nodo de configuración permite a los administradores crear, modificar o eliminar archivos. También podemos gestionar el conjunto de sus atributos. Esta nueva extensión es muy interesante para copiar los archivos de configuración en las carpetas del perfil de los usuarios. Esto puede ser el caso de los archivos necesarios para la personalización de algunas aplicaciones a través de la carpeta AppData.
- **Carpetas**: este nodo de configuración permite a los administradores crear, modificar o eliminar las carpetas. También podemos gestionar algunos atributos de las carpetas. Esta nueva extensión es muy interesante en el marco del mantenimiento de las carpetas temporales. Podemos decidir eliminar algunas carpetas, como los creados en la raíz del disco del sistema, o purgar el contenido de la carpeta temporal de Windows de forma regular.
- **Archivos .ini**: este nodo de configuración permite a los administradores crear, modificar o eliminar las secciones o propiedades en los

archivos de configuración de tipo archivos .ini.

- **Registro**: este nodo de configuración permite a los administradores crear, modificar o eliminar las parámetros del registro.
- **Recursos compartidos - disponible en las Preferencias del equipo**: este nodo de configuración permite a los administradores crear, modificar o eliminar recursos compartidos de red. Observe que esta extensión permite activar o no el uso del modo ABE (*Access Based Enumeration*).
- **Accesos directos**: este nodo de configuración permite a los administradores crear, modificar o eliminar los objetos de acceso directo dentro del entorno Windows. Esta nueva extensión permite manipular los objetos de tipo FSO (*File System Object*), las URL, así como la casi totalidad de los objetos del entorno Windows (*Shell Objects*) como las extensiones del panel de control, la papelera, el explorador, etc.

Configuración del Panel de control:

- **Orígenes de datos**: este nodo de configuración permite a los administradores crear, modificar o suprimir las DSN (*Data Source Names*) ODBC (*Open DataBase Connectivity*).
- **Dispositivos**: este nodo de configuración permite a los administradores forzar la activación o desactivación del funcionamiento de algunos controladores de dispositivos o de determinadas clases de controladores.
- **Opciones de carpeta**: este nodo de configuración permite a los administradores controlar las diferentes opciones específicas para las carpetas de Windows. Podemos gestionar las asociaciones mismas de los archivos.
- **Configuración de Internet**: este nodo de configuración permite a los administradores controlar todos los parámetros de Internet Explorer para Internet Explorer 5 y 6, Internet Explorer 7, Internet Explorer 8 y 9 e Internet Explorer 10. La versión 11 y las versiones posteriores de Internet Explorer son soportadas por medio de la opción de soporte de Internet Explorer 10. En general, estos parámetros son soportadas por un objeto directiva de grupo, para imponer y prohibir su modificación. La utilización de las Preferencias puede permitir definir una configuración de Internet Explorer por defecto que los usuarios podrán cambiar si lo consideren necesario. Observe que algunos parámetros pueden ser controlados por completo a través de un objeto GPO, mientras que otros pueden ser solo propuestos a través de un elemento declarado como Preferencia.
- **Usuarios y grupos locales**: este nodo de configuración permite a los administradores crear, modificar o eliminar usuarios y/o grupos de usuarios locales en los equipos. Esta característica es muy interesante para garantizar un buen nivel de coherencia de las cuentas locales de los equipos. Es más fácil de gestionar el contenido de los grupos importantes como los grupos de usuarios y administradores locales de los equipos.
- **Opciones de red**: este nodo de configuración permite a los administradores crear, modificar o eliminar elementos de conexiones de tipo VPN (*Virtual Private Network*) o Dial-Up. Esta nueva extensión es muy interesante para configurar los elementos de conexión de los usuarios remotos en su ordenador portátil de forma regular. De esta manera, podemos con facilidad mantener el conjunto de estos parámetros de forma centralizada, en función de varios criterios.
- **Opciones de energía**: este nodo de configuración permite a los administradores crear, modificar o eliminar los perfiles de gestión de la energía. Se trata de una opción muy interesante para obtener ganancias sustanciales con respecto al consumo eléctrico de los puestos de trabajo a nivel empresarial.
- **Impresoras**: este nodo de configuración permite a los administradores crear, modificar o eliminar las impresoras locales, de red o conectadas vía TCP/IP. Las directivas de grupo de los puestos de trabajo Windows 7 y posteriores soportan de forma nativa el despliegue de impresoras. Sin embargo, esto no afecta a las impresoras compartidas y requiere una extensión del esquema de Active Directory. La utilización de las preferencias nos permitirá desplegar impresoras locales, compartidas o conectadas vía TCP/IP en puestos Windows 7 y versiones posteriores hasta Windows 10. Esta extensión permite declarar la impresora por defecto del usuario.
- **Configuración regional**: este nodo de configuración permite a los administradores controlar los parámetros regionales.
- **Tareas programadas**: este nodo de configuración permite a los administradores crear, modificar o eliminar las tareas programadas. También podemos crear tareas inmediatas, sobre los puestos de trabajo que van desde Windows XP a Windows 10. Esta nueva extensión es muy interesante para, por ejemplo, declarar las tareas de mantenimiento periódico a ejecutar en los puestos de trabajo, y también en equipos Windows Server.
- **Servicios**: este nodo de configuración permite a los administradores controlar las diferentes opciones de los servicios Windows. Podemos gestionar las opciones de arranque, desencadenar acciones de tipo Start / Stop / Restart para configurar la cuenta asociada a la ejecución del servicio, así como las propiedades de recuperación en caso de incidente.
- **Menú Inicio**: este nodo de configuración permite a los administradores controlar el conjunto de opciones del menú Inicio para los equipos Windows XP, Windows 7 y versiones posteriores (como Windows 10).



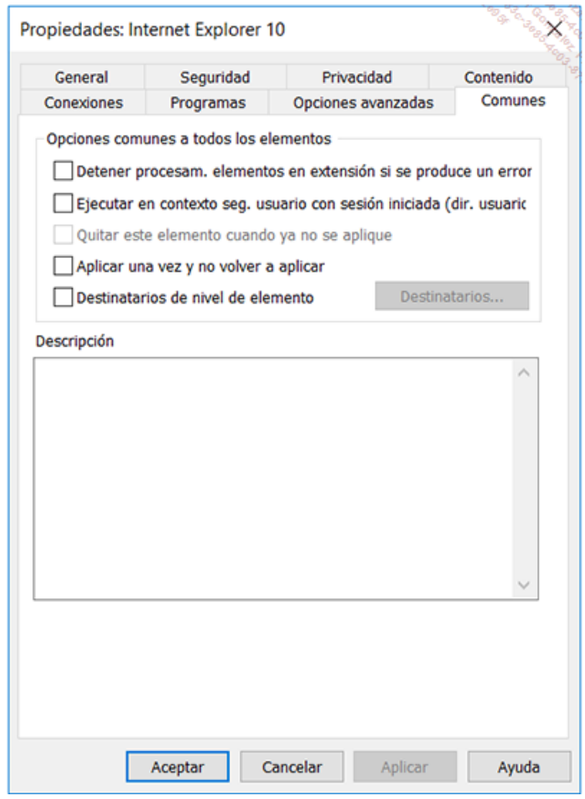
Objeto GPO y nodo de configuración de las preferencias

d. Operaciones y Acciones sobre los Elementos de las preferencias

La mayoría de las extensiones incluidas en las preferencias de Windows Server 2016 soportan las acciones de control de tipo Creación, Eliminación, Reemplazo o Actualización.

Por último, en cada elemento, la pestaña **Comunes** permite personalizar el comportamiento durante el tratamiento de las preferencias. La

imagen siguiente muestra las diferentes opciones.



Opción de selección a nivel del elemento

e. Detener procesamiento de los elementos de extensión si se produce un error

Por defecto, cualquier error de interpretación o ejecución se ignora. De esta manera, el tratamiento de los elementos de las preferencias de la misma extensión puede continuar sin ser interrumpido. Podemos decidir detener el tratamiento de los elementos adicionales de esta extensión activando esta opción. Observe que este parámetro se administra de forma independiente para cada objeto de directiva de grupo. Los demás objetos GPO no se ven afectados por la activación de esta opción.

f. Ejecutar en contexto seg. usuario con sesión iniciada (dir. usuario)

Esta opción desactivada por defecto, puede especificar si es necesario tratar el elemento afectado dentro del contexto de la sesión del usuario. Por defecto, se utiliza la cuenta System Local, permitiendo a las preferencias acceder a las variables de entorno del sistema y los recursos locales del equipo. Por lo tanto es necesario activar esta opción para acceder a las variables del usuario.

g. Quitar este elemento cuando ya no se aplique

A diferencia de los parámetros de directivas de grupo que se suprimirán cuando un objeto GPO ya no se aplique, los parámetros de Preferencias, no se eliminan. En el caso que deseemos eliminar los elementos antes aplicados, será necesario activar esta opción en el elemento a borrar.

h. Aplicar una vez y no volver a aplicar

Sabemos que las directivas de grupo se aplican de forma periódica en los equipos y los usuarios. Recordemos que los objetos GPO se aplican al arrancar el equipo, en el inicio de sesión de usuario, así como durante un intervalo cuyo valor se establece, por defecto, en 90 minutos además de un período variable de entre 0 y 30 minutos. Este refresco periódico podrá, de hecho, provocar el restablecimiento de los parámetros contenidos en las preferencias, incluso si el usuario realiza cambios durante su sesión en estos elementos de su entorno de trabajo. Para evitar el refresco de estos elementos y por lo tanto, la aplicación sistemática de los parámetros originales, será necesario activar esta opción.

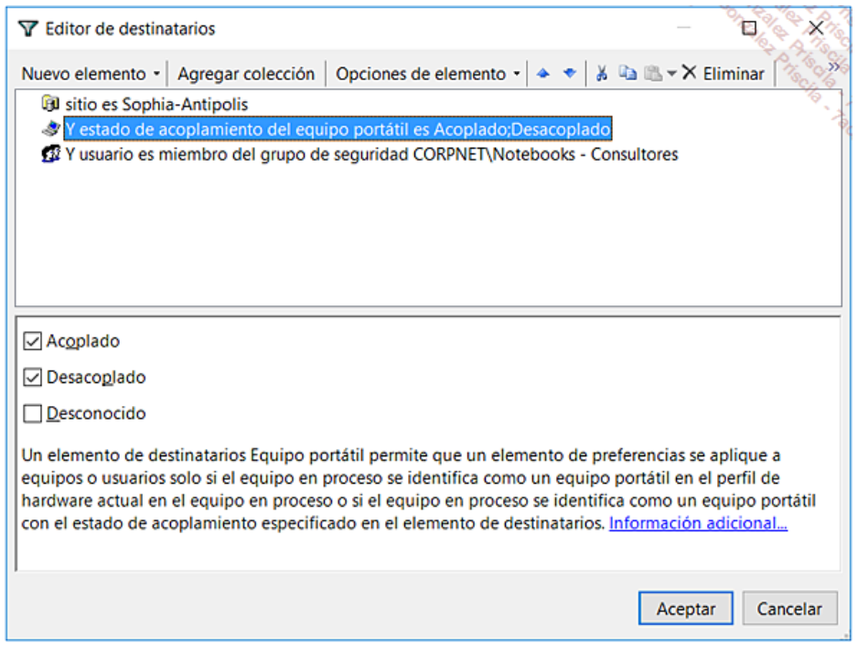
i. Selección a nivel del elemento de Preferencias

Esta característica es sin duda la más poderosa. En efecto, podemos definir a nivel de cada elemento de Preferencias declarado los usuarios y/o los equipos que se verán afectados. Sabemos que desde Windows 2000, la selección de objetos directivas de grupo se basa en la naturaleza del SOM (*Scope of Management*), es decir, la estructura SDOU, Sitio/Dominio/UO, en la cual se aplican los objetos directivas de grupo. Windows XP Profesional aportó a los administradores la posibilidad de aplicar filtros WMI, estos filtros obligan a cumplir varias condiciones para aplicar tal o cual GPO en el ámbito de gestión.

A diferencia del filtro WMI de los objetos directivas de grupo que actúa sobre la totalidad de los parámetros contenidos en el objeto GPO, los elementos de las preferencias de las directivas de grupo soportan una selección natural a nivel de cada elemento.

Mediante las Preferencias y la capacidad de selección disponible sobre cada elemento, podemos crear un único objeto GPO que contienen miles de condiciones para aplicar uno u otro parámetro sobre tal o cual selección específica del objetivo.

La imagen de abajo ilustra la creación de una nueva selección basada en la pertenencia de los equipos de tipo portátil a un sitio de Active Directory y a un grupo de seguridad.

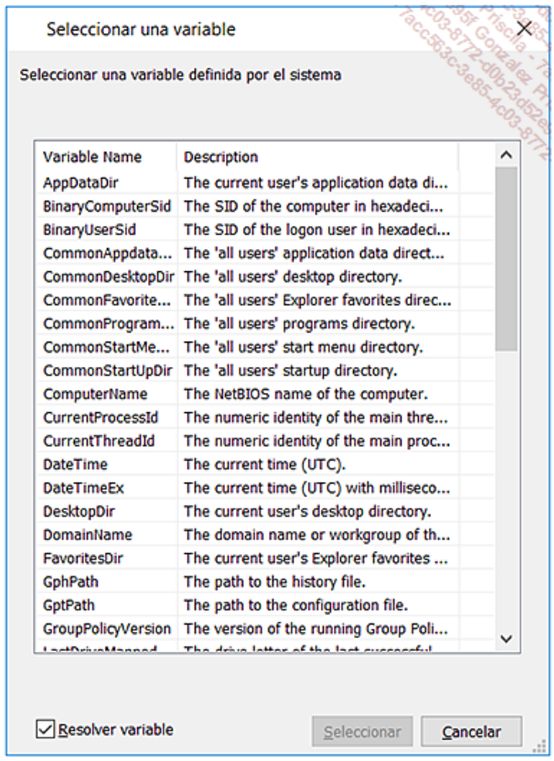


Ejemplo de selección a nivel de un elemento de las Preferencias de los objetos GPO

j. Uso de variables dentro del editor de selección

En la declaración de las diferentes condiciones de aplicación de un elemento, el administrador tiene la posibilidad de utilizar las muchas variables del sistema soportadas por las extensiones de las preferencias de directivas de grupo. El conjunto de estas variables puede ser utilizado a nivel de todas las propiedades definibles en el nivel de los elementos o de la orientación específica de cada elemento. A pesar de que sea posible introducir directamente los valores de estas muchas variables, se recomienda utilizar la tecla [F3] para acceder al selector de variables.

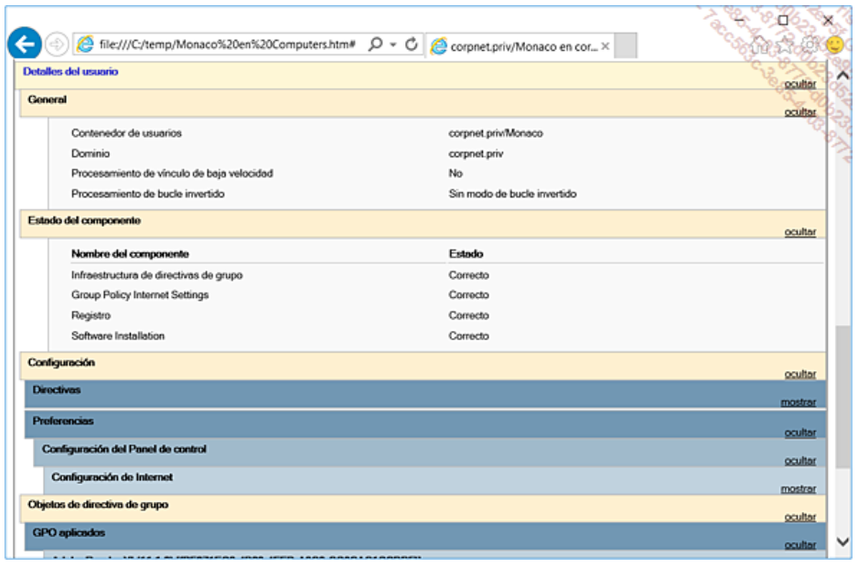
Esta opción evitará los ineludibles errores de sintaxis y nos permitirá utilizar de forma sencilla combinaciones complejas de variables de entorno en la definición de las normas de orientación, haciéndolo muy dinámico.



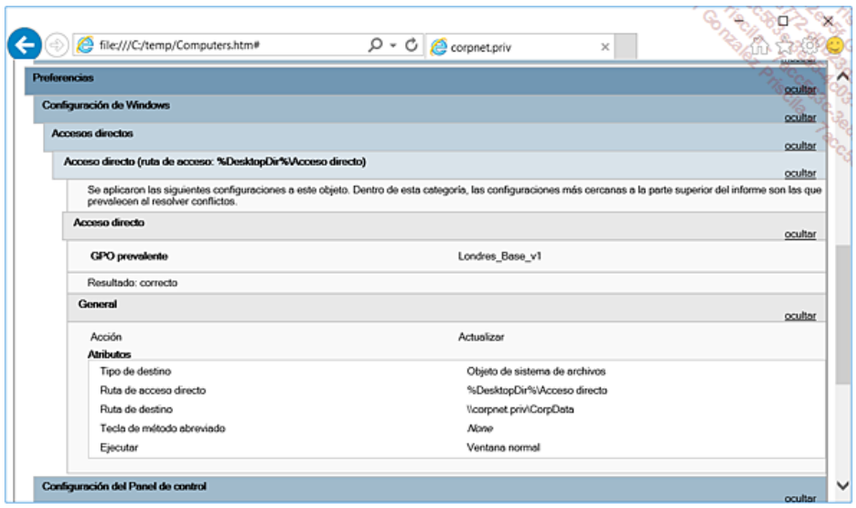
Pulse [F3] para acceder a la lista de las variables.

k. Seguimiento de la ejecución de las preferencias de las directivas de grupo

Las preferencias de las directivas de grupo soportan de manera integral el análisis RSoP soportadas por la consola de gestión de directivas de grupo. La imagen siguiente muestra un análisis realizado empleando GPMC en Windows Server 2016, incluyendo el tratamiento de las preferencias.



Tratamiento de GPO - GPP y estado de los componentes



Aplicación de las preferencias: Ejemplo de un acceso directo de red en el escritorio

La figura anterior muestra la creación de un acceso directo de red en el escritorio del usuario.

Tenga en cuenta que la interfaz del informe RSoP (*Resultant Set of of Policy*) precisa que, en la categoría indicada, los parámetros más cercanos al nivel superior del informe se utilicen con prioridad para la resolución de conflictos. En este ejemplo, los parámetros contenidos en el objeto directiva de grupo " Londres_Base_v1" se aplican con éxito (Resultado: Operación exitosa).

Como es el caso del análisis de la aplicación de los objetos directivas de grupo en los equipos Windows, la consola de administración de directivas de grupo será la herramienta preferida para el análisis y simulación de la aplicación de los parámetros contenidos en los objetos GPO y las preferencias de los objetos GPO.

Para más información sobre las nuevas preferencias de directivas de grupo, podemos consultar el sitio de Microsoft y buscar **Group Policy Preferences**. También podemos consultar el sitio Microsoft Technet dedicado a las directivas de grupo, utilizan el siguiente enlace: http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx

Creación y configuración de objetos de directiva de grupo

1. Introducción

Las directivas de grupo se caracterizan por los puntos siguientes:

- Se trata de objetos pertenecientes a los servicios de directorio Active Directory, cuyo principal objetivo es ayudar a los administradores de red Windows a ofrecer a los usuarios una herramienta y un entorno de trabajo adaptado aún más fiable, más seguro, y por lo tanto más eficiente.
- Las directivas de grupo permiten simplificar la administración centralizada de los parámetros en el directorio Active Directory, por lo tanto, en el exterior de los equipos.
- La administración es más fina, más eficiente, más rica, y también más sencilla.
- Los parámetros de los usuarios se aplicarán de forma independiente de los equipos.

Descubriremos más adelante el modo de tratamiento con bucle de retorno. Este método permite manejar ciertas situaciones y en este caso los parámetros de usuario pueden no ser "considerados" en los equipos que implementan este modo de funcionamiento.

- Los parámetros de equipo se aplicarán de forma independiente de los usuarios.

2. Directivas de grupo y relación con las tecnologías

Las directivas de grupo integran un importante número de tecnologías. Es indispensable saber ¿"Que hace qué"? El cuadro siguiente lista las tecnologías utilizadas para prestar el mejor servicio.

Tareas de administración	Tecnologías utilizadas para implementar el servicio
Gestión de los datos de usuario Active Directory	Active Directory Directiva de grupo Archivos sin conexión Gestor de sincronización Cuotas de disco Perfiles de usuarios móviles
Instalación y mantenimiento de software Active Directory	Active Directory Directiva de grupo Windows Installer
Gestión de parámetros de usuario	Active Directory Directiva de grupo Perfiles de usuarios móviles
Gestión de configuración de equipo	Active Directory Directiva de grupo Cuentas de usuario y de equipo
Servicios de instalación remota (RIS) Nota: hoy en día los servicios RIS están obsoletos y se han sustituido por los servicios WDS y el despliegue de los SO en modo LTI con MDT o ZTI con SCCM	Active Directory Directiva de grupo Servicios de instalación remota

La siguiente tabla muestra en que punto los servicios de directorio Active Directory son indispensables para la tecnología IntelliMirror.

La continuación de este capítulo introduce los detalles de un objeto de directiva de grupo dentro de los servicios de directorio Active Directory.

3. ¿Qué contiene una directiva de grupo?

Una directiva de grupo se compone de diversos tipos o familias de parámetros, los cuales presentamos a continuación. Una vez que hayamos abordado las posibilidades intrínsecas de los objetos de directivas de grupo, detallaremos la implementación de estos objetos dentro de una infraestructura de Active Directory.

a. Plantillas administrativas

Un objeto directiva de grupo integra las plantillas que soportan los parámetros del registro en los siguientes lugares: para los parámetros de usuario, la clave **HKEY_CURRENT_USER** y para los equipos, la clave **HKEY_LOCAL_MACHINE**.

Estas plantillas se implementan bajo la forma de archivos **.adm** que se encuentra de partida en el directorio **%SystemRoot%\Inf**. Mediante estas plantillas, y los que se entregan con los distintos kits de Recursos Técnicos de Office (versiones 2000, XP, 2003, 2007, 2010, 2013 y 2016), podemos configurar de forma muy fina todos los detalles de estas suites de ofimática. Por supuesto, podremos también crear nuestras propias plantillas e integrarlas dentro de objetos de directiva de grupo para difundir sus parámetros hacia toda o parte de la red de la empresa.

Estas plantillas se llaman **Plantillas administrativas**, o Administrative Templates en inglés. La información de registro de "equipo" almacenada en la clave de registro HKEY_LOCAL_MACHINE, se encuentra en GPT\MACHINE\Registry.pol, mientras que la información de registro de usuario se almacena en la clave HKEY_CURRENT_USER ubicada en GPT\User\Registry.pol. No es posible modificar de forma directa los archivos .pol que adoptan un formato binario comprimido. Estos archivos binarios no son más que el resultado de las operaciones realizadas empleando la consola de gestión MMC Editor de objetos de directivas de grupo.

Las plantillas administrativas nos permitirán controlar el comportamiento y la presentación del escritorio, la gestión de las funciones de búsqueda de impresoras, así como, por ejemplo, la posibilidad de bloquear el acceso a las herramientas de edición del Registro y muchos otros elementos.

El siguiente cuadro lista las distintas plantillas entregadas con los antiguos sistemas como Windows 2000, Windows XP Profesional y los sistemas de la familia Windows Server 2003.

Los archivos de plantillas utilizados por Windows 7 y los sistemas más recientes tales como Windows 10, usan los archivos ADMX / ADML escritos en formato XML. Estas plantillas se describen más adelante en este capítulo.

Nombre de plantilla en %SystemRoot%\Inf	Rol/Descripción
System.adm	Conjunto de los parámetros del sistema. Este archivo contiene la mayoría de los parámetros utilizados en la configuración de los puestos de trabajo y el entorno de los usuarios.
Inetres.adm	Conjunto de los parámetros de Internet Explorer.
Wmplayer.adm	Conjunto de los parámetros de Windows Media Player. Esta función no está disponible en Windows XP 64 bits Edition y Windows Server 2003, 64 bits Edition.
Conf.adm	Conjunto de los parámetros de NetMeeting. Esta función no está disponible en Windows XP 64 bits Edition y Windows Server 2003, 64 bits Edition.
Wuau.adm	Conjunto de parámetros de los servicios de Windows Update.

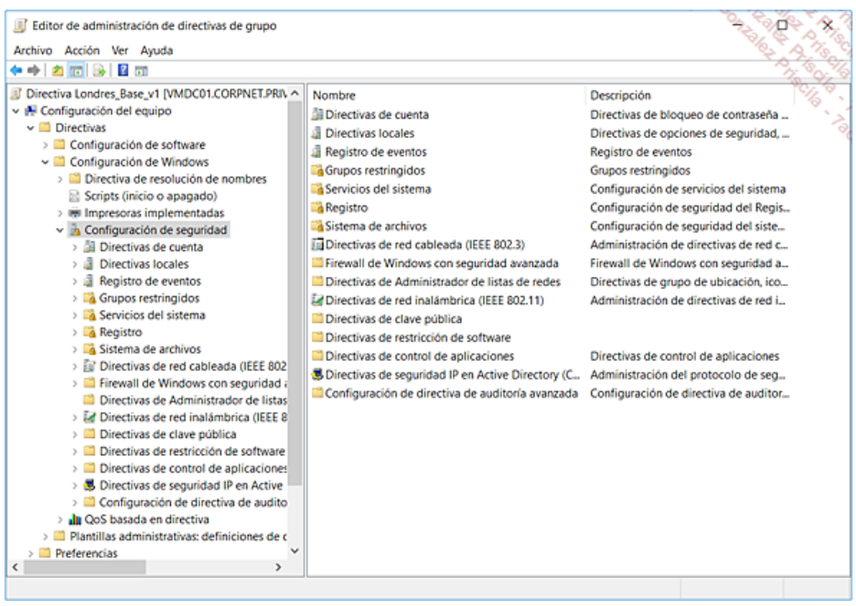
b. Reglas de seguridad para los equipos y plantillas de seguridad

Las directivas de grupo nos permiten realizar muchas tareas pesadas de manera homogénea para proteger los recursos del equipo de las muchas agresiones posibles procedentes de la red. De esta forma, podemos integrar en una directiva de grupo nuestras propias plantillas de seguridad, las plantillas son en sí fabricadas empleando la consola de gestión de las Plantillas de seguridad. Una vez creada una plantilla, esta puede integrarse en una directiva de grupo para que esté a disposición de los equipos deseados. Las reglas de seguridad incorporan los elementos de configuración siguientes:

- Parámetros de autenticación de red y acceso a los recursos.
- Configuración de los ajustes de los mensajes de auditoría en los registros de seguridad.
- La verificación de la pertenencia a grupos de seguridad especificados.

La imagen siguiente ilustra con claridad las grandes categorías de elementos que podemos controlar empleando una directiva de grupo. Estas categorías se listan a continuación:

- Los parámetros de las Directivas de cuentas del dominio, y también de los equipos locales cuando es necesario gestionar también los parámetros de directivas de cuentas locales.
- Las directivas locales de seguridad, es decir, las directivas de auditoría, de atribución de derechos de sistema así como las muchas opciones de seguridad.
- Los parámetros de registros de eventos.
- La gestión de grupos restringidos. Esta funcionalidad permite garantizar que los grupos "importantes" contienen los miembros correctos y ninguna otra persona no autorizada.
- Los parámetros de seguridad de los servicios. Podemos por ejemplo delegar en un usuario particular el derecho a detener, poner en pausa y arrancar un servicio determinado.
- Los parámetros de seguridad de las claves del registro y los directorios del disco del equipo.
- Los parámetros de clave pública, de restricción de software y de directivas IPSec en Active Directory.



Parámetros de seguridad: lista de elementos

En los antiguos sistemas Windows Server 2003, las plantillas de seguridad están ubicadas en el directorio %SystemRoot%\Security\Templates y luego son importables dentro de un objeto directiva de grupo, mientras que con sistemas como Windows Server 2012 R2 o Windows Server 2016, son almacenadas en el directorio %SystemRoot%\inf.

Las plantillas de seguridad predefinidas se suministran como punto de partida. No podrán servir para crear nuestras propias directivas de seguridad empleando la consola de gestión MMC plantillas de seguridad. Una vez desarrolladas nuestras plantillas podremos configurar decenas, cientos o miles de equipos importando nuestras plantillas en una directiva de grupo.

Las plantillas pueden también utilizarse para servir de referencia y realizar comparaciones en el marco del análisis de posibles fallos de seguridad empleando la consola de gestión MMC Configuración y análisis de seguridad.

Las diferentes plantillas suministradas en un servidor Windows Server 2003 se describen de forma breve a continuación:

Plantilla "Setup security.INF", Seguridad por defecto

Esta plantilla se crea durante la instalación del equipo. Contiene el conjunto de los parámetros de seguridad por defecto. Puede ser utilizada en servidores y equipos cliente.

Se recomienda no aplicar esta plantilla empleando una directiva de grupo. Teniendo en cuenta el volumen de información contenido en esta plantilla (702 Kb), podría ocasionar el deterioro del rendimiento. Además, esta plantilla no debe aplicarse a un servidor de tipo controlador de dominio. Podremos, sin embargo, aplicar la totalidad o parte de los parámetros que contiene en el marco de una

recuperación de emergencia. Para aplicar la totalidad o parte de esta plantilla, utilice el comando **Secedit**.

Seguridad por defecto del controlador de dominio (DC security.INF)

Este plantilla se crea de forma automática cuando un servidor se promueve a controlador de dominio. Contiene todos los parámetros de seguridad por defecto de los directorios, archivos, registro y otros servicios del sistema. Puede aplicarse empleando la consola de gestión MMC Configuración y análisis de seguridad o mediante el comando Secedit.

Plantilla "compatible": Compatws.inf

Esta plantilla contiene los permisos por defecto concedidos de partida a los grupos locales Administradores, Usuarios avanzados y Usuarios. Por norma, los miembros del grupo local Usuarios deben ser capaces de hacer funcionar las aplicaciones que disponen del logo de Windows 2000 o Windows XP Compatible. Sin embargo, siempre es posible que los usuarios no puedan ejecutar aplicaciones incompatibles.

Podemos optar por una de las dos opciones siguientes:

- Autorizar a los miembros del grupo Usuarios a convertirse en miembros del grupo de Usuarios avanzados.
- Proporcionar más derechos al grupo Usuarios.

La plantilla Compatible se destina evitar la primera opción. En efecto, la segunda opción modificará los permisos por defecto de los archivos y algunas claves del registro concedidas al grupo Usuarios.

No aplicar la plantilla compatible en los controladores de dominio.

Plantilla "Securizado": Secure*.inf

Esta plantilla establece mejores parámetros de seguridad que los establecidos al término de la instalación del sistema. Entre los parámetros modificados, encontraremos los parámetros de contraseña, bloqueo de cuenta y de análisis más detallados. En el mismo sentido, la utilización de los protocolos de autenticación de LAN Manager y NTLM se desactiva. De hecho, los clientes se configuran para no enviar respuestas de tipo NTLMv2 mientras que los servidores deniegan las respuestas LAN Manager.

El modelo de seguridad Securews.INF, establece que todos los controladores de dominio que contengan las cuentas de todos los usuarios que se conectan al cliente deben ejecutar Windows NT 4.0 Service Pack 4 o una versión posterior.

Observe a su vez que la plantilla de seguridad activa la firma de los paquetes SMB (*Server Message Block*) del lado del servidor, normalmente desactivada por defecto..

Plantilla "Altamente seguro": hisec*.inf

Esta plantilla es una versión más segura de la plantilla anterior. Impone restricciones adicionales en términos de cifrado y firmas necesarias para la autenticación y para los datos que circulan en los canales seguros y entre los clientes y servidores SMB. Por ejemplo, mientras que la plantilla segura impone a los servidores rechazar las respuestas de LAN Manager, la plantilla altamente seguro les impone rechazar las respuestas de LAN Manager y también las respuestas NTLM. Bajo el mismo principio, mientras que la plantilla de seguridad activa la firma de los paquetes SMB del lado del servidor, la plantilla altamente seguro lo exige. Además, la plantilla altamente seguro requiere un cifrado reforzado y la firma de los datos de los canales seguros que establezcan relaciones de confianza de dominio a miembro y de dominio a dominio.

Plantilla "Seguridad en la raíz del sistema": Rootsec.inf

Esta plantilla especifica los permisos sobre la raíz de los discos. Por defecto, Rootsec.inf define estas autorizaciones para la raíz del disco de sistema. Podemos utilizar esta plantilla para volver a aplicar los permisos de acceso al directorio raíz si han sido modificadas por descuido, o podemos cambiar la plantilla para aplicar los mismos permisos de acceso a la raíz a otros volúmenes.

La plantilla de seguridad de la raíz del sistema no borra las autorizaciones explícitas establecidas en los objetos secundarios. Se propaga solo a los permisos que se han heredado y en modo alguno las autorizaciones explícitas.

Plantilla "Sin SID usuario Terminal Server": Notssid.inf

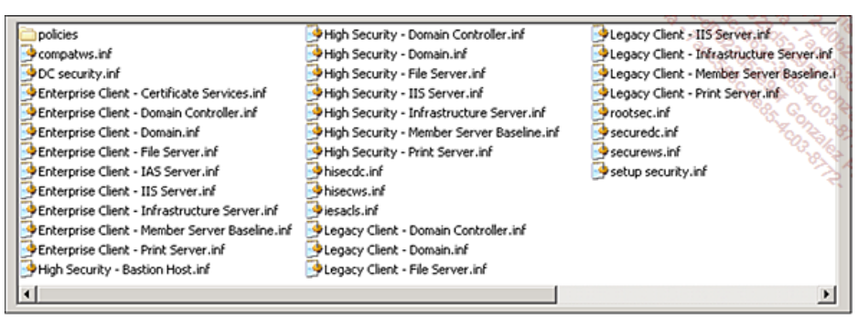
Los permisos por defecto en los discos, así como las listas de control de acceso del registro situadas en los servidores que conceden autorizaciones de un identificador de seguridad (SID) específico para Terminal Server. El SID Terminal Server se utiliza solo cuando Terminal Server se ejecuta en modo de compatibilidad de aplicación. Si Terminal Server no se encuentra operativo en el servidor en cuestión, esta plantilla puede aplicarse para eliminar los SID Terminal Server innecesarios.

Recomendaciones sobre el uso de las plantillas

Estas plantillas de seguridad fueron diseñadas para utilizarse en los equipos que se apartan de los parámetros de seguridad por defecto en Windows Server 2003. De hecho, estas plantillas se implementan de manera incremental por encima de los parámetros de seguridad por defecto, si están presentes en el equipo. Hay que ser consciente de que no instalan los parámetros de seguridad por defecto antes de efectuar las modificaciones.

Las plantillas de seguridad predefinidas no deben ser aplicadas a los sistemas de producción sin haber sido validadas de forma previa.

La figura siguiente muestra los muchos archivos de tipo plantilla de seguridad presentes en un sistema Windows Server 2003.



Muchas plantillas de seguridad están disponibles en el sitio de Microsoft para su descarga

Para descargar estas plantillas para entornos Windows Server 2003, busque "Windows Server 2003 Security Guide" en el sitio Microsoft

Technet en la dirección: https://technet.microsoft.com

Seguridad de Windows 7 y Windows 8.x: con esta versión de su sistema operativo, Microsoft propone un conjunto muy completo de normas de seguridad a través de la herramienta gratuita Microsoft Security Compliance Manager (SCM). Esta herramienta incluye decenas de plantillas de directivas de seguridad adaptadas a diferentes usos y directamente aplicables dentro de la Consola SCM. Luego pueden ser exportados a los GPO para por último desplegarse. Esta potente herramienta se encuentra disponible para descargar en el sitio de Microsoft a través del vínculo siguiente: http://go.microsoft.com/fwlink/?LinkId=182512

Las líneas básicas SCM específicas a Windows 8.1, Internet Explorer 11 y Windows Server 2012 R2 están disponibles para su descarga a partir del sitio de Microsoft a través de dos métodos: la forma más sencilla es utilizar la opción **Download Microsoft baselines automatically** a partir de la consola SCM.

El otro método consiste en descargar los archivos CAB de forma manual a partir del sitio de Microsoft a través de los enlaces siguientes:

- Línea de base SCM Para Windows 8.1 y documentación relacionada:
  http://go.microsoft.com/fwlink/?LinkID=507385&clcid=0x409
  http://go.microsoft.com/fwlink/?LinkID=507387&clcid=0x409
- Línea de base SCM Para Windows 11 y documentación relacionada:
  http://go.microsoft.com/fwlink/?LinkID=507388&clcid=0x409
  http://go.microsoft.com/fwlink/?LinkID=507389&clcid=0x409
- Línea de base SCM Para Windows 2012 y documentación relacionada:
  http://go.microsoft.com/fwlink/?LinkID=507390&clcid=0x409
  http://go.microsoft.com/fwlink/?LinkID=507391&clcid=0x409

Para más detalles sobre Microsoft Security Compliance Manager, utilice el siguiente enlace: http://go.microsoft.com/fwlink/?LinkId=113940

Securización de Windows 10: Microsoft publicó en el sitio Microsoft Security Guidance la línea de base de seguridad para Windows 10 (V1511, "Threshold 2"). Esta línea de base disponible en descarga incluye GPO importables, herramientas para aplicar las GPO de forma localm en caso necesario, archivos ADMX personalizados con nuevos parámetros, así como un archivo Excel que describe todos los nuevos parámetros. Para descargar estos elementos, busque "Security baseline for Windows 10" en el sitio de Microsoft. https://blogs.technet.microsoft.com/secguide/

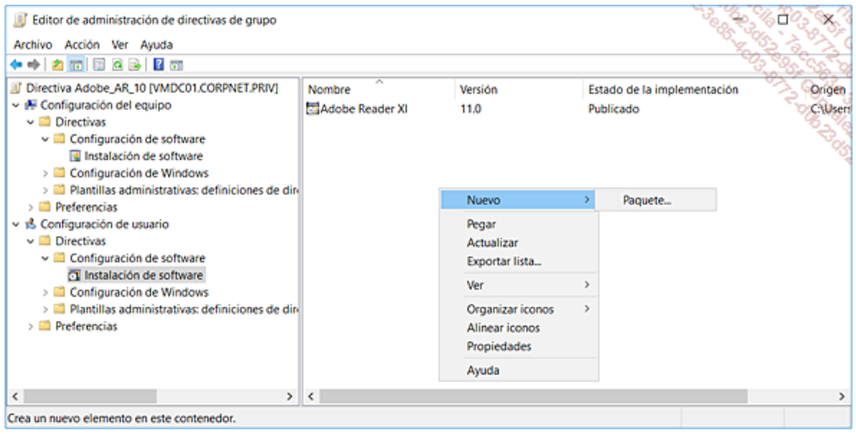
c. Gestión de las aplicaciones

Los servicios de gestión de software son uno de los elementos más importantes. La problemática relacionada con el funcionamiento de las aplicaciones exigió la aplicación de sistemas operativos pesados tales como Microsoft Windows o diferentes versiones del núcleo de Unix. Para constatar esto, basta con comprobar que Apple también ha seguido la misma trayectoria con Mac OSX (kernel Darwin), derivado de Nextstep, el mismo basado en un Sistema UNIX de tipo BSD.

Esta complejidad, tanto de los sistemas como de las aplicaciones, no ha dejado de producir en las empresas muchos problemas de funcionamiento "post despliegue". En efecto, sea cual sea el sistema operativo (Windows, Unix, Linux, Mac OS), ¡estos son frágiles cuando las configuraciones cambian! Era necesario avanzar sobre este tema para poder hacer el puesto de trabajo más dinámico de lo que era.

Los componentes de gestión y mantenimiento de software integrados en el corazón de Windows 7 y versiones posteriores a través del motor de instalación Windows Installer son elementos esenciales. A continuación, tendremos la posibilidad de utilizar esta tecnología para por fin integrar las aplicaciones que deben desplegarse empleando objetos de directivas de grupo.

La imagen siguiente ilustra este principio.



Instalación de software: añadir un nuevo software para desplegar

Descubriremos más allá del que las aplicaciones puedan ser desplegadas, eliminadas , actualizaciones en la misma familia de producto o de manera competitiva, sino que también será posible "parchear" cualquier aplicación desarrollada a través de IntelliMirror, es decir, empleando Active Directory y objetos de directiva de grupo.

Como se muestra en la figura anterior, los servicios de instalación nos permiten desplegar aplicaciones a los equipos. De esta manera, todos los usuarios de estos equipos tienen la posibilidad de utilizar las aplicaciones. Las aplicaciones también pueden ser desplegadas hacia los usuarios, de tal manera que sólo conciernen a los usuarios destinatarios, en cualquier equipo.

El despliegue de software empleando las directivas de grupo se trata en detalle en el capítulo siguiente.

Para saber más sobre las características del servicio Windows Installer, las diferentes versiones y sus grandes principios de funcionamiento, consulte el capítulo siguiente o al sitio MSDN y busque Windows Installer.

WSUS 4.0 y SCCM 2016: con respecto a las otras tecnologías y herramientas de Microsoft que permite gestionar el ciclo de vida de los programas y sistemas operativos.

La tecnología de gestión y mantenimiento de software es directamente dependiente de lo que permite hacer el motor Windows Installer. El motor fue diseñado para soportar las aplicaciones compatibles con las especificaciones de las diferentes versiones de Windows siguiendo las evoluciones de las diferentes versiones de Windows. Así, no se pretende asegurar que el servicio Windows Installer asuma el paso de los correctivos propios de los sistemas operativos.

La estrategia de Microsoft es clara: los sistemas operativos deben avanzar a su ritmo y las aplicaciones también. Para dos problemáticas diferentes, la estrategia requiere que haya dos tecnologías de gestión diferentes: una para los sistemas y otra para las aplicaciones. Los sistemas utilizan los servicios de Windows Update disponibles a través de HTTP / HTTPS (y el protocolo de transferencia inteligente de archivos BITS) o la versión WSUS 3.0.

Los servicios WSUS permiten controlar mejor el paso de los parches dentro de la red de la empresa, sabiendo que SCCM (*System Center Configuration Manager*) integra también una gestión de parches muy sofisticada con un seguimiento avanzado e informes muy detallados.

Además de los métodos presentados antes, siempre es posible obtener los parches y otras actualizaciones vía Internet a través del sitio Windows Catalog en la dirección: http://catalog.update.microsoft.com/

- WSUS es capaz de detectar las actualizaciones fallidas y otros errores de los parches en los equipos de la red.
- WSUS permite la eliminación de los parches y la definición de la frecuencia de actualización que debe garantizarse para que los equipos de la red estén al día.
- Para las instalaciones que no requieren el reinicio del ordenador, el paso de los correctivos puede ser totalmente silencioso, por lo tanto, transparente para los usuarios.
- Los servidores WSUS pueden ser encadenados entre sí con independencia de los privilegios de administración.
- La transferencia de los parches utiliza la tecnología BITS - *Background Intelligent Transfer Service*, y el motor Windows Installer para no ser agresivo sobre el ancho de banda disponible en la red.
- Las descargas tienen una gestión de los puntos de parada y el motor BITS es capaz de trabajar en modo delta de archivos binarios comprimidos.
- WSUS ofrece a los administradores la posibilidad de utilizar nuevos informes para realizar todas las estadísticas útiles para el paso de los parches.
- WSUS es una plataforma central de gestión de cambios.

Para más información sobre WSUS, consulte el siguiente enlace: https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

En relación con el soporte de servicios WSUS 4.0 con Windows Server 2012, 2012 R2 y 2016

Windows Server 2012 R2 y Windows Server 2016 incluyen los servicios WSUS 4.0 a través de un rol disponible dentro del Administrador del servidor. Esta versión de WSUS soporta las funcionalidades siguientes:

- Soporte de Windows Server 2012 R2 y Windows Server 2016.
- Integración de WSUS dentro del Administrador del servidor de Windows Server.
- Nuevas API cliente.
- Soporte de los mecanismos de distribución para las plataformas no Windows.
- Mejora de la grabación de los clientes.
- Filtrado de actualizaciones por categorías y clasificaciones.
- Informe de la condición de actualizaciones para cada cliente.
- Publicación avanzada de controladores a través de las API de administración existentes y los catálogos proporcionados por los proveedores de controladores.
- Soporte de la noción de *bundles* (conjunto de parches).
- Soporte de condiciones de aplicaciones (requerimientos).

Para más información sobre los servicios WSUS integrados en Windows Server 2012 R2 y Windows Server 2016, busque "Visión de conjunto de servicios WSUS" en el sitio Microsoft Technet en la dirección: https://technet.microsoft.com

El seguimiento de las versiones de los servicios WSUS no es evidente, ya que evoluciona en función de los KB publicados por Microsoft. Estas pocas líneas resumen las diferentes versiones proporcionadas en función de las versiones de Windows Server.

Servicios WSUS con Windows Server 2008 y 2008 R2:

- Version 3.0 (SP2): Build 3.2.7600.226
- Version 3.0 (SP2) + KB 2720211: Build 3.2.7600.251
- Version 3.0 (SP2) + KB2734608: Build 3.2.7600.256
- Version 3.0 (SP2) + KB2828185: Build 3.2.7600.262
- Version 3.0 (SP2) + KB2938066: Build 3.2.7600.274

Servicios WSUS de Windows Server 2012:

- Version 4.0 también llamada 6.2: Build 6.2.9200.16384
- Version 4.0 + KB3095113: Build 6.2.9200.17642

Servicios WSUS de Windows Server 2012 R2

- Version 4.1 + KB3095113: Build 6.3.9600.18057

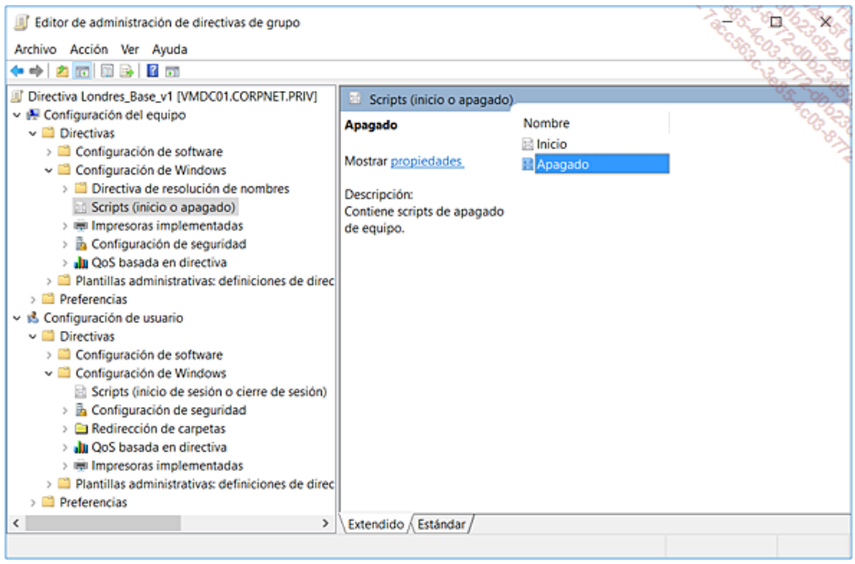
Servicios WSUS de Windows Server 2016

- Build 10.0.14300 (TP5 non-RTM)

d. Gestión de la ejecución de los scripts

Las estrategias de grupo nos permiten declarar diferentes niveles de scripts. También podemos declarar los scripts en los momentos siguientes:

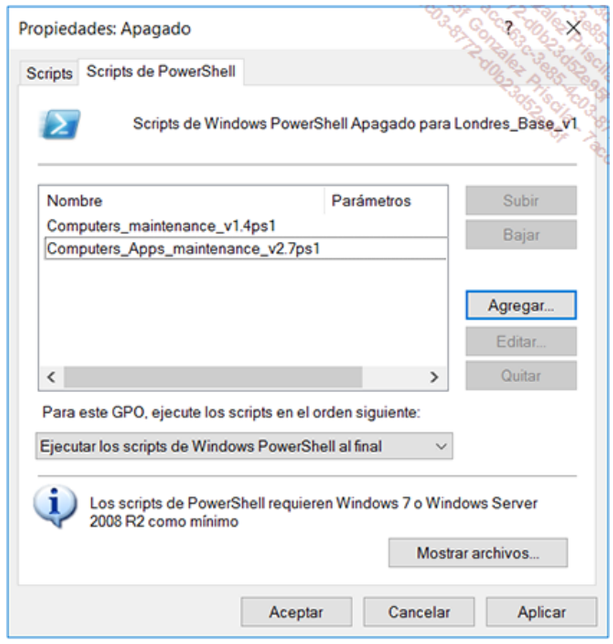
- scripts de arranque del equipo,
- scripts de inicio de sesión de usuario,
- scripts de cierre de sesión de usuario,
- scripts de parada del equipo,



Soporte de los scripts

Además de gestionar la ejecución de los scripts en esos momentos importantes, podremos también declarar varios scripts unos detrás de otros. Cada script declarado es almacenado de forma directa en el volumen de sistema en una ubicación como ésta: %Systemroot%\Windows\SYSVOL\sysvol\Corpnet.priv\Policies\{C8C119A6-1426-44EE-849F-324A3B76820C}\Machine\Scripts\Startup.

Los scripts que utilizará podrán ser escritos con las tecnologías de scripts soportadas por las plataformas Windows objetivo, es decir, scripts VBScript y JScript a través de WSH (*Windows Scripting Host*) y Windows PowerShell para sistemas Windows 7 hasta Windows 10.



Soporte de los scripts Windows PowerShell

e. Los servicios de instalación remota RIS a WDS, MDT y SCCM

Los servicios de instalación remota RIS (*Remote Installation Services*) permitían desplegar un sistema operativo en equipos. Hoy en día, están por supuesto totalmente obsoletos, sin embargo, cabe señalar que soportaban ya un mecanismo que permitía a los equipos de la red conectarse al servidor RIS a través de una operación de arranque a través de la red basada en el protocolo PXE habilitado por la tecla [F12]. Un servidor RIS con Windows Server 2003 podía hacerse cargo de la instalación y el despliegue de imágenes RIS de tipo Windows Server 2003 y Windows XP Profesional. Se trataba de una buena solución para instalar un sistema operativo completo en un equipo nuevo o bien para restaurar la configuración de un sistema defectuoso.

Con Windows Server 2012 R2 y Windows Server 2016, los servicios de despliegue WDS (*Windows Deployment Services*) y las herramientas de Microsoft como el ADK (Windows 10 Assessment and deployment Kit), el MDT (*Microsoft Deployment Toolkit*) y SCCM (*System Center Configuration Manager*), los servicios RIS son hoy más que obsoletos.

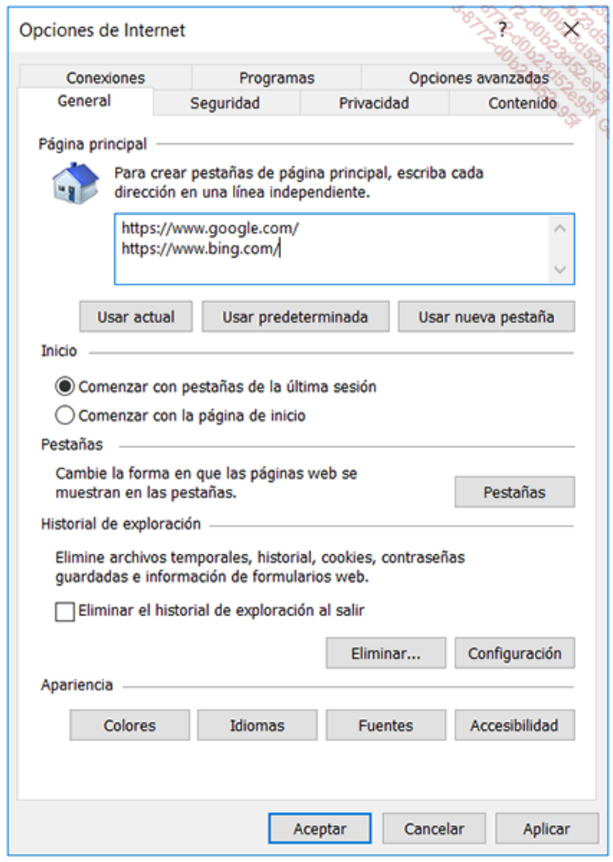
Los servicios WDS sustituyen a RIS

A partir de Windows Server 2003 y en las versiones posteriores hasta Windows Server 2016, los servicios RIS han sido sustituidos por los servicios WDS (*Windows Deployment Services*), el ADK y el MDT. Utilizando ADK, conocido antes como Windows AIK -podremos realizar instalaciones de Windows 7 hasta Windows 10 personalizadas en todos sus detalles y automatizadas por completo. Empleando ImageX, podemos también capturar imágenes Windows "máster" y crear nuestras propias imágenes de arranque Windows PE.

Para descargar el ADK de Windows 10, busque en el sitio de Microsoft "Windows 10 Assessment and deployment Kit" . Observe que los servicios WDS incluidos con Windows Server 2012 R2 y 2016 soportan el despliegue de imágenes en modo multicast.

f. Gestión de parámetros de configuración y seguridad de Internet Explorer

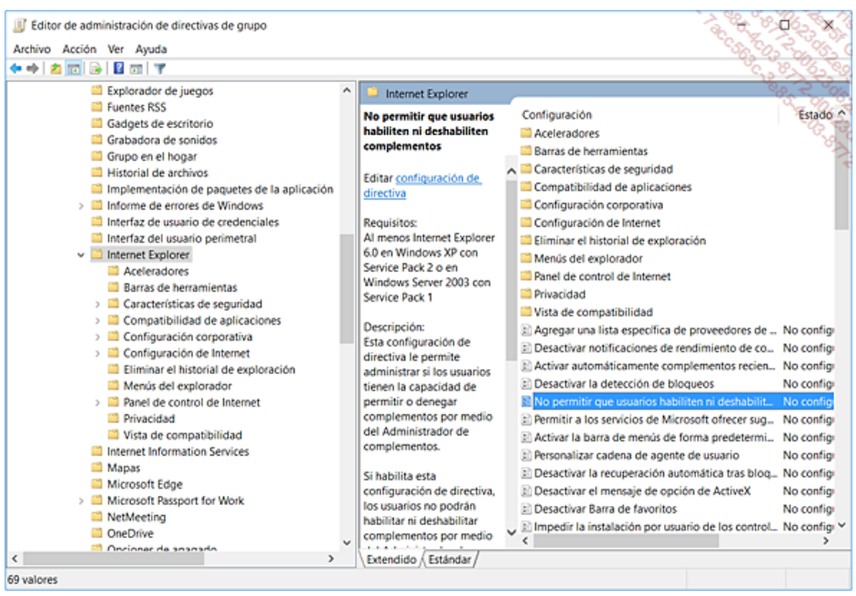
La configuración es en particular rica. En efecto, Internet Explorer es un componente muy importante de la plataforma Windows, al igual que puede ser ¡el shell (el escritorio) de Windows! En la medida en que IE y sus componentes suelen ser solicitados, la seguridad de IE nos lleva a securizar en gran medida el sistema. De qué sirve securizar el SO, si las aplicaciones no lo están, y viceversa. Aquellos que hayan utilizado IEAK (*Internet Explorer Administration Kit*) para personalizar Internet Explorer volverán a encontrar la mayoría de estos parámetros en las directivas de grupo y en las preferencias de las directivas de grupo.



Configuración de los parámetros de IE 11 empleando las Preferencias de las directivas de grupo

Observe la retirada del soporte de la extensión IEM (*Internet Explorer Manitenance*): la funcionalidad IEM, integrada en los objetos de directiva de grupo y en las versiones de IE anteriores a la versión 10, fue retirado en favor de los parámetros de preferencias de los objetos de directivas de grupo, el uso de los archivos ADMX e IEAK 11 (IE 11 Administración Kit). Los parámetros IEM, aun cuando existían antes, ya no pueden ser aplicados en las versiones Internet Explorer 10 y posteriores.

Del mismo modo, los antiguos GPO que contengan parámetros de tipo IEM, no podrán ser modificados a partir de equipos donde IE 10 o una versión posterior se encuentre instalada. Para más información sobre el uso de las Preferencias para configurar IE para sustituir la retirada de la funcionalidad IEM, consulte el enlace https://technet.microsoft.com/en-us/itpro/internet-explorer y busque "Internet Explorer Maintenance" o utilice el siguiente enlace: https://technet.microsoft.com/en-us/itpro/internet-explorer/ie11-deploy-guide/missing-internet-explorer-maintenance-settings-for-ie11



GPO y parámetros de Internet Explorer.

Los parámetros de Internet Explorer se dividen en tres grandes categorías:

- En la parte del **Equipo** en la ubicación **Configuración del equipo/Plantillas administrativas/Componentes de Windows/Internet Explorer** para todo lo que está en relación con las zonas de seguridad de Internet, los parámetros de proxy para el equipo, de tal manera que los usuarios no tendrán la posibilidad de alterar este valor, así como los parámetros de actualización de Internet Explorer, sus componentes y también los componentes de terceros.
- En la parte del **Usuario**, en la ubicación **Configuración de usuario/Plantillas administrativas/Configuración de Windows/Mantenimiento de Internet Explorer** para todo lo que está relacionado con la personalización del interfaz, las conexiones, los URL principales, los favoritos, los parámetros de seguridad y Authenticode y la configuración de los programas por defecto de Internet.
- En la parte del **Usuario**, en la ubicación **Configuración de usuario/Plantillas administrativas/Componentes de Windows/Internet Explorer** para todo lo que trata de opciones del panel de control de Internet, páginas sin conexión, los menús del navegador, las barras de herramientas y controles autorizados.

g. Redirección de las carpetas de usuario (carpetas especiales)

Las directivas de grupo ofrecen la posibilidad de redirigir algunas carpetas especiales a otros lugares de la red empleando una extensión integrada en las directivas de grupo. Esta ampliación, que es también un principio de administración, se denomina "redirección de carpetas".

La redirección de carpetas es una directiva de grupo de tipo Usuarios. Esto significa que un usuario para el que configuremos la redirección de carpetas deberá ser objeto de la aplicación de una directiva de grupo.

Después de haber creado la directiva de grupo y haberla asociado al contenedor adecuado, un administrador puede designar las carpetas que deberán ser redirigidas y a qué sitio local o de red. Esta opción está ubicada en la dirección siguiente en el objeto de directiva de grupo.**Configuración de usuario\Configuración de Windows\ Redirección de carpetas**.

Las carpetas especiales son 13:

- AppData (Roaming), Escritorio, Menú inicio, Documentos, Imágenes, Música, Vídeos, Favoritos, Contactos, Descargas, Vínculos, Búsquedas, Juegos guardados.

El nodo Redirección de carpetas contiene sólo las carpetas llamadas "especiales". No es posible añadir otras carpetas controladas por la redirección de carpetas.

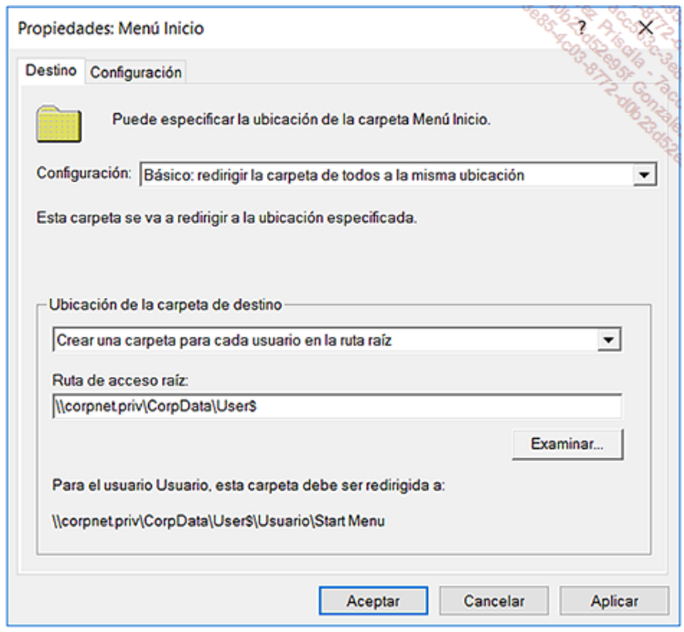
Son posibles varios niveles de redirección. Dirigiéndonos a las propiedades de la carpeta a redirigir, podemos elegir entre los dos grandes modos presentados a continuación:

- El primer modo se llama **Básico: redirigir la carpeta de todos a la misma ubicación**. Es bastante eficaz, ya que permitirá al administrador:
  - **Redirigir a la ubicación siguiente**: nos permite redirigir la carpeta al destino elegido. La variable **%username%** nos permitirá utilizar un directorio específico para cada usuario.
  - **Redirigir a la ubicación local de perfil de usuario**: la elección corresponde al comportamiento por defecto para la elección de la ubicación de la carpeta en caso de no ser redirigida por el Administrador.

Los administradores desean con frecuencia utilizar esta funcionalidad para redirigir de forma automática los archivos de un usuario a una carpeta creada de forma específica para cada usuario.

La variable **%username%** puede ser utilizada en la ruta de redirección, permitiendo al sistema crear de forma dinámica una carpeta de redirección para cada usuario para el cual se aplique el objeto de directiva. La redirección de las carpetas especiales es en especial interesante porque ha sido diseñada para satisfacer las necesidades de los usuarios con la ventaja de ser una aplicación simple y casi sin mantenimiento para los administradores.

La pantalla siguiente ilustra esta primera posibilidad.



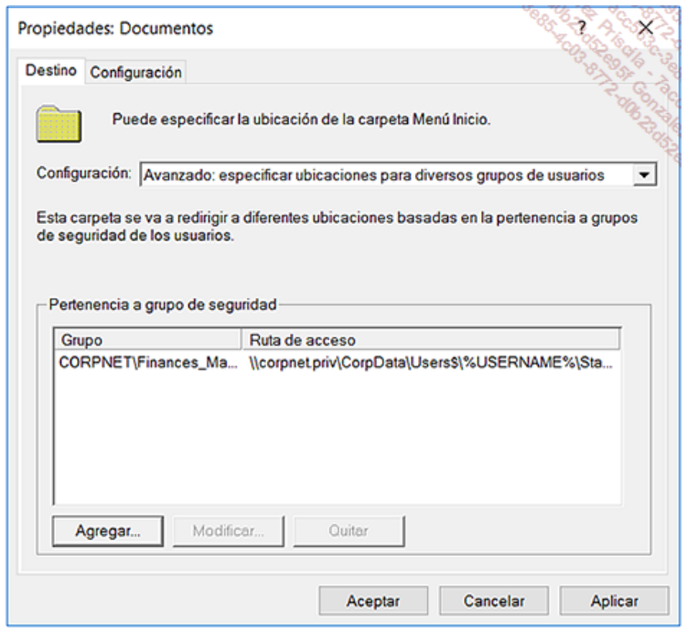
Redirección de carpetas y configuración del menú Inicio

- El segundo modo de funcionamiento se llama **Redirección avanzada**. A diferencia del parámetro "básico", este método permite al administrador especificar diferentes ubicaciones para las carpetas redirigidas en función de la pertenencia de los usuarios a un grupo de seguridad. El parámetro **no configurado** permite al perfil del usuario, y no a la directiva de grupo, determinar la ubicación de la carpeta. En este caso, la pestaña **Configuración** no está disponible. Si seleccionamos el parámetro **Documentos**, la carpeta **Mis imágenes**, por ejemplo, sigue siendo una subcarpeta de **Mis documentos** con independencia de la ubicación donde se redirija **Mis documentos**.

Este modo de funcionamiento es muy práctico ya que es posible declarar cientos de grupos cuyos miembros serán redirigidos hacia un único destino. Una única directiva de grupo puede ser empleada para todos los usuarios específicos en función de su pertenencia a un grupo.

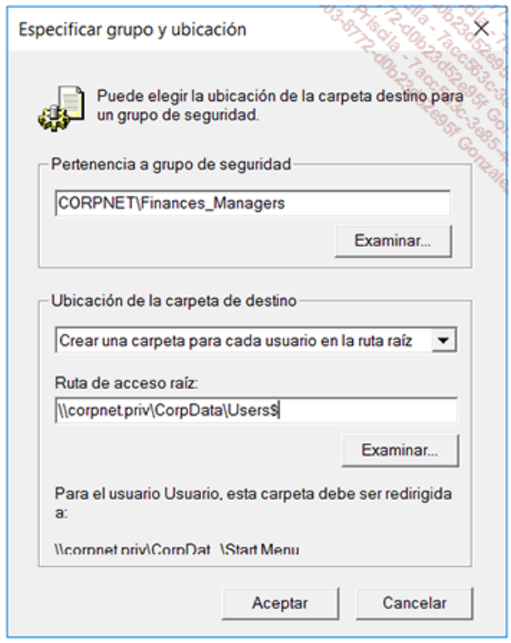
Podemos elegir la ubicación de la carpeta destino de la siguiente manera:

- **Crear una carpeta para cada usuario en la ruta raíz**: esta opción añade a la ruta una carpeta llamada en función de la variable de entorno %username%.
- **Redirigir a la ubicación siguiente**: esta opción nos permite especificar una ruta de acceso a la red de tipo UNC y también una ruta válida a nivel local, como C:\Nombre_carpeta.
- **Redirigir a la ubicación local de perfil de usuario**: esta opción corresponde al comportamiento por defecto para la elección de la ubicación de la carpeta en caso de no ser redirigida por el Administrador.
- **Redirigir el directorio particular del usuario**: esta opción es muy interesante si ya se han desplegado las carpetas de usuario (*Home directories*) y se quieren utilizar como carpeta "Mis documentos". Por supuesto, esta opción solo está disponible para la carpeta **Mis documentos**.



Redirección de carpetas y gestión de ubicaciones en función de los grupos

La pantalla siguiente ilustra las diferentes opciones de la selección del destino.



Selección de la ubicación de la carpeta de destino

Observaciones acerca de la redirección de carpetas: la funcionalidad de redirección de carpetas se utiliza con frecuencia con archivos sin conexión. El hecho de utilizar y configurar los archivos sin conexión con la redirección de carpetas permitirá a los usuarios acceder a sus documentos, incluso cuando el equipo se desconecta de la red. En el caso de utilizar también perfiles móviles entonces es la redirección de carpetas quién se encargará de la actualización de los archivos sin conexión. Con respecto a la redirección de la carpeta Mis documentos, se recomienda redirigir la carpeta de forma directa a un recurso compartido de red dedicado empleando DFS, y definir cuotas de disco para controlar el espacio ocupado por los usuarios. Observe también que las cuotas de perfil no funcionan para el control del espacio en disco utilizado por las carpetas redirigidas de los usuarios. Los archivos y carpetas sin conexión, son codificados en el disco local del puesto de trabajo, la redirección de las carpetas influirá sobre el uso del cifrado EFS en el sentido de que los archivos codificados son descifrados antes de ser transmitidos por la red.

Para más información sobre la aplicación paso a paso de las funcionalidades de redirección de carpetas con archivos sin conexión, busque "Deploy Folder Redireccionar with Offline Files" en el sitio Microsoft Technet en la dirección: https://technet.microsoft.com

h. ¿Qué es una directiva de grupo?

En el marco de la administración de sistemas y de la política global de seguridad, los servicios de directorio Active Directory ofrecen a los administradores los objetos directiva de grupo.

Mediante esos objetos que son los elementos fundamentales de la tecnología IntelliMirror, el personal responsable de las tareas de configuración y administración de sistemas, aplicaciones y servicios de seguridad puede definir y gestionar de manera centralizada o descentralizada todos los tipos de configuración para administrar los equipos y los usuarios.

Las directivas de grupo respetan los principios enumerados a continuación:

- Estos objetos se almacenan en un dominio y se replican en todos los controladores de dominio de dicho dominio.
- Solo están disponibles en un entorno Active Directory.
- Se aplicarán a los usuarios y a los equipos de un sitio, de un dominio o de una unidad organizativa cuyo objeto de directiva de grupo esté vinculado. Se trata del principal mecanismo por el cual una directiva de grupo se utiliza en un entorno Active Directory.

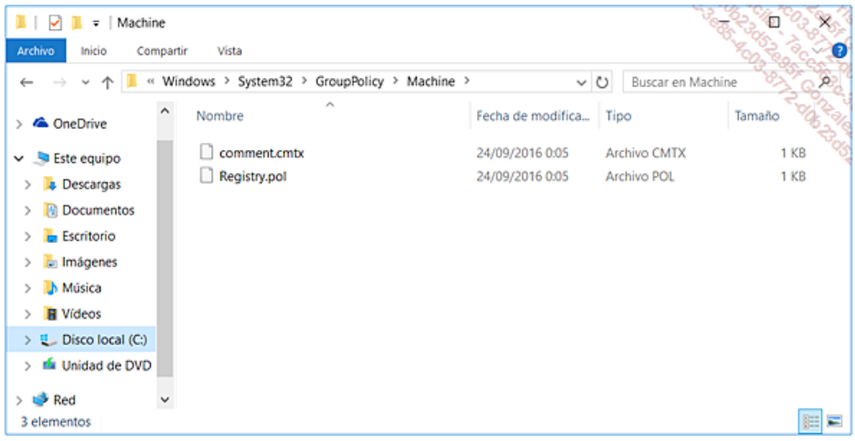
i. ¿Qué es una directiva de grupo local?

Un único objeto de tipo «directiva de grupo local» se almacena en cada equipo. Los objetos de directiva de grupo local son los que tienen menos peso en un entorno Active Directory.

Aparte, solo poseen un subconjunto de los parámetros presentes en los objetos de directiva de grupo basados en Active Directory. Podemos abrir la directiva local de un equipo o de todos los usuarios locales empleando la consola de gestión MMC Editor de objetos de directiva de grupo. Podemos iniciar esta consola ejecutando el archivo de consola **Gpedit.msc**.

Los archivos relativos al almacenamiento de la directiva se ubican en las rutas listadas a continuación:

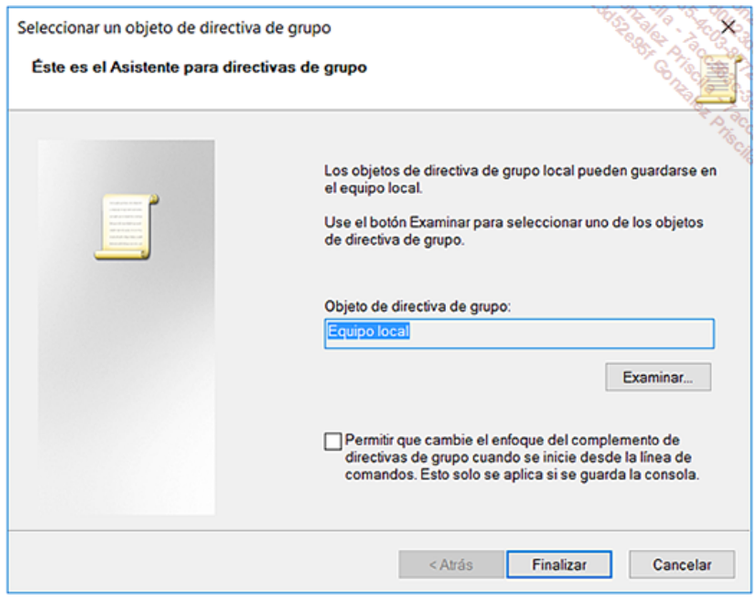
- La parte Usuario se encuentra en la ubicación: %Systemroot%\System32\Group Policy\User\Registry.pol
- La parte Equipo se encuentra en la ubicación: %Systemroot%\System32\Group Policy\Machine\Registry.pol



Archivos binarios Registry.pol

Todos los sistemas Windows Client poseen una directiva local siendo este punto cierto incluso si los equipos forman parte de un entorno de dominio Active Directory.

La pantalla siguiente ilustra como proceder para abrir y modificar la directiva del equipo local.



Apertura de la directiva local del equipo

La directiva local se aplica durante el arranque del equipo para el equipo y para todos los usuarios que inician una sesión local. En el caso de un inicio de sesión de red de dominio, está claro que una vez autenticado por el dominio un inicio de sesión local en el equipo tiene lugar para el usuario autenticado en el dominio.

Limitaciones del objeto de directiva de grupo local

Los objetos de directiva de grupo local no soportan ciertas extensiones, como la Redirección de carpetas o la Instalación de software vía directiva de grupo. Los objetos de directiva de grupo local soportan muchos parámetros de seguridad, pero la extensión Configuración de seguridad del Editor de objetos de directiva de grupo no soporta la gestión remota de objetos de directiva de grupo local.

Por ejemplo, la línea de comando `gpedit.msc /gpcomputer:"PC-Marketing-01"` nos permite modificar el objeto de directiva de grupo local en PC-Marketing-01, pero el nodo Configuración de seguridad no aparecerá.

Si empleamos los objetos de directiva de grupo local, observe que estos son los de menor peso en un entorno Active Directory, ya que los objetos de directiva de grupo basados en Active Directory tienen siempre la prioridad.

En este punto , si no existe ninguna directiva de grupo específica definida dentro del dominio Active Directory, sólo la directiva de grupo del dominio Active Directory se aplica (el tratamiento de las directivas de grupo en el entorno Active Directory se detalla más adelante).

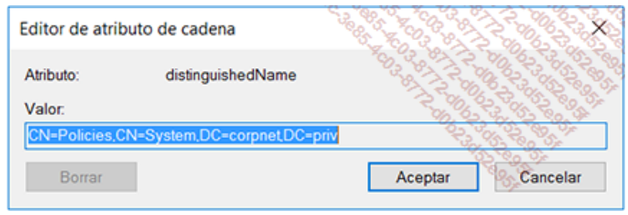
4. Estructura física de una directiva de grupo

Los datos que contiene un objeto directiva de grupo se almacenan en dos ubicaciones importantes:

- el contenedor Directiva de grupo o GPC (*Group Policy Container*),
- la plantilla Directiva de grupo o GPT (*Group Policy Template*),

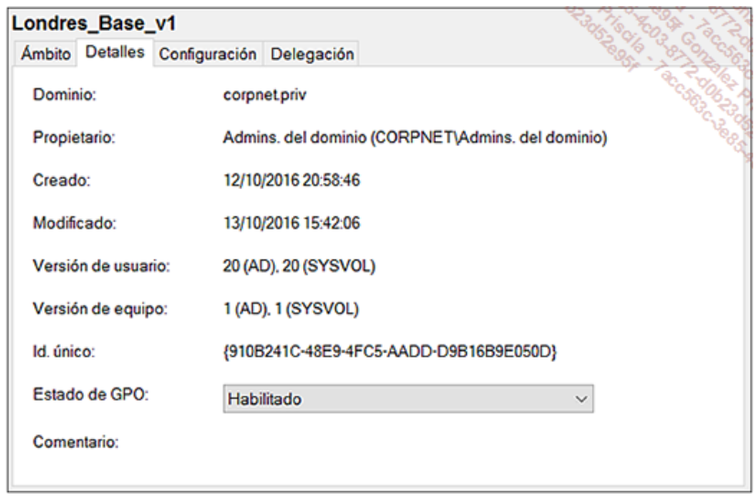
a. Objeto Contenedor de Directiva de grupo

El objeto contenedor de Directiva de grupo es un objeto del directorio que solo contiene el estado del objeto Directiva de grupo, sus datos de versión, información del filtro WMI del que pudiera disponer y una lista de los componentes cuyos parámetros se encuentran en el objeto Directiva de grupo.



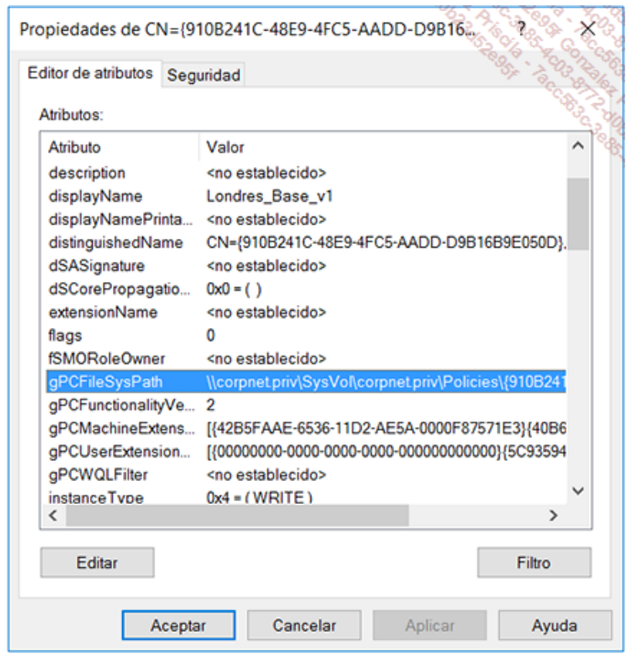
Ubicación de los objetos GPO dentro de la partición del directorio

Como podemos constatar, este contenedor está ubicado dentro de la partición de dominio en el contenedor System/Policies. Los equipos del dominio pueden acceder al contenedor Directiva de grupo para localizar las plantillas de Directivas de grupo. Los controladores de dominio acceden a éste si es necesario para obtener los datos de versión. Este parámetro es muy importante para garantizar la correcta replicación de la última versión del objeto Directiva de grupo.



Detalles de un objeto GPO e ID único.

La pantalla anterior ilustra las propiedades del objeto GPO llamado Londres_Base_v1 Observe el valor del ID único referenciado por un GUID.



GPO, almacenamiento en Active Directory y volumen SYSVOL

El atributo **gPCUserExtensionNames** define las extensiones CSE (*Client Side Extensions*) utilizadas para aplicar y actualizar los parámetros contenidos en la directiva de grupo. Por ejemplo, para implementar los parámetros de seguridad IPSec, el objeto referenciado por el GUID E437BC1C-AA7D-11D2-A382-00C04F991E27 en la ubicación del registro HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ GPExtensions será invocado y realizará las operaciones necesarias.

Estas diferentes extensiones, definidas dentro del objeto mismo, permiten verificar el soporte de las siguientes funciones:

- la redirección de carpetas;
- los parámetros del registro incluidos en las plantillas administrativas;
- los parámetros de cuotas de disco;
- los parámetros de QoS;
- la aplicación de los scripts;
- la aplicación de los parámetros de seguridad;
- los parámetros de recuperación EFS (*Encrypted File System*) ;
- la instalación y mantenimiento de las aplicaciones;
- la aplicación de los parámetros de seguridad IP (IPSec);

La imagen anterior muestra que un objeto de directiva de grupo está almacenado en una ubicación dada mediante una conexión de red de typo UNC. En nuestro ejemplo, el valor del atributo gPCFileSysPath apunta a la ruta DFS: \\corpnet.priv\SysVol\corpnet.priv\Policies\{GUID}

b. Plantilla de la directiva de grupo

Acabamos de ver que los atributos de un objeto de directiva de grupo ubicado en el contenedor System/Policies del dominio permite describir las características más fundamentales y necesarias.

¿Pero cuál es el contenido real de la directiva?

De hecho, la directiva de grupo está basada en una plantilla de partida. Esta plantilla es un árbol de carpetas ubicado en la carpeta SYSVOL de un controlador de dominio. Cada vez que creamos un nuevo objeto GPO, el controlador de dominio crea la plantilla de Directiva de grupo correspondiente. Esta plantilla contendrá todos los parámetros y datos de la directiva de grupo, incluyendo las plantillas administrativas, la configuración de seguridad, la instalación y mantenimiento de software, etc.

Los equipos cliente del dominio se conectarán a la carpeta SYSVOL mediante una ruta como la especificada a continuación: \\corpnet.priv\SysVol\corpnet.priv\Policies\{GUID}

El contenido de esta carpeta incluirá la plantilla GPT de la GPO a aplicar. El nombre de la carpeta de dicha plantilla corresponde al identificador único global (GUID) del objeto Directiva de grupo. Se trata del mismo número usado por Active Directory para identificar al objeto dentro del contenedor Directiva de grupo.

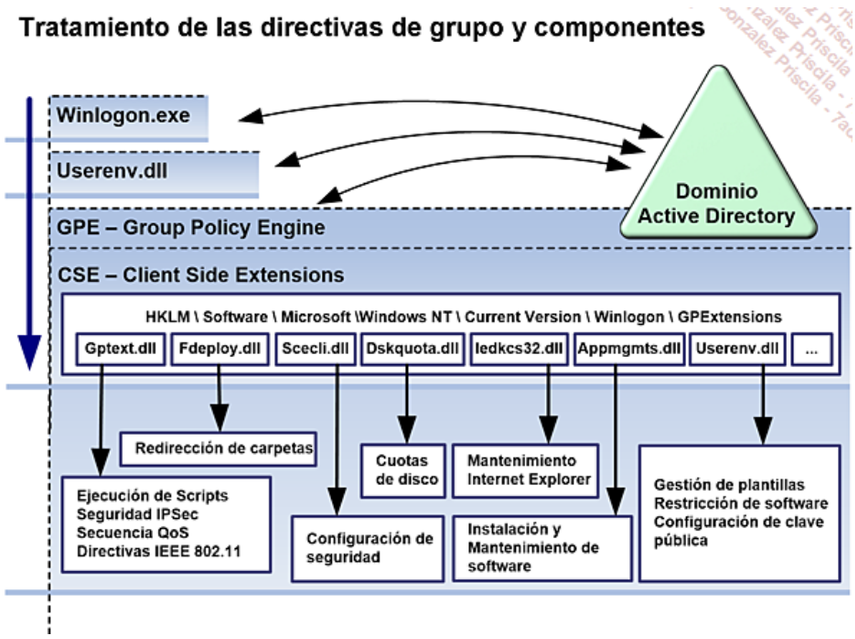
Para que un equipo cliente del directorio Active Directory pueda acceder a las directivas de grupo, debe poder acceder al volumen de sistema compartido Sysvol. Para esto, es indispensable que el servicio Sistema de archivos distribuidos esté operativo en todos los controladores de dominio.

Atención a la seguridad de los puestos de trabajo: la parte cliente DFS está integrada en el redirector Microsoft pero puede ser desactivada empleando la clave de registro HKLM\SYSTEM\CurrentControlSet\Services\Mup y el parámetro DisableDfs con un valor de tipo DWORD igual a 1. Si ese fuera el caso, el cliente no podría recorrer el volumen Sysvol y no podría, por tanto, aplicar los objetos GPO que le atañen. Para más información sobre el redirector DFS cliente y el componente MUP de Windows, busque "MUP and DFS Interactions" en el sitio Microsoft MSDN en la dirección: https://msdn.microsoft.com

c. Componentes de una directiva de grupo

La directiva de grupo contiene muchos parámetros y muy específicos. Es preciso que el equipo tenga cierta capacidad para "tratar" las muchas categorías de parámetros, todos muy diferentes entre sí.

La imagen siguiente muestra que los parámetros de las directivas de grupo son soportados por las plantillas siguientes.



Componentes del motor de tratamiento de las directivas de grupo

Proceso Winlogon.exe: se trata de un componente central del sistema operativo que proporciona servicios de inicio de sesión interactiva. El proceso Winlogon es el componente dentro del cual funciona el GPE. Winlogon es el único componente del sistema que interactúa con el GPE.

Userenv.dll: userenv.dll funciona dentro de Winlogon y alberga el GPE, así como la gestión de las plantillas administrativas.

GPE Group Policy Engine: se trata del módulo central de gestión de directivas de grupo. Soporta todas las funcionalidades mediante los múltiples CSE. La GPE funciona dentro de Userenv.dll.

Tenga en cuenta que en relación a sus predecesores, Windows 7 implementa un módulo cliente de directivas de grupo implementado bajo la forma de un servicio de Windows que arranca de forma automática. A partir de Windows 8 hasta Windows 10, el servicio cliente directiva de grupo arranca y se detiene de forma automática según sea necesario. El Administrador tiene, sin embargo, la posibilidad de desactivar esta optimización empleando el parámetro Desactivar la optimización AOAC del servicio cliente Directiva de grupo. Este parámetro de directiva - situado en la ubicación Configuración de equipo/ plantillas administrativas / Sistema / Directivas de grupo impide que el servicio cliente Directiva de grupo se detenga cuando está inactivo.

CSE Client Side Extensions: se trata de las extensiones especializadas capaces de soportar los diferentes parámetros a implementar.

Todos los componentes de tipo CSE se declaran en el registro con la clave **HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\ GPExtensions**.

Veremos más adelante durante la correcta verificación de las directivas de grupo que es importante conocer estas extensiones. En efecto, una directiva de grupo puede conocer ciertos problemas específicos relativos a los parámetros mas particulares que comprometen la integridad del componente o de la extensión CSE.

En la medida que los sistemas Windows disponen de nuevas funcionalidades, los componentes de la CSE siguientes se modifican para incluir estas nuevas funcionalidades. Por lo general, las nuevas funcionalidades y los parámetros asociados son implementados con las nuevas versiones de los sistemas operativos y a veces también con los *service packs*.

Como información, Windows 7 cuenta con alrededor de 40 extensiones CSE, mientras que Windows 10 tiene 50.

En la medida de las necesidades de configuración del puesto de trabajo Windows Client, Microsoft completa las funcionalidades de GPO y preferencias con nuevas extensiones CSE.

d. Plantillas de directiva de grupo ADMX para Windows 10

Aunque los principios fundamentales de las directivas de grupo sean de alguna forma inmutables desde Windows 2000 hasta Windows 10, pasando por Windows XP, hay que reconocer que a partir de Windows Vista los GPO han evolucionado más. Hemos visto antes que el contenido de los objetos directivas de grupo de Windows 7 se enriquecieron de forma significativa con más de dos mil cuatrocientos parámetros soportados como base, es decir, más de ocho cientos nuevos parámetros en relación a su predecesor Windows XP. Por supuesto, Windows 10 aporta su lote de nuevos parámetros, pero podemos considerar que ahora estas adiciones se centran en la configuración de las nuevas funcionalidades de Windows 10.

Como recordaremos, también indicamos que las nuevas familias de parámetros hicieron su aparición. De esta forma, las plantillas disponibles para Windows 7 y versiones posteriores son una evolución importante al soportar la gestión de la energía, el control de la instalación de controladores de dispositivos, la gestión uniforme y centralizada de los parámetros de seguridad del firewall e IPSec, así como el despliegue de las impresoras en función de los sitios.

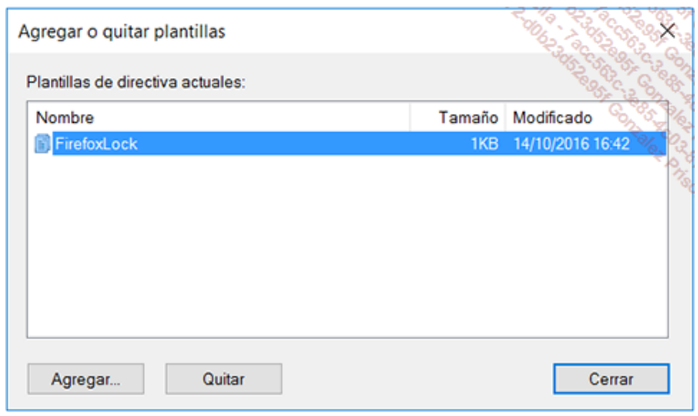
Con respecto a las particularidades de la implementación de GPO con Windows 7 y versiones posteriores, las plantillas de directivas de grupo evolucionan y se estructuran ahora en múltiples archivos XML. Este punto no extrañará a nadie, ya que hoy, ¡cualquier archivo de configuración debe estar en XML! Según Microsoft, el uso del XML estructura el archivo de forma muy clara de tal manera que los administradores podrán crear nuevas plantillas de forma muy sencilla.

Ahora debemos comprender los efectos de este nuevo formato de plantilla sobre el resto de la infraestructura. Presentamos estos puntos a continuación:

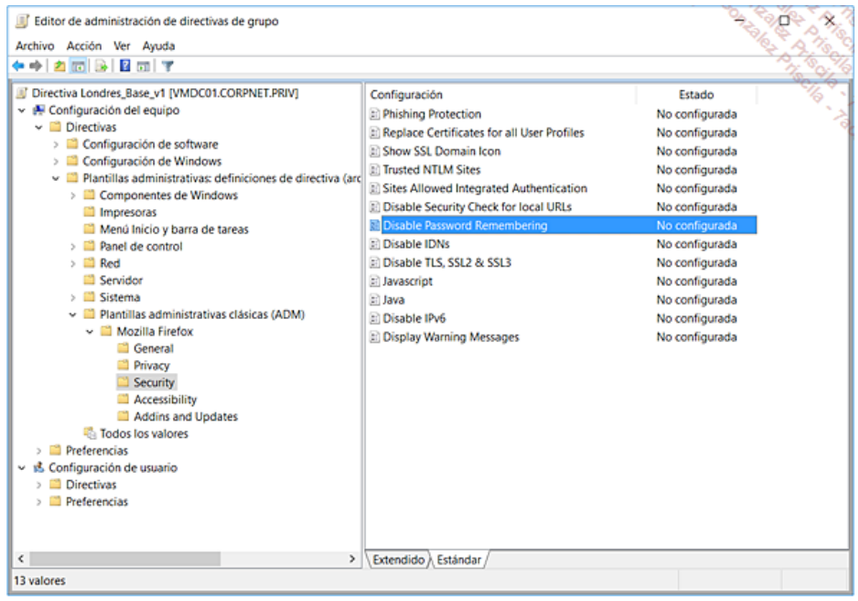
- Los nuevos archivos ADMX de Windows 10 o Windows Server 2016 permiten gestionar los GPO y GPP para todas las familias de sistemas operativos de Microsoft desde Windows 7 hasta Windows 10 y desde Windows Server 2008 R2 hasta Windows Server 2016. Aunque no mencionemos a Windows XP, que Microsoft ya no mantiene, la gestión de GPO para los equipos que todavía utilizan Windows XP Profesional SP3 está soportada.
- Los archivos de plantillas de administración ADMX previstos para ser utilizados con las consolas de gestión de directivas de grupo Windows 7 y versiones posteriores no están soportadas en las antiguas plataformas Windows XP.
- Aunque los objetos GPO creados a partir de Windows 7 o versiones posteriores hasta Windows 10 pueden residir en los controladores de dominio Windows Server más antiguos, ya no podemos editarlos en estas plataformas. En este caso, es necesario utilizar siempre la consola de gestión de directivas de grupo más moderna, por ejemplo desde un puesto de trabajo Windows 10 o un servidor Windows Server 2016.
- Las herramientas de administración de los GPO de versiones más modernas soportan, sin ningún problema la apertura y edición de objetos de directivas de grupo de Windows XP.

Microsoft recomienda que los administradores utilicen siempre las herramientas de administración más recientes. En efecto, conviene recordar que son las herramientas que realizan las operaciones solicitadas. Es importante limitar el uso de herramientas más antiguas en las plataformas más modernas. Con respecto a las directivas de grupo, la recomendación es utilizar con preferencia Windows 10 o como mínimo Windows 8.1, y la consola de gestión de directivas de grupo compatible con la plataforma elegida, para gestionar los objetos GPO basados en las nuevas plantillas ADMX. El hecho de disponer de la versión más moderna de las herramientas de administración RSAT nos permitirá gestionar los objetos directivas de grupo de los sistemas más modernos, garantizando la compatibilidad con los más antiguos hasta Windows XP. El punto más importante es sin duda la funcionalidad IEM - *Internet Explorer Maintenance*, retirada desde IE 10 en los entornos Windows 7 / Windows Server 2008 R2 y reemplazada por el uso de las GPP (*Group Policy Preferences*). Las GPP complementan muy bien las funcionalidades ofrecidas por los GPO, en particular con respecto a la configuración de Internet Explorer desde las versiones 5.0 hasta las versiones 10 y posteriores.

La imagen siguiente ilustra el caso de la utilización de una plantilla de administración de tipo ADM antigua empleando la consola de Windows 10 o Windows Server 2016.



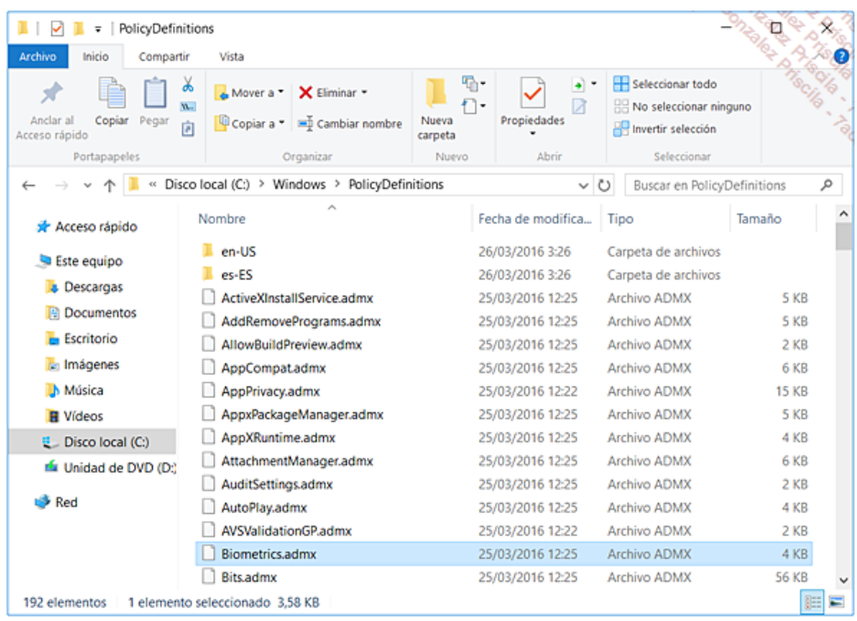
Añadir un antiguo archivo ADM



Adición de los antiguos modelos de administración convencionales (ADM)

- Los archivos ADM se sustituyen por los nuevos archivos ADMX, y por lo tanto son ignorados. Este punto se refiere solo a los archivos centrales como el conocido System.adm, así como los archivos adicionales Inetres.adm, Conf.adm, Wmplayer.adm y Wuau.adm. En el caso de que las modificaciones fueran introducidas en estos archivos ADM, deberán ser reimplementadas en sus nuevos homólogos en formato ADMX.
- A diferencia de los archivos ADM que existen en múltiples idiomas, los archivos ADMX son, al igual que las generaciones de sistemas operativos más modernos, independientes de los idiomas. En efecto, los archivos ADMX no contienen ninguna referencia al idioma, solo los datos de estructura. Este punto no implica que ninguna información de descripción de los parámetros de las directivas de grupo se almacena en los archivos de tipo ADMX. Estos datos se aíslan en archivos de descripción separados cuya extensión es ADML.

Archivos ADMX y ADML: esta nueva funcionalidad permite utilizar una única versión de un mismo archivo ADMX disponiendo de varias versiones de archivos ADML. De esta forma, es fácil disponer de archivos de idiomas diferentes, sabiendo que la Consola de edición de las directivas de grupo cargará de forma automática el archivo de idioma en función del sistema operativo. Esta nueva funcionalidad es por supuesto muy interesante para los administradores que podrán trabajar en una misma plantilla ADMX, y disponer de un archivo ADML adaptado a su lengua.



Plantillas ADMX y archivos de idiomas ADML

Para poder disponer de varios idiomas en el mismo equipo, basta con copiar los archivos necesarios en la carpeta de idioma adecuada, por ejemplo en-US para el idioma inglés/Estados Unidos.

- Con respecto a los archivos .POL: como era el caso con los antiguos archivos ADM, los archivos ADMX son sólo plantillas. En efecto, los parámetros configurados en la base a estas plantillas son codificados con detalle en un archivo binario llamado Registry.Pol. De esta forma, cuando las modificaciones de parámetros se basan en archivos de plantillas ADM o ADMX, todos los datos se combinan de forma final en un pequeño archivo .Pol de unos pocos kilobytes.

¡Observe! Aunque los parámetros existentes de forma previa en Windows XP en base a las plantillas ADM aplicados con más frecuencia en Windows 7 y versiones más modernas como Windows 10, los parámetros de directivas de grupo específicos a las versiones más modernas requieren la creación de un nuevo objeto GPO creado a partir de una equipo Windows del mismo nivel o superior. Esta observación se refiere solo a los nuevos parámetros de Windows ya que éstos solo se implementan a través de los nuevos modelos ADMX. Como hemos visto antes, los antiguos archivos ADM pueden simpre insertarse dentro de la consola de Administración de directivas de grupo.

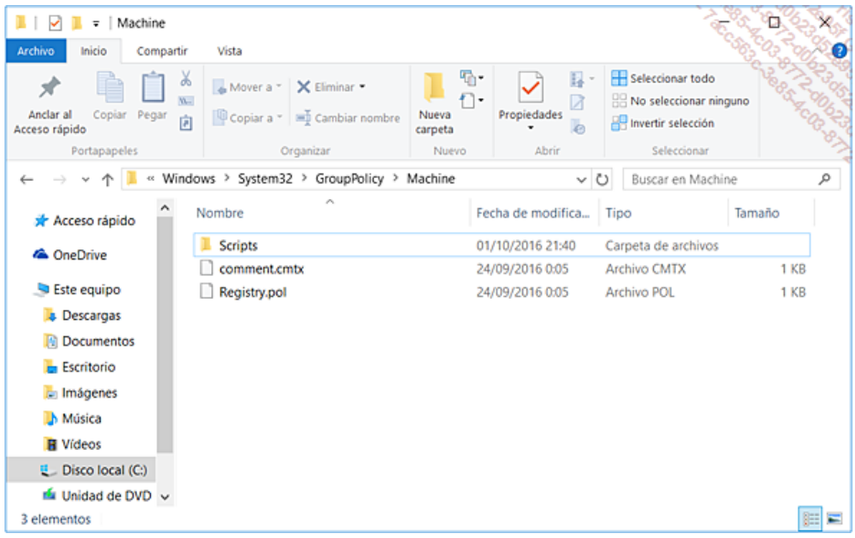
Creación de Central Store: almacenamiento de las plantillas de GPO

En las versiones previas de Windows, cuando un nuevo objeto directiva de grupo era creado, todos las plantillas añadidas por defecto al objeto GPO eran almacenadas dentro del mismo. En función de las versiones de Windows, el espacio consumido por un solo GPO podía alcanzar con facilidad 4 o 5 MB.

Algunas operaciones de infraestructura, como por ejemplo la actualización de controladores de dominio, podían causar picos de replicación

importantes, en especial cuando todas las plantillas de GPO -archivos ADM- debían ser replicados en todos los demás controladores de dominio.

Los sistemas como Windows 7 y versiones posteriores hasta Windows 10 permiten minimizar la replicación de todas las plantillas copiadas sin necesidad en cada objeto GPO aplicando un punto de almacenamiento centralizado dentro del volumen Sysvol que contiene la totalidad de los nuevos archivos ADMX. Además de esta optimización, conviene precisar que todos los objetos GPO creados mediante la consola de administración de directivas de grupo de Windows 7 y versiones posteriores no contienen más plantillas y solo representan algunos kilobytes en lugar de varios megabytes.



Los GPO han sido reducidos considerablemente...

El hecho de crear las GPO a partir de una estación de administración Windows 10 permite ahorrar no menos de 4 MB por GPO, ya que ningún ADM, ni ADMX se almacena aquí. Por último, en segunda instancia, la aplicación de DFS-R (*Distributed File System* - Replication) para la replicación del SYSVOL permitirá optimizar aún más el tráfico de replicación, en especial cuando el dominio Active Directory está compuesto por un gran número de controladores de dominio.

El siguiente cuadro resume las diferentes operaciones posibles en función de la estación de administración utilizada, es decir, la consola GPMC disponible en descarga para Windows XP SP2 y Windows Server 2003 o bien la consola GPMC disponible por defecto en Windows Server 2008 o Windows Vista.

Funcionalidades soportadas	GPMC Windows 7 a Windows 10	GPMC de Windows XP SP3
Puede administrar Windows Server 2003, Windows XP.	Si	Si
Puede administrar Windows y Windows. Server 2008 R2.	Si	No
Soporte multiidioma.	Si	No
Lectura de archivos ADM personalizados.	Si	Si
Ubicación por defecto de las plantillas.	En local en C:\Windows\ PolicyDefinitions	GPO
Utilización de Central store.	Si en \Sysvol\PolicyDefinitions	No
Evita los archivos duplicados en SYSVOL	Si	No
Posibilidad de añadir plantillas específicas.	Antiguos archivos ADM y nuevos archivos ADMX / ADML	Archivos ADM solo
Método de comparación de los archivos.	Número de versión	Timestamp

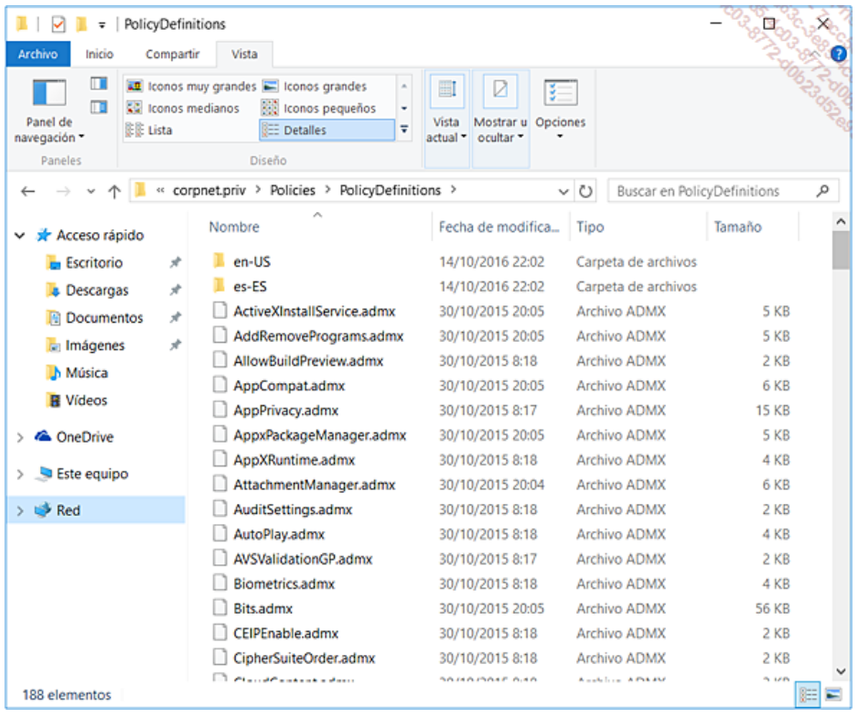
Consola de gestión de directivas de grupo y entornos Windows heterogéneos: ¡Tenga cuidado con el hecho de que las consolas GPMC en Windows 7, Windows 8, Windows 8.1 y Windows 10 presentan diferencias! Aunque algunas son menores, Microsoft recomienda de forma encarecida utilizar la consola de gestión de directivas de grupo más moderna, es decir, la disponible para Windows 10. Una buena práctica consiste en retirar las antiguas consolas para evitar la modificación accidental de objetos GPO utilizando los formatos más recientes.

e. Creación del Central Store dentro de SYSVOL

La creación del almacenamiento centralizado de las plantillas GPO en formato ADMX es un procedimiento manual. La estructura se crea de forma directa dentro del volumen de sistema SYSVOL en uno de los controladores de dominio del dominio. Luego, la replicación FRS (*File Replication Service*) o DFS-R, asumirá la replicación de la nueva carpeta a todos los controladores de dominio del dominio.

Una buena práctica consiste en crear el Central Store en el controlador de dominio que desempeña el papel de PDE (*Primary Domain Controller Emulator*). En efecto, las herramientas de administración tales como la consola de Gestión de directivas de grupo o también el editor de objetos de directivas de grupo seleccionan siempre por defecto el PDC de manera privilegiada.

Observe que cuando no existe Central Store, la consola del editor de objetos directivas de grupo utiliza archivos ADMX y ADML situados en el directorio local del equipo Windows en la ubicación \systemroot\PolicyDefinition.



Central Store:almacenamiento centralizado de los modelos ADMX

Para crear el almacenamiento centralizado, proceda como sigue:

A partir de un equipo Windows 10, copiar las últimas versiones de los archivos ADMX y ADML contenidos en la carpeta C:\Windows\PolicyDefinitions.

Abra una sesión en un controlador de dominio sabiendo que se recomienda seleccionar el controlador de dominio con el rol PDC Emulator.

Pegue la carpeta PolicyDefinitions copiada antes en c:\Windows\SYSVOL\domain\Policies del controlador de dominio.

Verifique que la replicación de la nueva carpeta \Policies\PolicyDefinitions se efectúa de forma correcta en el conjunto de los controladores de dominio del dominio.

f. Con respecto a las últimas versiones de plantillas ADMX para Windows 10 y Windows Server 2016

Encontraremos en el sitio de Microsoft los paquetes que contienen las últimas versiones de las plantillas ADMX para todos los sistemas operativos de Microsoft, así como la documentación asociada. Como ya se hemos explicado, se recomienda disponer de las últimas versiones de estas plantillas. En general están disponibles en descarga durante la salida de una nueva versión de Windows cliente o a veces también al publicar un Service Pack.

- Para descargar las plantillas de administración ADMX de Windows 10, regístrese en el vínculo http://www.microsoft.com/en-us/download/details.aspx?Id=48257. Observe que este paquete se ha actualizado y contiene los nuevos archivos ADMX adicionales no incluidos con la versión RTM de Windows 10.
- Para descargar las plantillas administrativas ADMX de Windows Server 2016, que soportan todas las versiones de Windows, así como la última versión de Windows Server, regístrese en el vínculo: https://www.microsoft.com/es-es/download/details.aspx?Id=51957.
- Para descargar la documentación de los archivos ADMX de Windows 10 y Windows Server 2016, regístrese en el vínculohttp://www.microsoft.com/en-us/download/details.aspx?Id=25250. Observe que esta descarga contiene los archivos ADMX y ADML en múltiples idiomas y son soportados sobre los sistemas cliente Windows 10, Windows 8.1, Windows 8, Windows 7 y en los servidores Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

Nota: directivas de seguridad para Windows 10: Podemos también añadir archivos ADMX relativos a de base de seguridad para Windows 10 (V1511, "Threshold 2") disponibles para descarga a través del enlace:https://blogs.technet.microsoft.com/secguide/2016/01/22/security-baseline-for-windows-10-v1511-threshold-2-final/

g. Recomendaciones para la administración de las GPO en entornos Windows Windows 7

Hemos visto que los puestos de trabajo Windows soportan un número importante de nuevos parámetros controlables empleando los objetos GPO. Las recomendaciones siguientes tienen por objeto facilitar la aplicación de los parámetros de configuración y respetar las mejores prácticas para aprovechar al máximo los aspectos más interesantes de las plataformas Windows y Windows Server.

- Debemos actualizar las estaciones de administración Windows actuales a Windows 10. Utilizaremos la nueva consola de administración de directivas de grupo disponible con las herramientas de administración de Windows 10 para todas las operaciones de administración de GPO.
- Crearemos un almacenamiento centralizado para gestionar con mayor facilidad todas las plantillas Windows en formato ADMX / ADML.
- Crearemos nuevos objetos GPO, tomando el tiempo de actualizar los antiguos, para aprovechar las nuevas funcionalidades que surgieron con Windows 7 y luego mejoradas con Windows 8.1 y Windows 10.

5. Aplicación de las directivas de grupo en el entorno Active Directory

a. Aplicación empleando el modelo S,D,UO y orden de tratamiento

La aplicación de las directivas de grupo es un proceso soportado de forma integral por el equipo cliente. No existe ningún tráfico iniciado por Active Directory hacia el puesto de trabajo.

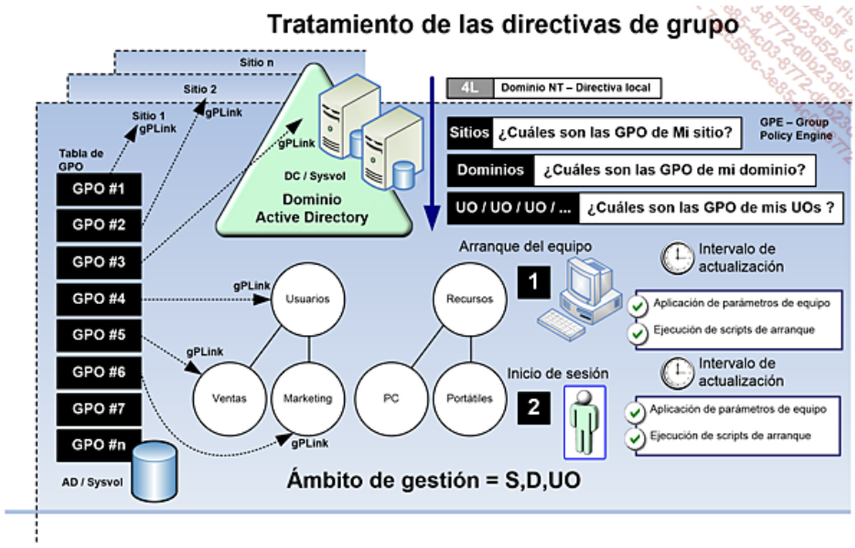
Las directivas de grupo que se aplican a un usuario o un equipo, o a los dos, no tienen las mismas prioridades. Sin embargo, el orden en las que se aplican respeta la fórmula L,S,D,UO. Esta fórmula significa directiva **Local**, y directivas de **Sitio**, luego directivas de **Dominio**, estrategias de **Unidades Organizativas** que contiene los objetos equipo y usuario determinado.

Los parámetros de la directiva de grupo son tratados en el orden siguiente:

- **Objeto de directiva de grupo local**: cada equipo dispone de un objeto de directiva de grupo almacenado de forma local. Se utiliza

para el tratamiento de los parámetros por defecto del equipo y el usuario, ya sea el equipo de un dominio Active Directory o no.

- **Sitio**: a continuación se tratan, los objetos de directiva de grupo vinculados al sitio al que el equipo pertenece. El proceso de más de una directiva se efectuará en el orden especificado por el Administrador, en la pestaña **Objetos de directiva de grupo vinculados para el sitio** en la consola de Administración de directivas de grupo GPMC (*Group Policy Management Console*), sabiendo que el objeto de la directiva de grupo situado en lo más alto será el que contará con la mayor prioridad.
- **Dominio**: la aplicación de varias directivas de grupo vinculadas al dominio se efectuará siguiendo el mismo principio de gestión de prioridades.
- **Unidades Organizativas**: por último, los objetos de directiva de grupo relacionados con la unidad organizativa de mayor nivel en la jerarquía de Active Directory se tratan en primer lugar, seguidos de los objetos de directiva de grupo relacionados con una unidad organizativa de segundo nivel, y así sucesivamente.



Ámbito de gestión de Active Directory y refresco de las directivas de grupo

El esquema siguiente ilustra el ámbito de gestión de la infraestructura Active Directory. Los contenedores Sitios, Dominio y Unidades Organizativas se encuentran presentes y contienen un equipo y un usuario. La secuencia siguiente explica el proceso completo del tratamiento de las directivas estrategias de grupo equipo y usuario comenzando por el arranque del equipo terminando con el inicio de sesión de un usuario en el ordenador.

1. La red se inicia. El Servicio RPCSS (*Remote Procedure Call System Service*) y el proveedor MUP (*Multiple Universal Naming Convención Provider*) inician.

Con respecto a los modos síncronos y asíncronos: los puestos de trabajo Windows 7 se inician de manera asíncrona y no tienen necesidad de esperar a que los componentes de red estén por completo inicializados. A diferencia de estos sistemas, Windows 2000 utiliza la misma secuencia pero de manera sincrónica. La aplicación del método asíncrono permite acelerar de forma significativa el arranque del sistema operativo. Observe que los equipos Windows 7 o posteriores hasta Windows 10 pueden ser configuradas a través de un parámetro de directiva de grupo para funcionar de manera síncrona.

2. Se obtiene para el equipo una lista ordenada de forma correcta de los objetos de directiva de grupo. Los siguientes factores pueden incidir en la composición de la lista:

- ¿Pertenece el equipo a un dominio Active Directory? En caso afirmativo, entonces se deberá considerar el proceso de descubrimiento de las directivas de grupo y aplicar las correspondientes.
- ¿En qué sitio Active Directory se ubica el equipo?
- Con respecto a la última ejecución de descubrimiento de objetos de directiva de grupo para el equipo, ¿existen modificaciones referentes a la lista de directivas a aplicar y/o han sido modificadas las directivas de grupo? En caso afirmativo, el tratamiento continúa, si no, no se ejecuta ninguna operación.
- ¿Disponen algunas directivas de modo obligatorio? Esta operación permite aplicar la directiva que dispone de este modo, aunque las unidades organizativas secundarias utilicen la opción **Bloquear herencia de directivas**.

En cuanto al modo de aplicar las directivas , aunque no hayan cambiado..." : un parámetro de directiva de grupo permite cambiar el comportamiento por defecto de las directivas de grupo para volver a aplicar las directivas, aun cuando no han cambiado. Este parámetro permite garantizar el correcto estado de las configuraciones y mantener un alto nivel de seguridad.

3. En este momento, las directivas de grupo son conocidas y aplicadas al equipo. Para obtener información detallada sobre la aplicación de las directivas de equipo, podemos activar los registros detallados a través de una directiva.

4. Los scripts de arranque se ejecutan de manera oculta y en modo síncrono, de uno en uno. Por defecto, cada script debe terminar para que el siguiente pueda arrancar. En el caso de que un script sea bloqueado, un plazo de ejecución de 10 minutos (600 segundos) o más será aplicado antes de continuar con el script siguiente, si es necesario. Los administradores disponen de varios parámetros de directivas para ajustar este comportamiento.

Preste atención al tratamiento en forma asíncrona en segundo plano: Windows 7 y versiones posteriores hasta Windows10, no esperan al arranque completo de la red para arrancar. Después del inicio de sesión, la directiva será tratada en segundo plano una vez que la red esté disponible. Esto significa que el equipo sigue utilizando los parámetros de directiva anteriores al arranque y al inicio de sesión. Por lo tanto, puede ser necesario y obligatorio realizar varios inicios de sesión sucesivos tras la modificación de una directiva para que los parámetros funcionen de forma adecuada. Este comportamiento se controla mediante el parámetro que figura en Configuración máquina\modelos de administración\Sistema\Inicio de sesión\ siempre esperar a la red en el arranque del ordenador y el inicio de sesión.

5. El usuario abre su sesión en un dominio Active Directory.

6. Tras la autenticación del usuario, el perfil del usuario se carga según los parámetros de directiva en vigor. Se obtiene para el usuario en sesión una lista ordenada de forma correcta de los objetos de directiva de grupo. Sin embargo, como en el caso del arranque del equipo, una serie de factores pueden incidir en la composición de la lista a aplicar:

- ¿Pertenece el usuario a un dominio? En este caso, estará sujeto a la directiva de grupo a través de Active Directory.
- ¿Está activado el bucle invertido? En caso afirmativo, este modo se configura para funcionar en modo fusión o en modo de sustitución?

El bucle, en inglés Loopback Processing Mode, permite gestionar la configuración de los equipos en autoservicio. Este comportamiento muy particular se detalla más adelante.

- ¿Cuál es la ubicación del usuario en Active Directory? ¿En qué sitio, en qué dominio y en qué jerarquía de unidades organizativas?
- ¿Disponen algunas directivas de modo obligatorio? Esta operación permite aplicar la directiva que dispone de este modo, aunque las unidades organizativas secundarias utilicen la opción **Bloquear herencia** de las directivas.

7. Las estrategias de grupo son por último determinadas y aplicadas al usuario en sesión.

8. Los scripts de inicio de sesión se ejecutan con los mismos principios que los que se refieren a los equipos.

9. Por último, la carga de la interfaz del usuario se realizará en función de los parámetros declarados en las directivas de grupo.

b. Dominios Active Directory y dominios NT: L, S, D, UO y 4, L, S, D, UO

Estas pocas líneas se refieren a la problemática propia de los entornos no Active Directory, tales como los que funcionaban bajo Windows NT (ideben ser muy raros hoy!), o de antiguos dominios LAN Manager que se ejecutan en versiones antiguas de Samba bajo Linux. Estos dominios, comprendiendo a los usuarios de dominios NT, podrán ser aprobados para trabajar en equipos miembros de un dominio Active Directory. Podrán, por supuesto, en función de sus permisos, acceder a cualquier recurso del dominio o de otros dominios Windows, miembros del bosque.

Debemos considerar tres grandes casos:

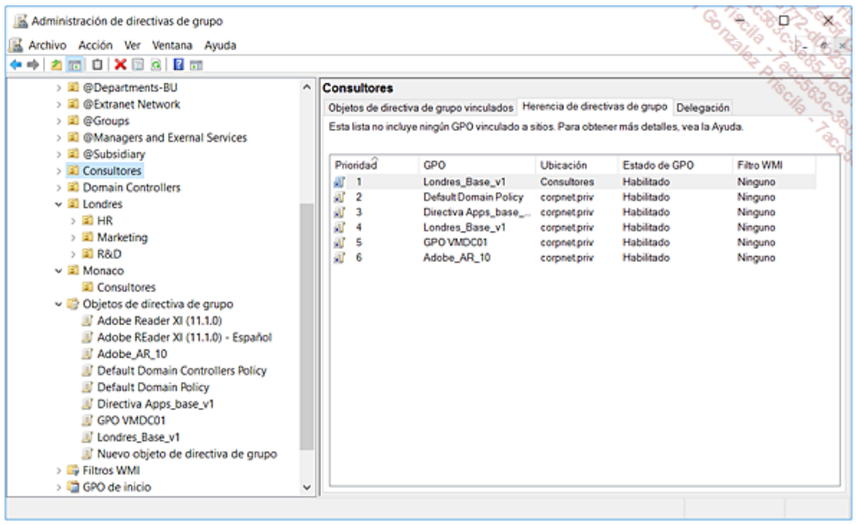
- Si el equipo cliente se encuentra en un dominio NT y el usuario se encuentra en Active Directory, sólo la directiva de sistema del equipo será tratada (y no la del usuario) durante el inicio de sesión. Luego, sólo se aplicará la directiva de grupo del usuario.
- Si el equipo se encuentra en Active Directory y el usuario se encuentra en un dominio NT, la directiva de grupo del equipo (y no la del usuario) será tratada durante el arranque del equipo. Cuando el usuario abre la sesión, sólo se trata la directiva sistema del usuario.
- Si las cuentas de equipo y usuario pertenecen a un dominio NT, sólo la directiva de sistema se aplica cuando el usuario inicia la sesión.

Aunque esto es hoy obsoleto, no confunda directivas de sistema y directivas de grupo. Las directivas de sistema, en inglés System Policy, se implementaban en los entornos de dominio NT para equipos en las antiguas versiones de Windows tales como Windows NT 4.0.

c. Vínculos de las directivas de grupo a los objetos Sitios, Dominios, Unidades organizativas y mecanismo de herencia

Como acabamos de ver, una directiva de grupo puede estar vinculada al nivel de múltiples contenedores de tipo S,D,UO dentro de una jerarquía de Active Directory.

De igual forma, contamos con la posibilidad de vincular varias directivas de grupo en el mismo dominio o la misma UO, o no vincularlo con ninguna. En este caso, nos beneficiamos de los mecanismos de herencia. Si varios objetos de directiva de grupo están relacionados con una unidad organizativa, contamos con la posibilidad de controlar su orden de aplicación utilizando la pestaña **Objetos de directiva de grupo vinculados** de la unidad organizativa en la consola GPMC.



Herencia, vínculos y prioridad de los objetos GPO

El objeto directiva estrategia de grupo con el orden de los vínculos más bajo es tratado como último y recibe la prioridad más alta. El gráfico anterior representa la información necesaria para "operar" y entender de forma correcta para comprender por qué esta directiva de grupo se debe considerar con mayor prioridad que otra.

Los datos siguientes nos permitirán entender la importancia de los parámetros de las directivas de grupo vinculadas a un contenedor dado.

El orden de vínculos: este parámetro nos permite administrar el orden de tratamiento de las directivas por el GPE, *Group Policy Engine*. Como ya se ha explicado antes, la directiva de grupo con el orden de los vínculos siguientes se trata como último y por lo tanto, con la más alta prioridad.

Aplicado: la relación de un objeto de directiva de grupo puede aplicarse, desactivarse o ambas. Por defecto, el vínculo de un objeto de directiva de grupo no está ni aplicado ni desactivado. Desconfiemos de esta opción. Cuando el vínculo está **Activado**, la directiva de grupo está "conectada" en el contenedor. Cuando el vínculo está **Aplicado**, entonces la directiva de grupo en cuestión tiene prioridad sobre el parámetro **Bloquear la herencia** de un dominio o de una unidad organizativa. Además, si activamos **Aplicado** y desactivamos **Vínculo habilitado** para un vínculo, entonces el objeto de directiva de grupo no será aplicado.

Bloquear la herencia esta opción protege el contenedor de la herencia proveniente de otros contenedores de niveles superiores. Observe sin embargo que la activación de la opción **Bloquear herencia** no se aplica a los parámetros de la directiva de grupo de los objetos de directiva de grupo que están directamente vinculados al dominio. Observe también que el bloqueo de la herencia aplicado sobre una unidad organizativa se simboliza por un punto de exclamación de color azul situado en la UO.

d. Vínculos y atributo gPLink

Los objetos contenedores de tipo Sitios, Dominios y Unidades Organizativas son las únicas clases de objetos del directorio que cuentan con el atributo **gPLink**.

Este atributo es fundamental, ya que permite a los distintos tipos de contenedores "aferrarse" a los objetos de directivas de grupo. En

efecto, el atributo gPLink cuya OID es 1.2.840.113556.1.4.891 es un atributo utilizado por las clases Site, Organizational-Unit y Sam-Domain. Como información, la versión del esquema de Active Directory prevé que el atributo gPLink esté también disponible para el contenedor Configuración que incluye la partición de configuración de Active Directory.

e. Selección del controlador de dominio preferido

La consola de administración de directivas de grupo utiliza el controlador de dominio que actúa como maestro de operaciones "PDC Emulator" de cada dominio como controlador de dominio por defecto para todas las operaciones de creación y modificación de las directivas de grupo.

Para evitar los conflictos de replicación, se recomienda elegir un controlador de entre los que se disponga como favorito para las operaciones que se refieren a la administración de las directivas de grupo. En efecto, hemos visto antes que los objetos directivas de grupo estaban compuestos de dos partes distintas: la parte contenedor de directiva de grupo dentro de la partición de dominio Active Directory y la parte plantilla de directiva de grupo dentro del volumen compartido SYSVOL. Estos dos espacios de almacenamiento utilizan mecanismos de replicación independientes. Por lo tanto, si dos administradores realizan cambios durante el mismo ciclo de replicación de un mismo objeto directiva de grupo en controladores de dominio diferentes, las modificaciones introducidas por uno de los administradores pueden perderse.

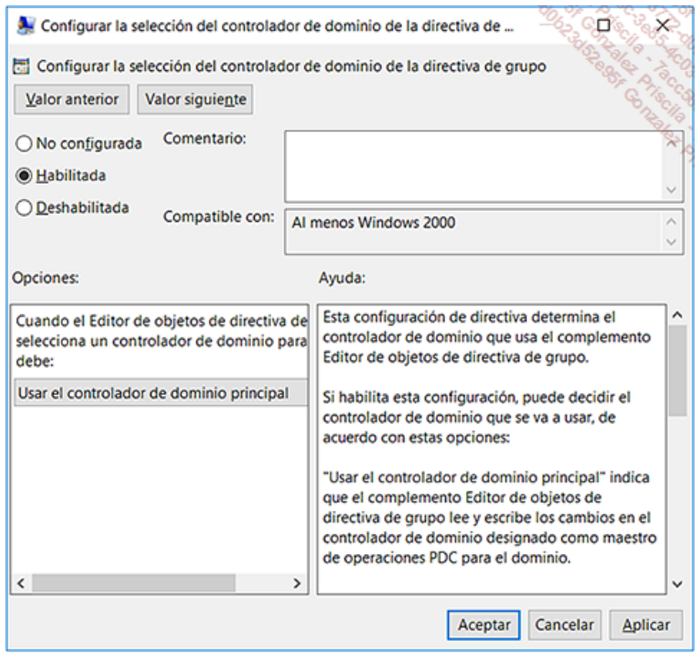
Por defecto, la consola de Administración de directivas de grupo utiliza el emulador PDC del dominio para garantizar que todos los administradores usan el mismo controlador de dominio. Sin embargo, es posible que deseemos de forma puntual solicitar un controlador de dominio particular situado en un sitio remoto.

Si varios administradores gestionan la misma directiva de grupo al mismo tiempo, se recomienda que seleccionen el mismo controlador de dominio. Esta selección permitirá evitar colisiones de replicación a nivel del servicio de replicación de archivos FRS (*File Replication Service*) o DFS-R.

La consola de administración de directivas de grupo le permite cambiar el controlador activo que realizará las modificaciones.

Esta operación es, en nuestro ejemplo, una tarea manual que se realizará en función de las necesidades de administración.

Tenemos no obstante, la posibilidad de cambiar la forma en que el controlador de dominio por defecto se selecciona. Por ejemplo, podemos crear una nueva directiva de grupo al estilo de los administradores y configurar así: **Configuración de usuario/Directivas/Plantillas administrativas/Sistema/Directiva de grupo/Configurar la selección del controlador de dominio de la directiva de grupo**. Active la opción y seleccione entre las tres opciones la que mejor se adapte a su entorno de administración.



Selección del controlador de dominio a utilizar con la consola de Administración de directivas de grupo

Usar el controlador de dominio principal: se trata de la opción por defecto. Esta opción indica que el componente **Editor de objetos de directivas de grupo** lee y escribe los cambios en el Controlador de Dominio designado como supervisor de operaciones PDC Emulator para el dominio en que la operación se realiza.

Heredar de complementos de Active Directory: esta opción indica que el componente **Editor de objetos de directivas de grupo** lee y escribe los cambios en el controlador de dominio que las consolas de gestión MMC **Usuarios y equipos de Active Directory** o **Sitios y servicios de Active Directory** utilizan.

Usar cualquier controlador de dominio disponible: esta opción indica al componente **Editor de objetos de directivas de grupo** que se puede utilizar cualquier controlador de dominio disponible.

Si desactiva esta opción o si no la configuramos, el Editor de objetos de directivas de grupo utiliza el controlador de dominio designado como el maestro de operaciones de controlador de dominio primario para el dominio.

6. Creación de un objeto de directiva de grupo con la consola GPMC

Como hemos visto antes, Microsoft recomienda que los administradores utilicen las últimas versiones de las herramientas de administración. En la medida en que estas herramientas tienen lo que les pedimos, es bueno poder contar con las herramientas más eficaces, tanto desde un punto de vista de estabilidad, como las facultades de estas herramientas para simplificar algunas tareas complejas. Recordemos que las herramientas de administración RSAT (*Remote Server Administration Tools*) de Windows 10 están disponibles para descargar en el sitio de Microsoft.

Las operaciones siguientes se refieren a la consola de administración de directivas de grupo GPMC.

Para descargar las herramientas de administración remota de servidor para Windows 10, use el vínculo http://www.microsoft.com/en-us/download/details.aspx?Id=45520 o busque "Remote Server Administration Tools" en el sitio de Microsoft. Observe que esta última versión incluye el soporte para Windows Server 2016.

a. Creación de una directiva de grupo no vinculada

En el árbol de la consola:

Haga un clic con el botón derecho sobre **Objetos de directiva de grupo** en el bosque y el dominio donde quiere crear el objeto de directiva de grupo (GPO, *Group Policy Object*). Para poder ubicarnos, siga la ruta **Nombre del bosque/Dominios/Nombre de**

dominio/Objetos de directiva de grupo.

Haga clic en **Nuevo**.

En el cuadro de diálogo **Nuevo GPO**, especifique un nombre para el nuevo objeto de directiva de grupo y haga clic en **Aceptar**.

b. Creación de una directiva de grupo vinculada

En el árbol de la consola:

Haga un clic con el botón derecho sobre el nombre de dominio, en el bosque en el que desea crear y vincular un objeto de directiva de grupo. Para poder ubicarnos, siga la ruta **Nombre del bosque/Dominios/Nombre de dominio** y vaya al contenedor deseado.

Haga clic en **Crear un GPO en este dominio y vincularlo aquí**.

En el cuadro de diálogo **Nuevo GPO**, especifique un nombre para el nuevo objeto de directiva de grupo y haga clic en **Aceptar**.

c. Administración de vínculos de directivas de grupo

La gestión de los vínculos es una operación técnicamente simple, pero tan pesada como sea de amplia la infraestructura de administración de Active Directory. En efecto, la creación de un vínculo puede prestar grandes servicios a los equipos y/o usuarios, pero también puede causar molestias e incluso problemas de funcionamiento para otros.

Es por esta razón que se diseño la consola de administración GPMC. Presentaremos más adelante las funcionalidades de modelización y análisis necesarios para una gestión más fácil y con menos riesgos de las directivas de grupo.

Vincular una directiva de grupo existente

Para vincular un objeto de directiva de grupo ya existente, haga un clic con el botón derecho sobre el dominio o unidad organizativa del dominio y haga clic en **Vincular un GPO existente**.

En el cuadro de diálogo **Seleccionar GPO**, haga clic sobre el objeto de la directiva de grupo que desea vincular, y luego el botón**Aceptar**.

Desactivar un vínculo de directiva de grupo

Vaya al bosque que contiene el dominio, el sitio o la unidad organizativa que incluye la relación de objeto de directiva de grupo que deseamos desactivar.

Haga un clic con el botón derecho sobre el vínculo de objeto de directiva de grupo deseado: una marca al lado de **Vínculo habilitado**indica que el vínculo está activado.

Haga clic en **Vínculo habilitado** para borrar la marca y desactivar el vínculo.

Para efectuar esta operación, debemos contar con el permiso **Vincular objetos GPO** para el dominio, el sitio o la unidad organizativa organización que contenga el vínculo de objeto de directiva de grupo. Si no es el caso, la opción **Vínculo habilitado** no estará disponible.

d. Eliminar una directiva de grupo

Vaya al árbol de la consola de administración de directivas de grupo, haga doble clic en **Objetos de directiva de grupo** en el bosque y el dominio con el objeto de directiva de grupo que deseamos eliminar.

Haga clic con el botón derecho sobre el objeto de la directiva de grupo y haga clic en **Eliminar**.

Cuando se solicite confirmar la eliminación, haga clic en **Aceptar**.

Para crear un objeto de directiva de grupo, debemos disponer de los privilegios de creación de objetos de directiva de grupo. Por defecto, sólo los Administradores de dominio, los Administradores de empresas y los miembros del grupo de Propietarios creadores de directiva de grupo pueden crear objetos de directiva de grupo.

Para eliminar un objeto de directiva de grupo, debemos tener los permisos **Editar configuración**, **Eliminar** y **Editar la seguridad** para el objeto de la directiva de grupo.

e. Desactivar una directiva de grupo

Para desactivar todo o parte de un objeto directiva de grupo nos ubicamos sobre el objeto directiva de grupo que contiene los parámetros de usuario o equipo que deseamos desactivar, seleccionamos la pestaña **Detalles**, señalamos **Estado de GPO**, y luego realizamos una de las acciones siguientes:

- Hacemos clic en **Configuración de usuario deshabilitada** para desactivar la configuración de usuario del objeto. Una marca de verificación al lado de **Configuración de usuario deshabilitada** indica que la configuración de usuario está desactivada.
- Hacemos clic en **Configuración de equipo deshabilitada** para desactivar la configuración de equipo del objeto. Una marca de verificación al lado de **Configuración de equipo deshabilitada** indica que la configuración de equipo está desactivada.

Para desactivar un objeto de directiva de grupo, debemos disponer del permiso **Editar** para el objeto directiva de grupo.

f. Gestión de conflictos de tratamiento de las directivas de grupo

Conflictos entre los parámetros

Los parámetros controlados por una directiva pueden ser configurados de diferentes formas.

No configurado: este estado significa que el parámetro no se gestiona. No se efectúa ninguna operación.

Habilitada: este estado significa que el parámetro está activo. Si varias directivas de grupo se refieren al mismo parámetro para el mismo objeto equipo o usuario, entonces se aplicará el último parámetro, es decir aquel que disponga de la mayor prioridad prevalecerá.

Deshabilitada: este estado significa que el parámetro está inactivo. Si varias directivas de grupo se refieren al mismo parámetro para el mismo objeto equipo o usuario, entonces se aplicará el último parámetro, es decir aquel que disponga de la mayor prioridad prevalecerá.

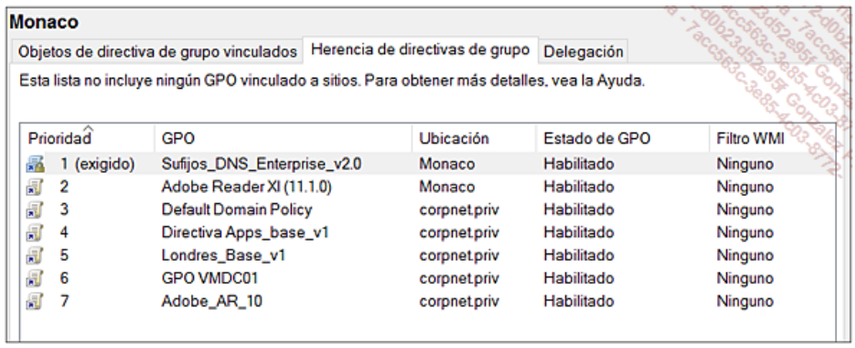
Opción Exigido (antes No reemplazar)

Un administrador puede definir una directiva en un nivel más elevado para que siempre se aplique. Este proceso, llamado "Exigir" con GPMC,

se conocía antes como el término "No reemplazar". Un administrador puede definir un contenedor para bloquear la aplicación de las directivas de los niveles superiores.

Una directiva definida por el administrador en un nivel superior para ser aplicada continuará del mismo modo con un bloqueo de nivel superior.

La pantalla siguiente muestra la opción habitual **Exigido**.



*Prioridad máxima empleando la opción **Exigido** en un objeto GPO*

Bloquear la herencia

Podemos optar por bloquear la herencia de directiva para un dominio o una unidad organizativa. El uso del bloqueo de herencia impide que los objetos de directiva de grupo vinculados a los sitios, dominios o unidades organizativas de niveles superiores sean heredados de forma automática por los niveles secundarios. Por defecto, los contenedores secundarios heredan el conjunto de objetos de directiva de grupo principal, pero a veces puede ser útil bloquear esta herencia.

Por ejemplo, si desea aplicar un único conjunto de directivas en un dominio entero con excepción de una unidad organizativa, podemos vincular los objetos de directiva de grupo requeridos dentro del dominio (a partir del cual todas las unidades organizativas heredan las directivas por defecto), luego bloquear la herencia solo para la unidad organizativa para las que las directivas no deben ser aplicadas.

Esta posibilidad se muestra en la figura anterior.

Para realizar esta operación empleando la consola de administración de directivas de grupo, seguimos este procedimiento:

Diríjase al dominio o una unidad organizativa.

Hacemos un clic con el botón derecho en el contenedor seleccionado.

Seleccionamos la opción **Bloquear herencia**.

g. Gestión de filtrado del despliegue de las directivas de grupo

El filtro de seguridad permite redefinir los usuarios y equipos que recibirán y aplicarán los parámetros de un objeto directiva de grupo.

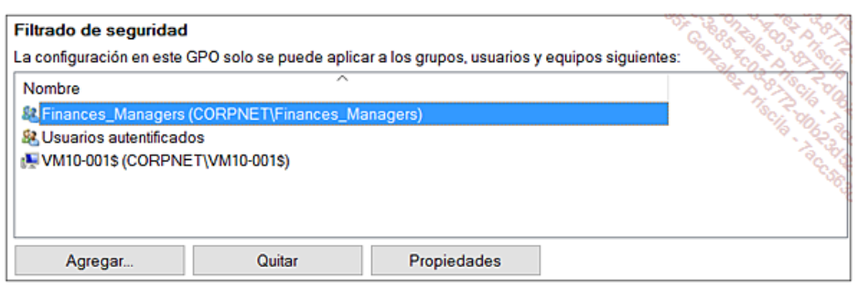
Empleando el filtro de seguridad, podemos especificar que sólo algunas de las entidades de seguridad de un contenedor al que está vinculado el objeto de directiva de grupo aplicarán la directiva de grupo. El filtro de grupo de seguridad determina si el objeto de la directiva de grupo se aplica en su conjunto a los grupos, usuarios o equipos.

Para que el objeto de la directiva de grupo se aplique a un usuario o a un equipo determinado, este usuario o equipo debe poseer dos permisos indispensables:

- Debe ser capaz de abrir, por lo tanto, de **Leer** la directiva de grupo,
- También debe contar con el permiso **Aplicar directiva de grupo** sobre el objeto de la directiva de grupo, ya sea de manera explícita o a través de la pertenencia habitual a un grupo.

Permisos por defecto en los objetos directivas de grupo: por defecto, el valor de los permisos **Leer** y **aplicar directiva de grupo** están definidos como **Habilitado** para todos los objetos de directiva de grupo del grupo de **Usuarios autenticados**. Observe que para que los administradores puedan aplicar una directiva de grupo, los permisos por defecto de los grupos Administradores de empresas y Administradores del dominio no son suficientes. Necesitaremos, en este caso, añadir al grupo de los Administradores del dominio el permiso**Aplicar directiva de grupo**.

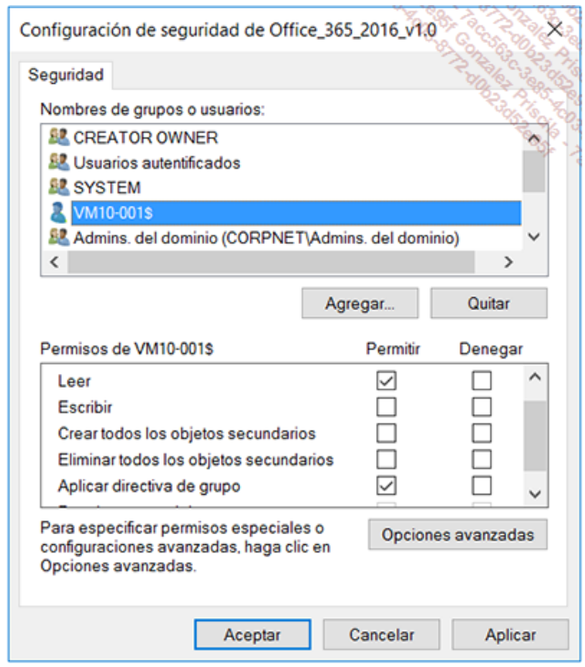
El ejemplo siguiente ilustra una operación de filtrado realizada empleando la consola GPMC.



Filtrado empleando equipos, usuarios y grupos

El Grupo Usuarios autenticados incluye a los usuarios y equipos. Es de esta forma que todos los usuarios autenticados reciben los parámetros de un nuevo objeto de directiva de grupo cuando éste se aplica a una unidad organizativa, en un dominio o un sitio. Como mostramos en la figura anterior, podemos cambiar estos permisos para limitar el alcance a un conjunto específico de usuarios, grupos o de equipos en la unidad organizativa, el dominio o el sitio.

La figura anterior muestra también que la consola MMC **Administración de directivas de grupo** administra dichos permisos como una sola unidad. Así, la declaración a realizar es más sencilla. Para cambiar el filtro de seguridad, podemos añadir o eliminar los grupos en la sección**Filtrado de seguridad** en la pestaña **Ámbito** de un objeto de directiva de grupo. En la práctica, no es necesario crear las dos entradas (**Leer** y**Aplicar directiva de grupo**), ya que la consola GPMC los define de forma automática. Por contra, siempre es posible editar y modificar los permisos en el modo avanzado. Para esto, podemos abrir el editor de listas de control de acceso haciendo clic en el botón **Opciones avanzadas...** en la pestaña **Delegación** del objeto de directiva de grupo.



Permisos: Leer y Aplicar directiva de grupo

h. Puntos importantes

- Los objetos directiva de grupo sólo pueden estar vinculados a los sitios, dominios y unidades organizativas.
- En el marco de los principios de la tecnología IntelliMirror, los objetos de directiva de grupo no pueden estar vinculados de forma directa a usuarios, equipos o grupos de seguridad.
- El filtro de seguridad nos ayudará a limitar el alcance de un objeto directiva de grupo para que se aplique solo a un grupo, a un usuario o a un único equipo.
- Los permisos **Leer** y **Aplicar directiva de grupos** no son suficientes para garantizar que una directiva de grupo se aplique para un usuario o un equipo determinado. El objeto directiva de grupo también debe estar vinculado a un sitio, un dominio o a una unidad organizativa con el usuario o el equipo, ya sea de forma directa o a través de los mecanismos de herencia.
- La ubicación de los grupos de seguridad en Active Directory no tiene nada que ver con el filtrado empleando los grupos de seguridad. Los grupos no tienen ninguna relación directa con el tratamiento de las directivas de grupo. Los grupos son sólo un medio de gestionar los permisos sobre los objetos. Permiten así obtener los permisos **Leer** y **Aplicar directiva de grupos**.
- Filtrado empleando la interfaz WMI.

Prestar atención a los conflictos entre los parámetros y las opciones **Aplicar** y **Bloquear herencia** de los objetos directivas de grupo en los contenedores del tipo unidades organizativas.

i. Definición de filtros WMI

Funcionamiento de los filtros WMI

Podemos utilizar los filtros WMI para determinar de forma dinámica el alcance de las directivas de grupo a partir de los atributos conocidos de tipos de usuario o equipo. De esta manera, podemos ampliar la capacidad de filtrado de los objetos directiva de grupo más allá de los mecanismos de inspección de seguridad presentados antes.

Un filtro WMI está asociado a un objeto directiva de grupo. Cuando aplicamos un objeto directiva de grupo en el equipo de destino, Active Directory evalúa el filtro en el equipo de destino. Un filtro WMI estará compuesto por una o varias peticiones evaluadas por Active Directory en función del espacio de almacenamiento WMI del equipo de destino. Si el valor total de las peticiones es falso (false), Active Directory no aplica el objeto directiva de grupo. Si todas las peticiones son verdaderas (true), entonces Active Directory aplica la directiva de grupo.

Las peticiones WMI están escritas empleando el lenguaje WQL, *WMI query language*. Este lenguaje es muy parecido al lenguaje SQL y permite interrogar la totalidad del espacio de almacenamiento WMI.

Cada objeto directiva de grupo solo puede referirse a un filtro WMI que puede contener varias condiciones. En cambio, podemos vincular un mismo filtro WMI a varios objetos de directiva de grupo. La interfaz de la consola de administración de directivas de grupo nos permite crear, importar, exportar, copiar y pegar filtros WMI con mucha facilidad.

¿Cómo crear un filtro WMI?

Abrir la consola de **Administración de directivas de grupo**.

En el árbol de la consola, haga un clic con el botón derecho sobre **Filtros WMI** en el bosque y el dominio en el que deseamos crear un filtro WMI. Para hacer esto, nos dirigimos a **Nombre del bosque/Dominios/Nombre del dominio/Filtros WMI**.

Hacemos clic en **Nuevo**.

En el cuadro de diálogo **Nuevo filtro WMI**, introducir el nombre para el nuevo filtro y luego una descripción en la zona **Descripción**.

Hacemos clic en **Agregar**.

En el cuadro de diálogo **Consulta de WMI**, seleccionamos el **Espacio de Nombres** o dejamos el espacio de nombres por defecto,**root\CIMv2**.

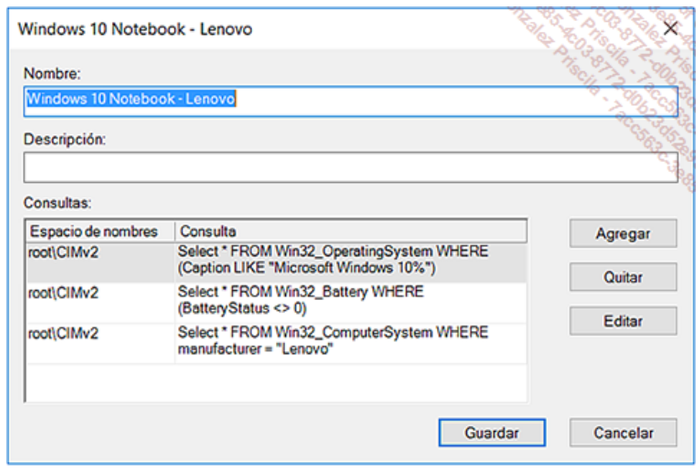
En la zona **Consulta** teclee una consulta WMI y haga clic en **Aceptar**.

Para añadir otras consultas, repita los tres últimos pasos para cada nueva consulta.

Después de añadir todas las consultas, haga clic en **Guardar**.

Creación de filtros WMI y privilegios necesarios: para poder crear filtros WMI, debemos tener los permisos necesarios para esta operación. Los grupos Administradores de dominio, Administradores de empresas y Creadores (Creator Owner) de la directiva de grupo cuentan por defecto con estos permisos.

La imagen muestra los detalles relativos a la creación del filtro. Como se explica más arriba, debemos declarar el nombre del filtro, una descripción, el espacio WMI al que se refiere la consulta, así como el contenido de dicha consulta.



Filtro WMI y condiciones a verificar

Una vez creados los filtros WMI, no queda más que asociar el filtro de la directiva de grupo afectada por la operación de filtrado.

¿Cómo vincular un filtro WMI a un objeto de directiva de grupo en particular?

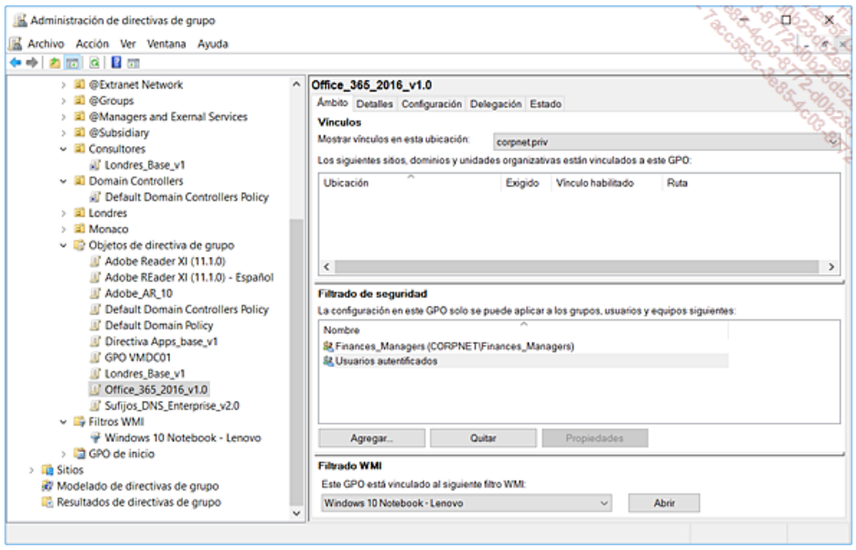
Abrir la consola de **Administración de directivas de grupo**.

En el árbol de la consola, vayamos al objeto directiva de grupo para el cual deseamos vincular un filtro WMI. Para conseguirlo, vayamos a **Nombre del bosque/Dominios/Nombre del dominio/Objetos de directiva de grupo** y hacemos clic en el objeto directiva de grupo.

En la solapa de resultados, bajo la pestaña **Ámbito**, en **Filtro WMI**, seleccione un filtro WMI de la zona de la lista desplegable.

Cuando se solicite confirmar la selección, haga clic en **Si**.

La pantalla siguiente ilustra esta operación realizada empleando la consola de administración de directivas.



Vínculo de un objeto GPO en un filtro WMI

También tenemos la posibilidad de ir al nodo **Filtros WMI** y seleccionar de forma directa el objeto filtro WMI para el que interesa controlar los vínculos, los permisos relativos a la delegación de control en los filtros WMI y el contenido del código del filtro.

También podemos vincular un filtro WMVI a un objeto de directiva de grupo aplicando el método siguiente: en el árbol de la consola, arrastramos el filtro WMI al objeto de directiva de grupo al que lo queremos vincular.

Para vincular un filtro WMI a un objeto de directiva de grupo, debemos disponer de los privilegios de modificación en el objeto de directiva de grupo. Solo puede vincularse un filtro WMI a un objeto de directiva de grupo. Si intentamos vincular un filtro WMI a un objeto de directiva de grupo en el que ya se encuentra un filtro WMI, el sistema preguntará si deseamos reemplazar el anterior filtro por el nuevo. Podemos vincular solo un filtro WMI a un objeto de directiva de grupo del mismo dominio.

Para eliminar un filtro WMI, en el árbol de la consola, efectuamos un clic con el botón derecho en el filtro WMI a eliminar, y luego hacemos clic en **Eliminar**. Cuando se solicite confirmar la eliminación, hacer clic en **Si**.

Soporte de los filtros WMI y versiones de Windows: los filtros WMI funcionan en todas las plataformas Windows y Windows Server. Observe sin embargo que los equipos cliente Windows 2000 ignoran los filtros WMI. Siguen aplicando las directivas de grupo en función del ámbito de gestión y el filtrado de seguridad. En cuanto a los viejos puestos de trabajo Windows XP, tenga en cuenta que esta característica se implementó con el SP2 y que el SP3 se recomienda encarecidamente.

Los equipos cliente que funcionan con Windows 7 y versiones posteriores funcionan de forma nativa con los filtros WMI.

Los filtros WMI están disponibles solo en los dominios de Active Directory que poseen al menos un Controlador de Dominio Windows Server. Si no es el caso, la consola de gestión de directivas de grupo no mostrará las opciones WMI. Lo que puede suceder si se utilizan controladores de dominio no Windows como Samba. Este punto es por supuesto normal, ya que estos sistemas que funcionan con Linux, no implementan la interfaz WMI.

Aquí encontrará algunos ejemplos de filtros WMI.

- Equipos Windows 10 x64
  select * from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="1" AND OSArchitecture = "64-Bit"

- Controladores de dominio x64 (cualquier versión)
  select * from Win32_OperatingSystem where (ProductType = "2") AND OSArchitecture = "64-bit"
- Controladores de dominio Windows Server 2016 x64
  select * from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="2"
- Equipos Windows 2016 x64 (no-DC)
  select * from Win32_OperatingSystem WHERE Version like "10.%" AND ProductType="3"
- Filtrado WMI de la versión de un *parche* de type QFE Root\cimv2
  select * from Win32_QuickFixEngineering where HotFixID ='q147222'
- Filtrado WMI con un parámetro de configuración de red (Multicast)
  select * from Win32_NetworkProtocol where SupportsMulticasting = true
- Filtrado WMI con la plantilla de equipo Root\CimV2
  select * from Win32_ComputerSystem where manufacturer ="Toshiba" and Model = "Tecra 8000" OR Model = "Tecra 8100"

Para más información sobre la interfaz WMI, podemos dirigirnos a la dirección siguiente:

- Windows Management Instrumentation Web site : http://msdn.microsoft.com/es-es/library/aa394582(v=vs.85).aspx
- Consulte el directorio de programas de la consola de administración de directivas de grupo (GPMC), o sea en la carpeta**%programfiles%\gpmc\scripts**. Esta carpeta contiene muchos scripts WMI disponibles para la automatización de algunas operaciones que atañen a las directivas de grupo.

Configuración de los parámetros de actualización de las directivas de grupo

1. Refresco de las directivas de grupo

a. Refresco de las directivas en segundo plano

Además de las operaciones efectuadas durante la fase de arranque del equipo y de inicio de sesión del usuario, las directivas de grupo se aplican en segundo plano de forma periódica.

Los diferentes componentes de extensiones replican sus parámetros solo cuando es necesario, o cuando una directiva obliga a volver a aplicar de forma sistemática los parámetros, por posibles razones de seguridad o por el estado de la configuración.

Los componentes cliente especializados en la instalación del software o la redirección de carpetas solo vuelven a aplicar sus parámetros durante el arranque del equipo o el inicio de la sesión de usuario.

b. Ciclo de refresco

Por defecto, las directivas de grupo se verifican cada 90 minutos al que se añade un valor aleatorio comprendido entre 0 y 30 minutos. Por último, el tiempo máximo de refresco puede llegar hasta 120 minutos.

Veremos más adelante que es posible controlar cada CSE (*Client Side Extensions*), de forma que algunas extensiones, como por ejemplo los parámetros de seguridad de Internet Explorer, se apliquen siempre cuando las directivas de grupo no se modifiquen.

Este modo de operación es muy importante para la aplicación de los parámetros de seguridad por el principio de garantía «justo a tiempo» del nivel de conformidad configurado al inicio.

c. Refresco bajo demanda

Podemos evitar el reinicio del equipo al igual que el reinicio de sesión utilizando el comando **Gpupdate**. Observe que por defecto, los usuarios cuentan con la posibilidad de invocar este comando, que no es por cierto peligroso, pero puede generar un tráfico de red importante.

El comando **Gpupdate.exe** se ejecuta del lado del cliente. Observe que a partir de Windows Server 20112, 2012 R2 y Windows Server 2016 la consola de Administración de directivas de grupo permite refrescar de forma remota la aplicación de los objetos GPO de los equipos. Esta funcionalidad está soportada para todos los sistemas operativos destino que funcionen con Windows 7 hasta Windows 10 y puede ser realizada empleando el comando Windows PowerShell Invoke-GPUpdate. Para más información sobre esta nueva funcionalidad busque « Force a Remote Group Policy Refresh (GPUpdate) » en el sitio Microsoft Technet en la dirección https://technet.microsoft.com.

2. Configuración de la frecuencia de refresco de las directivas de grupo

Podemos personalizar la frecuencia de actualización de las directivas de grupo de tipo usuario y/o equipo en función de nuestras necesidades. Para efectuar esta operación, procedemos de la siguiente manera:

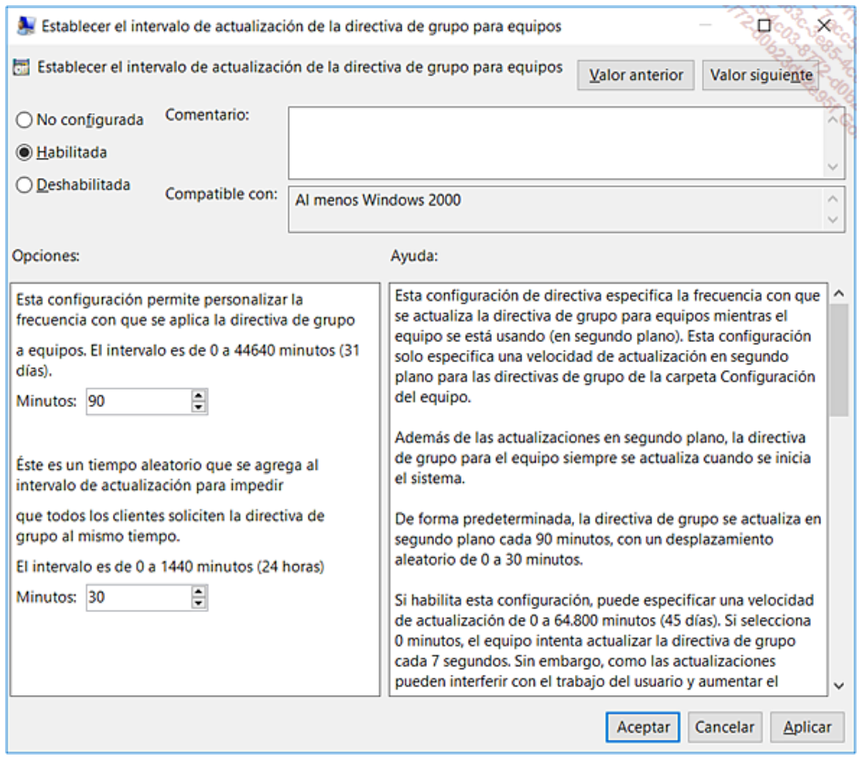
Seleccionamos y abrimos el objeto directiva de grupo apropiado. Vayamos a la parte **Configuración de usuario** o **Configuración del equipo** en función de las necesidades, luego a **Plantillas administrativas/Sistema**.

Hacemos clic en **Directiva de grupo**, y luego doble clic en los parámetros siguientes:

- **Establecer el Intervalo de actualización de la directiva de grupo para usuarios** (el valor por defecto es de 90 minutos, más un valor entre 0 y 30 minutos).
- **Establecer el Intervalo de actualización de la directiva de grupo para equipos** (el valor por defecto es de 90 minutos, más un valor entre 0 y 30 minutos).
- **Establecer el Intervalo de actualización de la directiva de grupo para los controladores de dominio** (el valor por defecto es de 5 minutos).

Seleccionamos **Habilitado**.

Definimos el intervalo de actualización en minutos.



Configuración de la frecuencia de aplicación de los objetos de directivas de grupo

Defina el desfase aleatorio y haga clic en **Aceptar**. Si desactivamos esos parámetros, la directiva de grupo se actualizará por defecto cada 90 minutos Para especificar que la directiva de grupo nunca debe ser actualizada cuando el equipo está en uso, seleccionamos la opción **Desactivar la actualización** de la tarea en segundo plano de las directivas de grupo.

Si seleccionamos 0 minutos, el equipo intenta actualizar la directiva de usuario cada 7 segundos. Este modo de prueba o demostración no debe utilizarse en producción, o si es necesario emplearse en un número limitado de equipos.

3. Refresco empleando Gpupdate.exe

El comando **Gpupdate.exe** nos permite invocar el proceso de descubrimiento y actualización de las directivas de grupo para actualizar la información vigente.

Este comando existe en todos los sistemas Windows excepto en los que funcionan con Windows 2000. Como información, los equipos Windows 2000 utiliza el comando Secedit.exe, que soporta la funcionalidad de refresco.

Observe: ¡El hecho de que el comando Secedit se sustituyera por el comando Gpupdate no significa que Secedit haya desaparecido! Los parámetros de **Secedit [configure, /analyze, /import, /export, /validate, /generaterollback]** están todavía disponibles. Solo el parámetro **/RefreshPolicy** fue suprimido y desplazado al comando Gpupdate.exe.

La sintaxis del comando **Gpupdate** -a menudo utilizado por los administradores de los puestos de trabajo, se especifica a continuación.

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

4. Tratamiento de los componentes de las directivas de grupo en conexiones de baja velocidad

Cuando el componente GPE (*Group Policy Engine*) detecta una conexión lenta, cambia un parámetro para prevenir a los distintos componentes de la extensión del cliente (CSE) que el tratamiento de la directiva de grupo debe realizarse en una conexión "lenta".

Los valores por defecto de los distintos componentes se comportan de la siguiente manera:

- Los parámetros de seguridad se aplican: por razones de seguridad, no es posible especificar que no se apliquen los parámetros de seguridad bajo el pretexto de que los rendimientos de la red en un momento dado sean lentos.
- Plantillas administrativas: por razones necesarias para el buen funcionamiento de las directivas de grupo, las plantillas administrativas no pueden ser desactivadas.
- Instalación y mantenimiento de software: cuando la red se considera lenta, entonces los componentes de instalación y mantenimiento de software son desactivados. De esta manera, la red no será sobrecargada por un exceso de tráfico.
- Se desactiva la ejecución de los scripts.
- Se desactiva la redirección de las carpetas.

a. Tratamiento de parámetros de directivas de grupo no modificados

Por defecto, cada extensión especializada del lado del cliente (exceptuando la extensión de Servicios de instalación remota), aplica solo los parámetros de directiva de grupo que se han modificado desde la última aplicación de la directiva de grupo. Como consecuencia, el tratamiento se ve optimizado y por lo general no será necesario modificar la forma en que las directivas de grupo se evalúan y aplican.

Sin embargo, puede que , por razones de seguridad, deseemos garantizar una correcta aplicación de los parámetros especificados en las directivas de grupo.

¿Que podemos decir de la modificación de los parámetros locales?

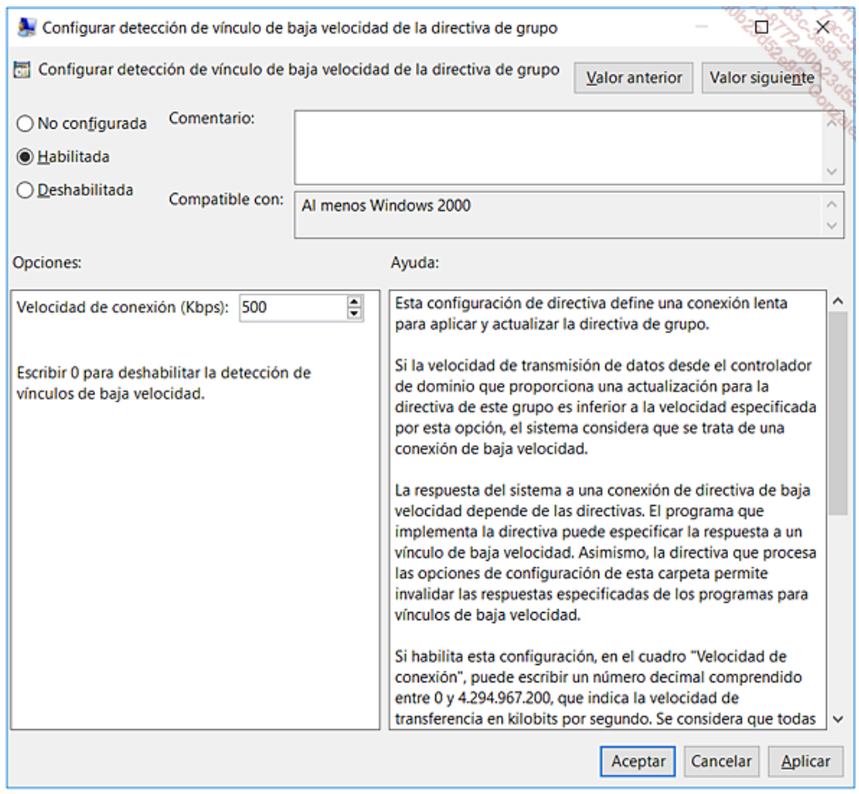
En el caso de que un parámetro controlado por una directiva de grupo sea modificado "en directo" durante un inicio de sesión y si la directiva de grupo no se modifica, entonces la modificación hecha por el usuario permanecerá activa.

Para contrarrestar este fenómeno, tenemos la posibilidad de configurar cada extensión cliente para tratar la aplicación sistemática de todos los parámetros contenidos en la directiva, hayan sido o no modificados. Esta configuración puede realizarse empleando los parámetros de

directivas de grupo incluidos en las plantillas administrativas.

b. Activación de la detección de vínculos de baja velocidad

La detección de vínculos de baja velocidad puede activarse de manera muy simple accediendo a la ventana de configuración disponible en la ubicación siguiente: **Configuración de usuario/Directivas/Plantillas administrativas/Sistema/Directiva de grupo/Configurar detección de vínculo de baja velocidad de la directiva de grupo**

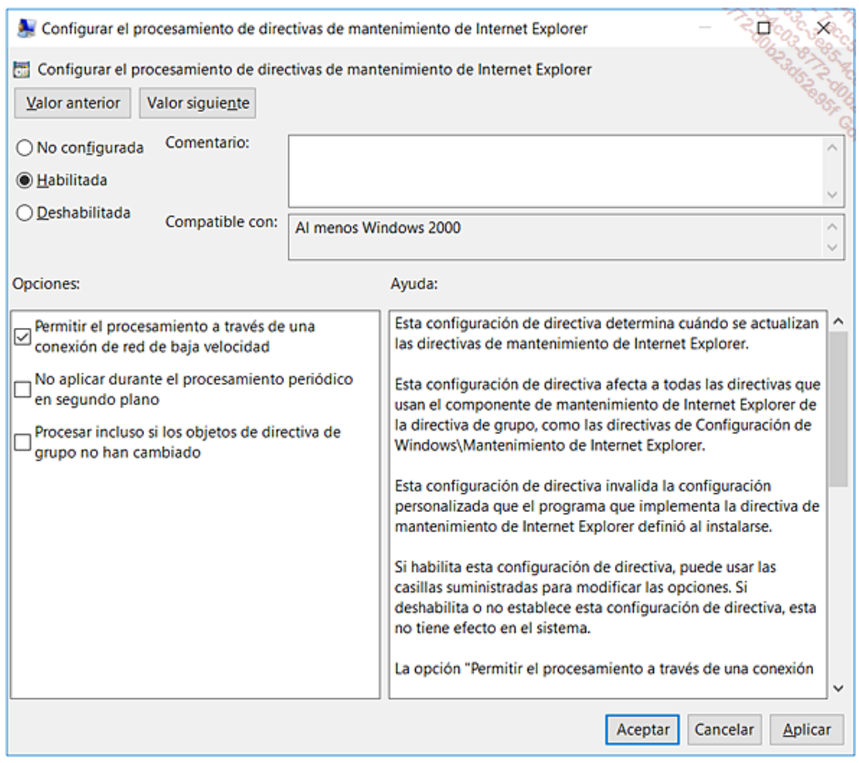


Activación de la detección de vínculos de baja velocidad

Cuando seleccionamos esta funcionalidad, se establece de forma automática el valor de 500 Kbits/s.

c. Forzar la aplicación de los parámetros de directiva aunque no hayan cambiado

La figura siguiente ilustra la activación de la opción **Procesar incluso si los objetos de directiva de grupo no han cambiado** sobre la ampliación de la CSE especializada en el tratamiento de mantenimiento de Internet Explorer.



Activación del tratamiento de una extensión específica para una conexión de red de baja velocidad

Observe que la lista de extensiones cliente se puede controlar empleando las plantillas administrativas.

Otra opción interesante llamada **No aplicar durante el procesamiento periódico en segundo plano** impedirá que el sistema actualice las directivas en segundo plano cuando el equipo está en uso. En efecto, las actualizaciones en segundo plano mientras el usuario trabaja no son recomendables ya que esto puede molestar al usuario, provocar la parada de un programa o incluso en casos raros, dañar los datos.

Los componentes en los que podemos controlar el procesamiento cuando la información no ha sido modificada son:

- la directiva de procesamiento del registro;
- la directiva de Mantenimiento de Internet Explorer;

- la directiva de instalación de software;
- la directiva de redirección de carpetas;
- La directiva de los scripts;
- la directiva de seguridad;
- la directiva de seguridad IP;
- la directiva de redes inalámbricas;
- la directiva de recuperación EFS;
- La directiva de cuotas de disco;

5. Prohibición del refresco por parte de los usuarios

Por defecto, los usuarios cuentan con la posibilidad de ejecutar el comando **Gpupdate**. De esta forma, pueden refrescar los datos de configuración obtenidos de las directivas de grupo, sin reiniciar de nuevo el equipo.

El parámetro **Quitar la capacidad de usuarios para invocar la actualización de directivas de equipo** situado en la ubicación **Configuración del equipo/Plantillas administrativas/Sistema/Directiva de grupo**, nos permite controlar la capacidad del usuario de invocar una actualización de la directiva del equipo.

Si habilitamos este parámetro, los usuarios no podrán solicitar la actualización de la directiva de equipo. La directiva de equipo continuará aplicándose durante el arranque o cuando se produzca una actualización oficial de la directiva. Si desactivamos o si no configuramos este parámetro se aplicará el comportamiento por defecto.

Por defecto, la directiva de equipo se aplica durante el arranque del equipo. Se aplica a su vez en el intervalo de actualización especificado o cuando se invoca de forma manual por el usuario.

Este parámetro no se aplica a los Administradores. Los Administradores puede solicitar una actualización de la directiva de equipo en cualquier momento, sea cual sea la configuración de la directiva. Este parámetro requiere el reinicio del equipo.

6. Procesamiento de bucle invertido (Loopback)

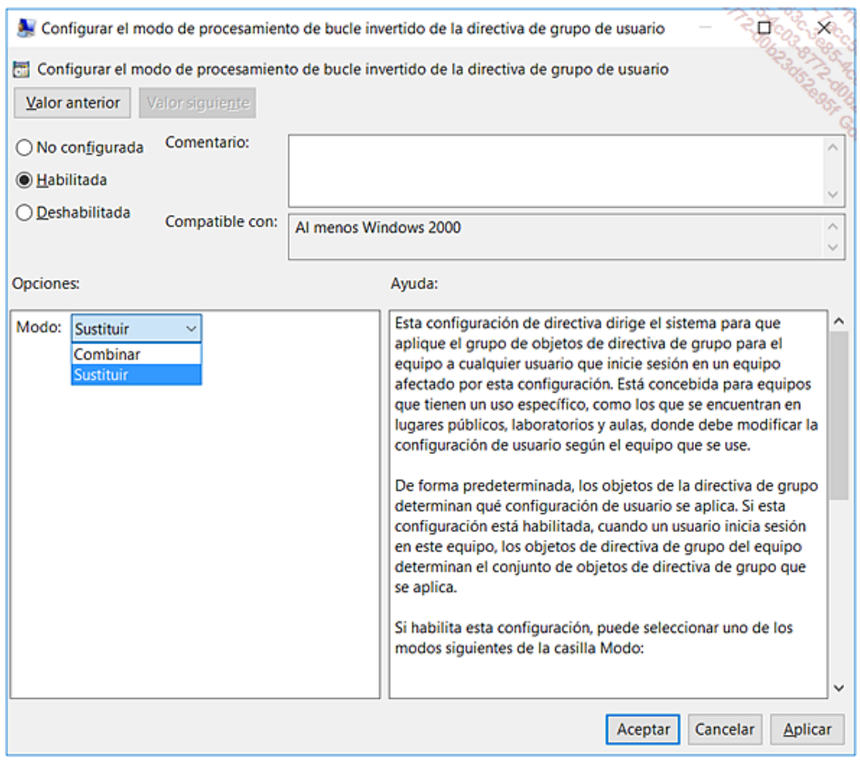
El procesamiento de bucle invertido es una funcionalidad particular destinada a los equipos, tales como los equipos de auto servicio ubicados en lugares públicos como aeropuertos o salas de espera.

Por defecto, las directivas de grupo de un usuario determinan el conjunto de parámetros que serán aplicados cuando el usuario abre una sesión en cualquier equipo de la red.

En el caso de un puesto de auto servicio, que no se trata del equipo habitual del usuario, no deseamos que el entorno de producción del usuario se despliegue de esta forma.

Para conseguirlo, debemos implementar en los equipos de auto servicio el modo de procesamiento de bucle invertido en inglés *Loopback Processing Mode*. Para ello, podemos crear una directiva de grupo que permitirá determinar la parte del entorno de usuario de una forma específica. Este importante parámetro de configuración se ubica en la parte equipo en la dirección siguiente: **Configuración del equipo/Directivas/Plantillas administrativas/Sistema/Directiva de grupo/Configurar el modo de procesamiento de bucle invertido de la directiva de grupo de usuario**.

Como podemos constatar, se trata de un parámetro de tipo equipo. Por lo tanto, este modo de funcionamiento se aplicará al conjunto de usuarios que abran una sesión en el equipo al que se aplica el modo de funcionamiento.



Activación del modo de procesamiento de bucle invertido y selección del modo

El procesamiento por bucle invertido puede ejecutarse según dos modos:

- **Sustituir**: este modo substituye los parámetros de usuario definidos en los objetos directiva de grupo por los parámetros de usuario contenidos en la directiva de grupo aplicada al equipo.
- **Combinar**: este modo combina los parámetros de usuario definidos en los objetos directiva de grupo del equipo con los parámetros de usuario aplicados de forma habitual al usuario. En el caso de que existan parámetros en conflicto, los parámetros de usuario de los objetos de directiva de grupo del equipo tendrán por supuesto prioridad sobre los parámetros del usuario.

Como podemos constatar, los parámetros de usuario de la directiva de grupo que conciernen al equipo se aplican reemplazando o fusionándose con los parámetros de usuario de la directiva específica del usuario. De esta forma, el equipo prevalece en detrimento del usuario.

Gestión de directivas de grupo empleando GPMC

1. Operación de respaldo y restauración de directivas de grupo

La copia de seguridad de las directivas de grupo era, hasta la aparición de la consola de gestión de directivas de grupo, una operación reservada a las herramientas de protección y restauración de Active Directory.

Ahora, podemos utilizar la consola de administración de directivas de grupo para respaldar uno o varios objetos de tipo directiva de grupo, en cualquiera que sea su dominio de pertenencia. Para efectuar esta operación, procedemos de la siguiente manera:

Abrir **Administración de directivas de grupo**.

En el árbol de la consola administración de directivas de grupo, hacemos doble clic en **Objetos de directiva de grupo** en el bosque y el dominio que contenga las directivas de grupo que deseamos respaldar.

Para respaldar un único objeto de directiva de grupo, hacemos clic con el botón derecho sobre él, y luego clic en **Hacer copia de seguridad**.

Para guardar todos los objetos de directivas de grupo del dominio, hacemos clic con el botón derecho sobre **Objetos de directivas de grupo**, y luego hacemos clic en **Hacer copia de seguridad de todos**.

En el cuadro de diálogo **Guardar objeto de estrategia de grupo**, en la zona **Ubicación**, introduzca la ruta de acceso de la ubicación que desea almacenar los respaldos y haga clic en **OK**.

En la zona **Descripción**, introducimos una descripción de los objetos de directiva de grupo que deseamos guardar, y luego hacemos clic en **Hacer copia de seguridad**. Si almacenamos varios objetos de directiva de grupo, la descripción se aplicará a todos los objetos de directiva de grupo respaldados.

Una vez terminada, hacemos clic en **Aceptar**.

Los objetos de directivas de grupo contienen muchos parámetros de configuración. Por esto es importante pensar en la seguridad de las directivas de grupo respaldadas. Debemos garantizar que sólo los administradores autorizados tienen acceso al directorio al cual se exporta el objeto de directiva de grupo.

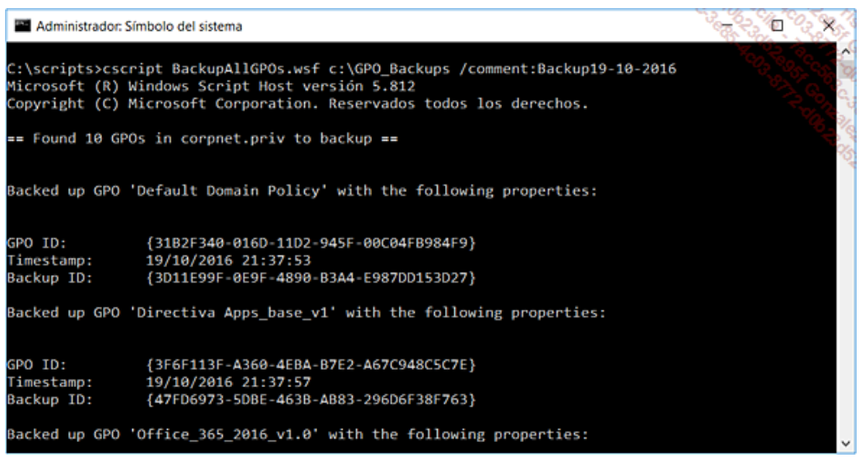
Para ejecutar este procedimiento, debemos contar con los permisos de lectura para el objeto de la directiva de grupo y permisos de escritura para la carpeta que contiene el respaldo del objeto de directiva de grupo.

Group Policy Management Console Scripting Samples: los scripts incluidos al principio con la consola GPMC ya no se suministran con los servidores Windows Server 2008 y versiones posteriores. Inicialmente previstos para Windows Server 2008, estos scripts funcionan sin problema en Windows 10 y Windows Server 2016. Para descargarlos, nos dirigimos al sitio de Microsoft TechNet Code Gallery en la dirección:https://gallery.technet.microsoft.com/group-policy-management-17a5f840

Copiamos los scripts descargados desde el sitio Microsoft Technet Gallery en una carpeta conveniente, como por ejemplo la carpeta C:\Scripts.

Para realizar una copia de seguridad de nuestras directivas de grupo empleando la línea de comandos, nos dirigimos al directorio C:\Scripts y luego usamos el comando siguiente:

```
BackupAllGPOs C:\Backup-AllGPOs /comment:"ALL GPOs"
```



Script para automatizar la copia de seguridad de los objetos de directiva de grupo

La restauración de un objeto de directiva de grupo es tan sencilla como la operación de copia de seguridad.

Haga un clic con el botón derecho en **Objetos de directiva de grupo**, y seleccione **Administrar copias de seguridad**.

En el cuadro de diálogo **Administrar copias de seguridad**, en la zona **Ubicación de la copia de seguridad**, escribimos la ruta de acceso de la carpeta de copia de seguridad. También podemos hacer clic en **Examinar** para acceder a la carpeta de copia de seguridad.

Podemos disponer de varios directorios de respaldo. Cada directorio de respaldo contiene un archivo llamado **Manifest.xml** que contiene la descripción de los elementos guardados.

En la zona **Objetos de directiva de grupo con copia de seguridad**, seleccionamos el objeto de directiva de grupo que deseamos restaurar en la lista de los respaldos de objetos de directiva de grupo que aparecen, y hacemos clic en **Restaurar**.

Cuando se solicite confirmar la operación de restauración, hacemos clic en **Aceptar**.

Para ejecutar este procedimiento, debemos contar con los permisos Modificar permisos, Eliminar y Modificar seguridad para el objeto de la directiva de grupo y permisos de escritura para la carpeta que contiene el respaldo del objeto de directiva de grupo.

Para restaurar un objeto de directiva de grupo que se ha eliminado, debemos poseer los permisos para crear objetos de directiva de grupo en el dominio y los permisos de lectura en la ubicación del sistema de archivos del objeto de directiva de grupo guardado.

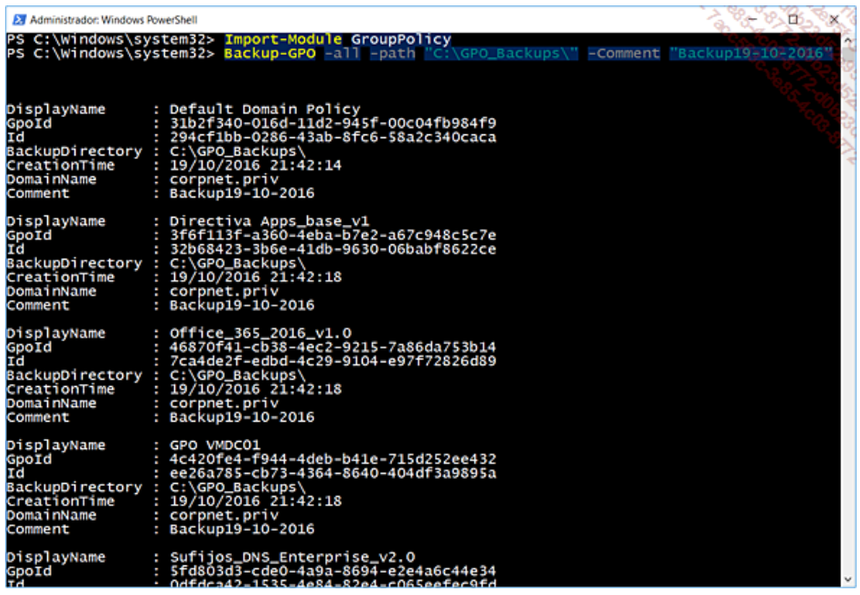
También podemos restaurar un objeto de directiva de grupo ya existente o eliminado empleando la función **Administrar las copias de seguridad**, realizando un clic con el botón derecho en **Dominios** o en **Objetos de directiva de grupo**.

Windows Server, las GPO y Windows PowerShell

Si bien los antiguos scripts WSF de Windows Server 2008 son por lo general suficientes, Microsoft recomienda utilizar los nuevos comandos cmdlet PowerShell incluidos con Windows Server 2008 R2. A continuación listamos los comandos más importantes:

- New:
  - New-GPLink
  - New-GPO
  - New-GPStarterGPO
- Get:
  - Get-GPInheritance
  - Get-GPO
  - Get-GPOReport
  - Get-GPPermissions
- Maintenance:
  - Backup-GPO
  - Copy-GPO
  - Import-GPO
  - Restore-GPO
- Set:
  - Set-GPInheritance
  - Set-GPlink
  - Set-GPermissions

La imagen ilustra el uso del comando PowerShell Backup-GPO para respaldar todos los GPO del dominio un directorio de copia de seguridad.



Respaldo de los GPO con Windows PowerShell

2. Operación de copia de las directivas de grupo

Una operación de copia permite transferir los parámetros de un objeto de directiva de grupo existente a un nuevo objeto de directiva de grupo.

¿Por qué utilizar la funcionalidad de copia de la GPMC?

Las operaciones de copia se adaptarán al desplazamiento de una directiva de grupo entre los entornos de producción, así como entre un dominio de pruebas y un entorno de producción. Para realizar estas operaciones, es necesario que exista una relación de confianza entre los dominios fuente y destino.

El nuevo objeto de directiva de grupo creado durante la operación de copia se asignará a un nuevo identificador global único (GUID, *Globally Unique Identifier*) eliminando sus posibles vínculos.

Podemos utilizar una operación de copia para transferir la configuración a un nuevo objeto de directiva de grupo perteneciente al mismo dominio, en otro dominio del mismo bosque o en un dominio de otro bosque.

Una operación de copia utiliza un objeto de directiva de grupo ya existente en Active Directory como fuente. Se requiere una confianza entre los dominios fuente y destino.

La copia es similar a la copia de seguridad seguida de una importación, pero no contiene ninguna etapa intermedia de sistema de archivos. Se crea un nuevo objeto de directiva de grupo en el marco de la operación de copia.

3. Operación de importación de los parámetros

La operación de importación transfiere los parámetros a un objeto de directiva de grupo existente utilizando como fuente un objeto de

directiva de grupo almacenado en el sistema de archivos.

a. ¿Por qué utilizar la funcionalidad de importación de la GPMC?

Las operaciones de importación pueden utilizarse para transferir parámetros de un objeto de directiva de grupo a otro situado en el mismo dominio, en otro dominio del mismo bosque o en un dominio de otro bosque.

La operación de importación ubica siempre los parámetros guardados en un objeto de directiva de grupo ya existente.

Preste atención al hecho de que esta operación borra todos los parámetros preexistentes en el objeto de la directiva de grupo de destino.

Si disponemos de bosques de prueba y de producción separadas, con o sin relación de confianza, se aconseja probar los objetos de directiva de grupo en el bosque de prueba antes de importarlos al bosque de producción.

La importación no exige la creación de una relación de confianza entre el dominio fuente y el dominio de destino.

Esta operación puede ser útil para transferir los parámetros entre un bosque de producción y un dominio situado en un bosque de prueba no aprobado.

La importación de parámetros en un objeto de directiva de grupo no afecta a su lista de control de acceso discrecional (DACL, *Discretionary Access Control List*), ni a los enlaces a este objeto de directivas de grupo en los sitios, dominios o unidades organizativas, ni el vínculo a un filtro WMI.

b. Utilización de una tabla de correspondencia entre los objetos de diferentes dominios o bosques

Si utilizamos la operación de importación para transferir los parámetros de un objeto de directiva de grupo a un objeto similar en otro dominio o en otro bosque, podemos utilizar una tabla de migración conjuntamente con la operación de importación. Una tabla de migración nos permite facilitar la transferencia de referencias a los grupos de seguridad, usuarios, equipos y rutas de acceso UNC desde el objeto directiva de grupo fuente al objeto de destino.

Verificación y resolución de problemas vinculados a las directivas de grupo con RsoP

Contamos con la posibilidad de simular el despliegue de las directivas de grupo para los usuarios y los equipos antes de implementarlas en realidad en el entorno de producción.

Esta funcionalidad de la consola Administración de directivas de grupo se conoce como conjunto resultante de directivas para el usuario (RSoP,*Resultant Set of Policies*) en modo de planificación.

Observe que el soporte del protocolo RsoP requiere al menos un controlador de dominio que ejecute Windows Server 2003 o una versión posterior, tal como Windows Server 2012 R2 o Windows Server 2016 en el bosque.

Para comprobar los parámetros de la directiva de grupo empleando el asistente Modelado de directivas de grupo, debemos primero crear una consulta de modelado de la directiva de grupo y mostrar esa consulta. Para crear una nueva consulta de modelado de la directiva de grupo, proceda de la siguiente manera:

Abra la consola **Administración de directivas de grupo**, navegue hasta el bosque en el que deseamos crear una consulta de modelado de la directiva de grupo, hacemos clic con el botón derecho en **Modelado de directivas de grupo**, luego **Asistente para modelado de directivas de grupo**.

En la página **Asistente para modelado de directivas de grupo**, hacemos clic en **Siguiente**; introducimos la información en las páginas del asistente y luego hacemos clic en **Finalizar**.

Para mostrar la consulta de modelado de la directiva de grupo, proceda de la siguiente manera:

Abrimos la consola **Administración de directivas de grupo**.

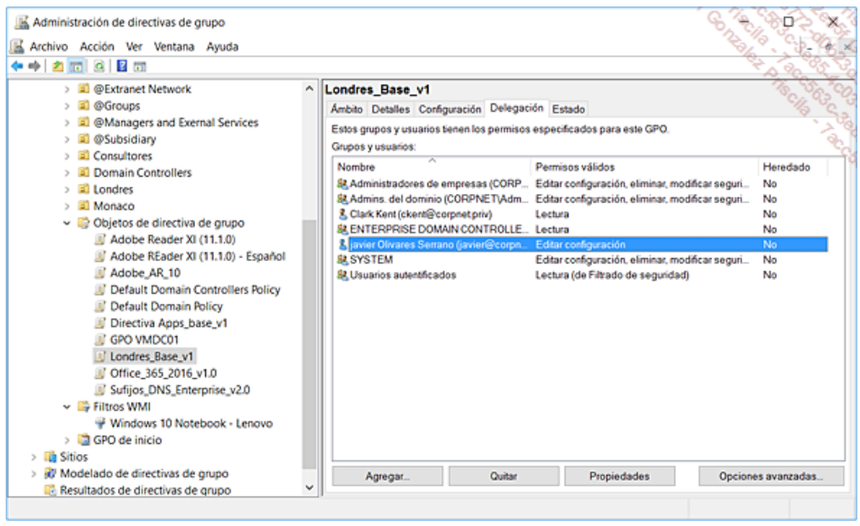
Navegamos hasta el bosque que contiene la consulta de modelado de la directiva del grupo a mostrar, desplegamos **Modelado de directiva de grupo**, y hacemos un clic con el botón derecho en la consulta y luego clic en **Vista avanzada**.

Solo queda comprobar que los resultados presentados en el informe generado al final de la simulación corresponden a los resultados esperados.

Delegación del control administrativo sobre las directivas de grupo

La consola de Administración de directivas de grupo permite gestionar las operaciones de delegación de manera muy fácil. Así, es muy sencillo realizar las operaciones siguientes:

- Crear objetos de directiva de grupo en un dominio.
- Definir los permisos sobre un objeto de directiva de grupo.
- Definir los permisos de directiva en un sitio, un dominio o una unidad organizativa.
- Vincular los objetos de directiva de grupo a un sitio, un dominio o de una unidad organizativa determinados.
- Iniciar análisis de modelado de directivas de grupo en un dominio o una unidad organizativa dados, pero no en un sitio.
- Leer los datos de los resultados de la directiva de grupo para los objetos de un dominio o de una unidad organizativa dados, pero no de un sitio.
- Crear filtros WMI en un dominio.
- Definir los permisos de un filtro WMI.



Implementación de una delegación en la directiva de grupo Londres_Base_v1

La consola de administración de directivas de grupo simplifica mucho la delegación gestionando las diversas entradas de control de acceso (ACE,*Access Control Entry*) necesarias para una tarea como un único grupo de autorizaciones para la tarea. Sin embargo, como ya se ha visto en el marco del filtrado de directivas de grupo empleando los permisos **Leer** y **Aplicar las directivas de grupo**, siempre es posible acceder a los detalles de la lista de control de acceso utilizando el botón **Opciones avanzadas...** de la pestaña **Delegación**.

1. Conceder una delegación a través del grupo propietarios creadores (Creator Owner) de la directiva de grupo

El procedimiento siguiente permite la delegación de la creación de objetos de directiva de grupo. Proceda paso a paso:

Abrir **Administración de directivas de grupo**.

En el árbol de la consola, hacemos clic en **Objetos de directiva de grupo** para los que queremos delegar los permisos de creación de objetos de directiva de grupo. Para hacer esto, nos dirigimos a **Nombre del bosque/Dominios/Nombre del dominio/Objetos de directiva de grupo**.

En la pestaña de resultados, hacemos clic en la pestaña **Delegación**.

Para añadir un nuevo grupo o usuario empleando el grupo de propietarios creadores de la directiva de grupo: en la zona de la lista**Grupos y usuarios**, hacemos doble clic sobre **Propietarios creadores de la directiva de grupo**.

Tenga en cuenta que el grupo **Propietarios creadores de la directiva de grupo** cuenta con todos los permisos sobre los objetos directivas de grupo.

En el cuadro de diálogo **Propiedades de creadores de la directiva de grupo**, seleccionamos la pestaña **Miembros** y hacemos clic en**Agregar**.

En el cuadro de diálogo, seleccionamos **Usuarios**, **equipos o Grupos**, hacemos clic en **Tipos de objeto**, seleccionamos el tipo de objeto para los que queremos delegar los derechos de creación y luego hacemos clic en **Aceptar**.

Hacemos clic en **Ubicaciones**, seleccionamos **el directorio**, sea el dominio o unidad organizativa que contiene el objeto para el cual deseamos delegar los permisos de creación y hacemos clic en **Aceptar**.

En la zona **Escriba los nombres de objeto que desea seleccionar**, introducimos el nombre del objeto en el que queremos delegar los permisos de creación.

Los miembros de este grupo pueden modificar la directiva de grupo del dominio. Observe que la cuenta Administrador forma parte de este grupo, por defecto. Este grupo dispone de todos los derechos en el dominio, se aconseja añadir usuarios con precaución.

Para realizar este procedimiento, debemos ser miembros del grupo de Administradores de dominio o Administradores de empresas.

También podemos eliminar un grupo o un usuario de la lista de permisos mediante un clic con el botón derecho sobre su nombre en la zona de la lista **Grupos y usuarios** en la pestaña **Delegación**, y haciendo clic en **Eliminar**.

Si queremos delegar permisos a usuarios y grupos del mismo dominio que los objetos de directiva de grupo, se recomienda la adición al grupo Propietarios creadores de la directiva de grupo. Sin embargo, debemos tener en cuenta que no es posible añadir grupos o usuarios de otro dominio al grupo de Propietarios creadores de la directiva de grupo.

Para delegar los permisos autorizaciones de creación de objetos de directiva de grupo a grupos o usuarios de otro dominio, debemos conceder de manera explícita los permisos de creación de objetos de directiva de grupo en este grupo (sin utilizar el grupo de Propietarios creadores de la directiva de grupo). También podemos crear un grupo local del dominio en el dominio en el cual queremos delegar el permiso de creación de objetos de directiva de grupo y conceder a este grupo el permiso de crear objetos de directiva de grupo. Luego añadimos los miembros de este grupo local del dominio a partir de otros dominios según las necesidades. Podremos insertar en este grupo local las cuentas de usuarios o grupos globales de dicho dominio.

2. Conceder una delegación empleando la consola de administración GPMC

La consola de Administración de directivas de grupo GPMC nos permite añadir y eliminar los grupos, usuarios y equipos a utilizar, como los filtros de seguridad para cada objeto de directiva de grupo.

Por otra parte, las entidades de seguridad utilizadas para el filtrado de seguridad aparecen también en la pestaña **Delegación** de un objeto de directiva de grupo como con los permisos **Lectura** ya que disponen de un acceso de lectura.

a. Conceder una delegación de vinculado de las directivas de grupo

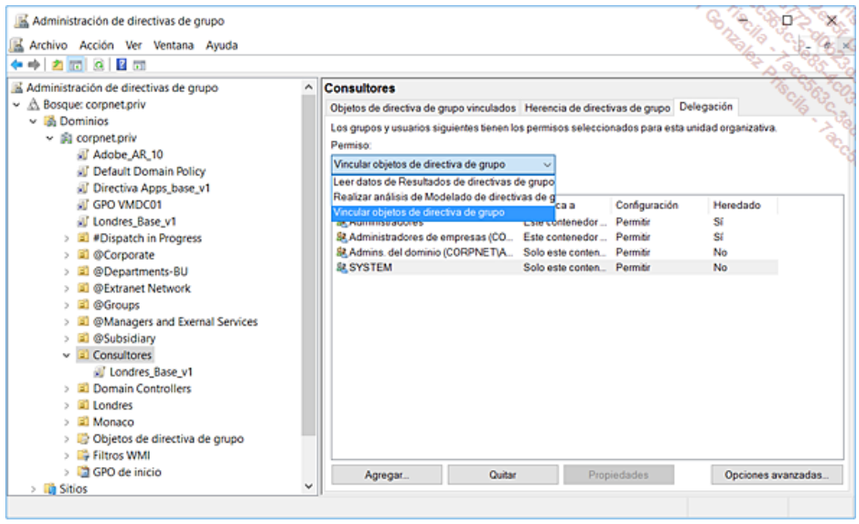
Para delegar los permisos de directiva para un dominio, una unidad organizativa o incluso un sitio que permite vincular objetos directiva de grupo, seguimos el procedimiento siguiente:

Abrir la consola **Administración de directivas de grupo**.

Para delegar un permiso para vincular objetos de directiva de grupo en el dominio, o en una unidad organizativa, hacemos clic en el dominio o en la unidad organizativa.

En la ventana de resultados, hacemos clic en la pestaña **Delegación**.

En la lista desplegable **Permiso**, seleccionamos **Vincular objetos de directiva de grupo**, y luego especificamos los permisos para relacionar los objetos de directiva de grupo para un grupo o un usuario: para añadir un nuevo grupo o usuario a la lista de los permisos de los dominios y unidades organizativas, en la pestaña **Delegación**, hacemos clic en **Agregar**.



Delegación de las operaciones de GPO en las UO y tipos de permisos

Para delegar los permisos para relacionar los objetos de directiva de grupo en un sitio, un dominio o una unidad organizativa, debemos contar con el permiso **Editar permisos** para este sitio web, este dominio o la unidad organizativa. Por defecto, sólo los administradores de dominio y los administradores de empresas cuentan con este permiso.

Los usuarios y grupos que tienen un permiso para vincular objetos de directiva de grupo en un sitio, un dominio o una unidad organizativa específica podrán vincular los objetos de directiva de grupo, cambiar el orden de los vínculos y definir el bloqueo de la herencia para este sitio web, este dominio o la unidad organizativa.

No podemos borrar grupos y usuarios con herencia de permisos de un contenedor padre.

Algunas entradas de la zona de la lista **Grupos y usuarios**, como **Sistema**, no tienen un cuadro de diálogo de propiedades asociado. El botón **Propiedades** no está disponible para estas entradas.

b. Conceder una delegación de modelado de directivas de grupo

Para delegar los permisos de modelado de directiva, procedemos como se indica a continuación:

Abrir la consola **Administración de directivas de grupo**.

En el árbol de la consola, hacemos clic en el dominio o la unidad organizativa en la que deseamos delegar los permisos de modelado de directiva de grupo.

En la ventana de resultados, hacemos clic en la pestaña **Delegación**.

En la zona **Permiso**, seleccionamos **Realizar análisis de modelado de directiva de grupo**; para añadir un nuevo grupo o usuario a la lista de los permisos, bajo la pestaña **Delegación**, hacemos clic en **Agregar**.

Para delegar los permisos que permiten efectuar el análisis de modelado de directivas de grupo para los objetos de un dominio o de una unidad organizativa, debemos contar con el permiso Editar permisos para este dominio o esta unidad organizativa.

Por defecto, sólo los administradores de dominio y los administradores de empresas cuentan con este permiso.

No podemos delegar el permiso para realizar los análisis de modelado de directivas de grupo para los sitios.

c. Conceder una delegación de creación de filtros WMI

Para delegar la creación de filtros WMI, proceda como sigue:

Abrir la consola **Administración de directivas de grupo**.

En el árbol de la consola, hacemos clic en **Filtros WMI** en el bosque y el dominio en los que queremos delegar los permisos de gestión para todos los filtros WMI.

En la ventana de resultados, hacemos clic en la pestaña **Delegación**; para añadir un nuevo grupo o usuario con permisos de gestión en todos los filtros WMI, y hacemos clic en **Añadir**.

Observación sobre la seguridad de acceso a los filtros WMI

Debemos ser administrador de dominio o administrador de empresas para delegar permisos sobre todos los filtros WMI de dominio.

Los usuarios que tienen el permiso **Control total** pueden crear y controlar todos los filtros WMI de un dominio, incluidos los filtros WMI creados por otros usuarios. Los usuarios con permisos **Creador propietario** pueden crear filtros WMI, pero sólo pueden controlar aquellos que han creado.

Si eliminamos **Propietarios creadores de la directiva de grupo** de la lista de permisos, los usuarios que crean los objetos de directiva de grupo no pueden crear filtros WMI excepto si esta autorización se concede de forma explícita a través de su pertenencia a otro grupo.

Todos los usuarios deben tener acceso de lectura a todos los filtros WMI. De lo contrario, la directiva grupo interrumpe el procesamiento cuando encuentra un filtro WMI que no puede leerse. No podemos utilizar la gestión de directivas de grupo para eliminar los permisos de lectura de los filtros WMI.

La opción **Filtros WMI** está disponible sólo si al menos un controlador de dominio ejecuta una versión a partir de Windows Server 2003 hasta Windows Server 2016. Esto es lo mismo para **Filtrado WMI** bajo la pestaña **Ámbito** para los objetos de directiva de grupo.

Recomendaciones para la definición de una directiva de grupo para la empresa

La planificación de una infraestructura de Active Directory requiere la creación de un plan que se tenga en cuenta las mejores prácticas para la empresa en relación con los temas presentados a continuación:

- la herencia de las directivas de grupo.
- la administración y el despliegue más adecuado en relación a la gestión de directivas de grupo.

Debemos hacerlo de la mejor manera para que la tecnología sea una baza, y sobre todo no un freno. Para lograrlo, considere la manera en que podemos implementar las directivas de grupo dentro de nuestra empresa.

Al final, no debemos dejar de pensar en la delegación de los permisos sobre la base de una reflexión que deberá reflejar las diferentes tareas de administración, la elección de un modelo de administración, así como la facilidad de diseño y ejecución.

Los puntos siguientes son las reglas que hay que tratar de respetar al máximo:

- Aplicar los parámetros de la directiva de grupo al más alto nivel para aprovechar los mecanismos de herencia.
- Determine los parámetros comunes de los objetos de directiva de grupo para el mayor contenedor, es decir, el objeto dominio Active Directory mismo.
- Vincular la estrategia de grupo en el dominio,
- Disminuya el número de directivas de grupo. Reducir el número utilizando varios vínculos en lugar de crear varios objetos de directiva de grupo idénticos. Intente vincular un objeto de directiva de grupo al mayor contenedor posible, para evitar crear varios vínculos del mismo objeto a un nivel más bajo.


Este método reduce el número de directivas de grupo, pero también limita las posibilidades de delegación de la administración.

- Cree objetos de directiva de grupo especializados. Úselos para aplicar parámetros únicos, si es necesario.
- Los objetos de la directiva de grupo a un nivel superior no aplicarán los parámetros de estos objetos de directiva de grupo especializados.
- Desactive los parámetros de configuración del equipo o del usuario. Cuando creemos un objeto de directiva de grupo destinado a contener los parámetros de uno de estos dos niveles (usuario o equipo), desactive la porción no utilizada del objeto directiva de grupo. Esto permite mejorar los rendimientos durante la aplicación de los objetos de directiva de grupo durante la conexión del usuario. Esto permite a su vez evitar cualquier aplicación de parámetros no deseados.

Introducción a la gestión de software

1. IntelliMirror y la gestión de software

La tecnología de instalación y mantenimiento de software integrada en los puestos de trabajo Windows 2000 hasta Windows 10, y los sistemas de la familia Windows Server 2003 hasta Windows Server 2016, permite a los administradores resolver uno de los puntos más problemáticos de las infraestructuras Windows. En efecto, la gestión de los ordenadores no es solo su inventario, así como la buena gestión del sistema operativo. También es necesario -y quizá sobre todo- ser capaz de prestar servicios de gestión de software de un nivel tal que los usuarios dispondrán del software para el ejercicio eficaz de su actividad.

Pero la gestión del problema supera el simple marco de la fase de despliegue. La tecnología nos ayudará a hacernos cargo de la totalidad de las operaciones involucradas en el ciclo de vida del software. Así, los usuarios tendrán siempre el "mejor software" para realizar sus actividades.

Por supuesto, la funcionalidad IntelliMirror de gestión de software está en el corazón de los servicios globales. Antes de emprender nuestro aprendizaje de la tecnología de instalación y gestión de software, los puntos siguientes recuerdan los beneficios asociados con la tecnología IntelliMirror integrada en la infraestructura Windows basada en los servicios de dominio de Active Directory.

IntelliMirror acomete los tres problemas de gestión listados a continuación:

1. La gestión de los datos de usuario: estas características permiten a los usuarios acceder a los datos necesarios para su actividad, estén o no conectados a la red de la empresa.

2. La gestión de la instalación y mantenimiento del software: los usuarios disponen del software que necesitan para realizar sus tareas cotidianas. El software puede instalarse en el último momento. Una vez desplegado mediante la tecnología IntelliMirror, el software dispone de funcionalidades de autoreparación. Además, siempre que estén bajo el control de las directivas de grupo definidas en el directorio Active Directory, todas las funcionalidades de gestión de actualizaciones y también su eliminación estarán disponibles. De esta forma, el coste de gestión de software podrá reducirse deo forma considerable, disminuyendo al mismo tiempo el TCO (*Total Cost of Ownership*) asociado a la infraestructura.

El TCO es igual a la suma de todos los costes asociados a los diferentes elementos que componen el sistema de información en un período determinado: costes de los servidores, puestos de trabajo, accesorios, contratos de mantenimiento de equipos, licencias de los sistemas operativos y programas informáticos, mantenimiento de servicios de infraestructura y puestos de trabajo, operaciones de cambios menores (paso de los QFE (*Quick Fix Engineering*) y SP (*Service Pack*) y los avances importantes como el despliegue o la actualización de una aplicación, coste del desarrollo de aplicaciones específicas, a menudo necesario, costes asociados a la gestión de la seguridad de los perímetros de red, los servidores, equipos cliente y las aplicaciones de carácter estratégico.

Los costes más importantes no suelen estar en la compra o adquisición de licencias, ni los equipos cliente, sino en los costes post-despliegue relacionados con la administración de sistemas, aplicaciones y de forma más general el ciclo de vida del software. Los precios de los equipos se han reducido por seis en diez años, aunque es cierto que a la inversa el coste de una licencia de Windows 10 profesional es muy superior al de una licencia de Windows XP; ¡también es cierto que los servicios incluidos en los sistemas modernos no tienen nada que ver con sus ilustres antepasados! Es en este eje de funcionalidades que los servicios de directorio Active Directory, los servicios distribuidos y los servicios de seguridad asociados se posicionan para reducir de forma considerable el TCO y añadir en el ROI, retorno de inversión.

Los estudios realizados por las más grandes empresas han demostrado que las empresas que han invertido en la tecnología Active Directory habían rentabilizado su migración al año siguiente y progresado de forma global en todos los ámbitos.

Para más información sobre los métodos de cálculo del TCO, visite el sitio de Microsoft y haga una búsqueda en REJ (*Rapid Economic Justificación*).

3. La gestión de parámetros de usuario: los parámetros de usuario le siguen donde quiera que vaya. Esta funcionalidad permite garantizar que cualquiera que sea el equipo en el que el usuario inicia su sesión, éste dispondrá de todos los parámetros de entorno mínimos para poder ejercer su actividad, como si se tratara de su equipo principal.

a. Change and Configuration Management = IntelliMirror más WDS/MDT

Desde el punto de vista de la estrategia de Microsoft, IntelliMirror es sólo un elemento de los servicios de "Gestión de los Cambios de Configuración". En efecto, para que el equipo pueda ser considerado como un elemento "desechable" a voluntad, también es necesario que sea fácil regenerar el equipo. A tal efecto, los servicios de despliegue Windows WDS disponibles en todas las versiones desde Windows Server 2008 R2 hasta Windows Server 2016 (*Windows Deployment Services*) asociados con el MDT (*Microsoft Deployment Toolkit*), u otros productos adicionales, tales como el System Center Configuration Manager, pueden ser utilizados para soportar el despliegue a través de la red.

Por último la sustitución o bien la instalación de un nuevo equipo podrán realizarse instalando una imagen predefinida adaptada al usuario principal del equipo. Luego, la tecnología IntelliMirror (AD + GPO) implementará sobre la marcha el entorno de producción operativo más reciente.

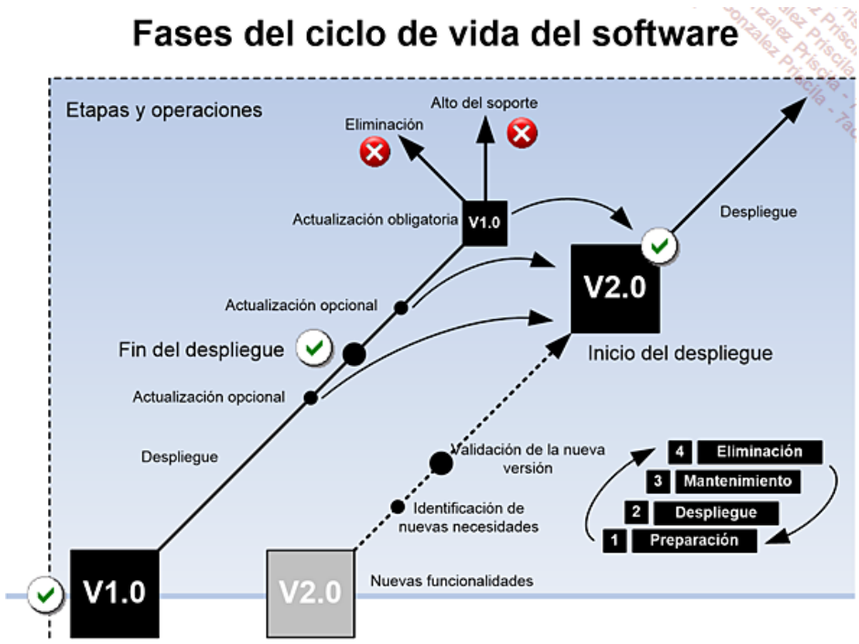
2. El ciclo de vida del software

El ciclo de vida del software describe los grandes principios de operación que los administradores deberán implementar durante la vida útil de una aplicación en la red empresarial.

Los administradores responsables de las operaciones de soporte y de mantenimiento del software deberán gestionar el software en función del modelo de ciclo de vida que vamos a presentar.

La idea es identificar los momentos importantes que los administradores deben tener en cuenta para gestionar la evaluación, viabilidad de una transición y luego el proceso concreto de implementación entre las diferentes versiones de software. La tecnología IntelliMirror de Gestión y Mantenimiento de software permitirá a los administradores soportar la totalidad del ciclo de vida de cada aplicación desplegada y luego controlada por esta tecnología. De esta forma, el departamento responsable de las operaciones de despliegue y de mantenimiento del software podrá efectuar las operaciones en un tiempo reducido en gran medida con una garantía de éxito cercana al 100%.

La siguiente imagen ilustra las diferentes etapas de la vida de un software.



El ciclo de vida del software y sus diferentes etapas y operaciones asociadas

Los puntos siguientes describen las grandes etapas y que luego trataremos con más detalle con las directivas de grupo y la tecnología de gestión y de mantenimiento de aplicaciones.

1. Aplicación en V1.0: fase de despliegue y uso de la aplicación

Por supuesto, el ciclo de vida del software comienza cuando el administrador despliega la primera versión de la aplicación. Los usuarios reciben la aplicación y la utilizan.

2. Aplicación en V2.0: una nueva versión está disponible, y luego se evalúa

Contemplamos responder a una nueva necesidad de un departamento o unidad empresarial, empleando una nueva versión de la aplicación. Observe que se puede tratar de una nueva versión de la misma aplicación o bien de una aplicación proveniente de otro fabricante.

El concepto es el mismo, la tecnología nos permitirá efectuar una actualización técnica de la versión 1.0 a la versión 2.0, o bien una actualización competitiva. ¡Esta última efectuará la eliminación de la primera aplicación en beneficio de la nueva instalación!

Antes de desplegar la nueva aplicación, será por supuesto necesario conducir una fase de pruebas que permitirá validar el correcto funcionamiento del software. Esta fase de pruebas deberá ser lo más realista posible. ¡Para lograr esto, desplegamos la nueva aplicación en un pequeño número de usuarios representativos y confirmamos que la aplicación es por completo operativa, tanto a nivel técnico como funcional!

La fase de validación, llamada con frecuencia «piloto», deberá ser lo más realista posible. ¡Será importante que participen los usuarios más exigentes! De esta forma el piloto encuentra su utilidad con gran eficacia. Muchos de los problemas son descubiertos y muchos solucionados, sin afectar a un gran número de usuarios.

No olvidemos introducir puntos de control como la compatibilidad de la nueva versión de la aplicación con la versión anterior -que será todavía utilizada a nivel empresarial- pero también con las otras aplicaciones.

3. Aplicación en V2.0: gestionar la transición

La mejor solución es por supuesto beneficiarse de una migración total y lo más rápida posible. De esta forma, todos los usuarios que utilizan la misma versión tienen las mismas ventajas y también los mismos límites o restricciones.

Por desgracia, es poco probable que podamos realizar esta operación en una red de gran tamaño (salvo un posible caso de redespliegue general de los equipos) en un periodo corto.

El método más común es proceder a una actualización progresiva de los usuarios por lotes a la nueva versión. Podemos por ejemplo, decidir no migrar un departamento que se encuentre en particular sobrecargado. De esta forma, los usuarios continúan su trabajo de forma normal con la aplicación V1.0 y se beneficiarán de un periodo de calma posterior para migrar a la nueva versión.

La tecnología no es la panacea. Es primordial preservar la productividad y el confort de los usuarios sobre todo si se encuentran en un periodo de sobrecarga. Un problema pequeño se convierte en un gran problema cuando la situación se tensa.

4. Estado de la aplicación V1.0

Una vez decidido migrar a una nueva aplicación, los administradores deberán considerar a su vez lo que ocurrirá con la antigua versión de la mencionada aplicación. La figura anterior muestra varias alternativas:

- Los usuarios se verán forzados a efectuar la actualización a la nueva versión de la aplicación. Se trata de la decisión más deseable porque solo tendremos que mantener una versión.
- Autorizaremos que la versión 1.0 no sea actualizada a su última versión. En este caso, es claro que esta «autorización» no debe causar ningún problema de compatibilidad. Por lo general, cuando se puede ofrecer esta posibilidad al usuario, conviene que la aplicación anterior no mantenga su soporte. Por lo tanto, a pesar de todo se recomienda una actualización, por lo menos a largo plazo. Tal situación no se permitirá para los nuevos usuarios, que por definición deben utilizar la aplicación en su versión más moderna.

5. Aplicación en V2.0: fase de despliegue

A medida que el despliegue avanza, la meta a alcanzar se aproxima y los usuarios disponen, poco a poco, de la aplicación que requieren.

Las aplicaciones desplegadas empleando los servicios de gestión y mantenimiento de software se asignan, en función de las opciones definidas por el Administrador, a los equipos o a los usuarios y beneficiándose así de la tecnología Windows Installer (Instalación automática bajo demanda, reparación de componentes y eliminación completa).

6. Aplicación V1.0: operación de eliminación

La última etapa concierne la eliminación de la antigua aplicación. La última recomendación se centrará en la recuperación o la realización de operaciones que requerirían la utilización de la aplicación en su versión 1.0. Podemos y debemos conservar los archivos y los procedimientos de instalación. También debemos mantener un clon de una configuración tipo (imagen de disco o configuración de tipo máquina virtual) de tal manera que sea fácil acceder en cualquier momento.

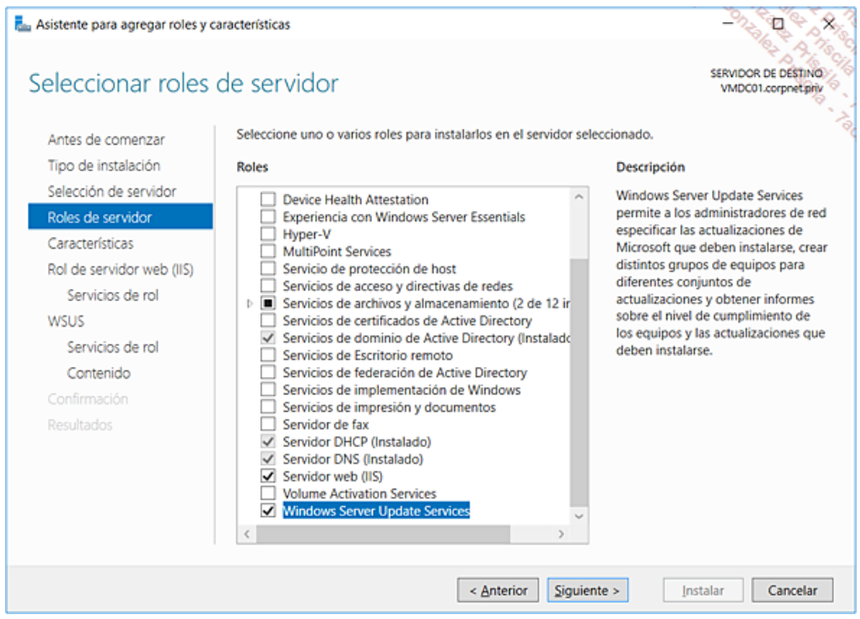
7. Implementación de los Service Packs y parches

Además de las actualizaciones importantes, el ciclo de vida del software debe tener en cuenta las operaciones de aplicación de parches y otros Service Packs. En términos absolutos, se trata de una actualización algo especial, ya que la versión del producto no cambia, sino el nivel de Service Pack o sólo uno o varios componentes «parcheados» de entre muchos.

Archivos MSI (Microsoft Instaler) y MSP (Microsoft Patchs)

Aunque es posible desplegar los Service Packs de Windows o Windows Server y las actualizaciones de aplicaciones tales como los productos de la suite Microsoft Office, la tecnología de gestión y mantenimiento de software incluida en Windows no es la más flexible para realizar este tipo de tareas.

El paso de los parches y actualizaciones críticas requiere mecanismos de emergencia y la posibilidad de gestionar de forma específica el seguimiento de los parches "no implementados" con el enfoque IntelliMirror. Es por esta razón que estas operaciones de mantenimiento son soportadas por otras soluciones adicionales y complementarias. Hoy en día, el rol WSUS (*Windows Server Update Service*) disponible con Windows Server 2012 R2 y Windows Server 2016 puede aplicarse de forma rápida para soportar todas las tareas de actualización de los sistemas y aplicaciones de Microsoft. Por último, cuando la empresa desea una solución de gestión del ciclo de vida de los equipos y del software Microsoft y también no Microsoft, una solución como Microsoft System Center Configuration Manager será una muy buena opción.



Añadir el rol de Servicios WSUS a Windows Server 2016

Despliegue de software

1. Las diferentes etapas

Los administradores responsables del despliegue de aplicaciones deberán gestionar varias etapas, todas independientes entre sí, pero todas necesarias para lograr el despliegue de una nueva aplicación en la red empresarial.

Para desplegar una nueva aplicación, los administradores deberán realizar distintas tareas preparatorias:

- la fase de preparación del software,
- la fase de distribución del software,
- la fase de despliegue real del software.

a. Disponer de un paquete MSI

Fase de preparación de despliegue

La fase de preparación requiere que dispongamos de un software que soporte los archivos de instalación MSI requeridos por el servicio Windows Installer.

El Servicio Windows Installer es un servicio instalado por defecto en el sistema operativo Windows y los sistemas de la familia Windows Server.

Una vez que poseemos un paquete en formato MSI compatible con la plataforma objetivo, podemos considerar la utilización de un objeto de directiva de grupo ya existente o bien la creación de un nuevo objeto de directiva de grupo para desplegar dicho software.

Debemos también considerar la infraestructura de Active Directory S,D,UO existente e identificar los posibles riesgos relacionados con dicha infraestructura. Puede ser que sea necesario crear una nueva unidad organizativa para seleccionar mejor algunos equipos o algunos usuarios del directorio Active Directory.

Ubicamos los archivos necesarios para la instalación en una carpeta compartida de un servidor cerca de las objetivos contemplados en el despliegue.

Las operaciones de reempaquetado son a veces fastidiosas por su complejidad. La instalación de los servicios, componentes, actualizaciones pueden complicar de forma singular los procesos de creación de la preparación del paquete MSI. Para simplificar estas tareas, se recomienda la adquisición de un producto profesional como Admin Studio editado por Flexera Software. Para más información o descargar los productos en versión de evaluación, diríjase al sitio http://www.flexerasoftware.com.

b. Desplegar el software:distribución y selección

Fase de distribución

La fase de distribución del software no debe ser confundida con la fase de instalación propiamente dicha. Esto es especialmente cierto con respecto a los productos de gestión de aplicaciones como Microsoft SCCM u otros, que distribuyen e instalan aplicaciones. A menudo, estos productos son muy eficaces para la distribución de los conjuntos de archivos en varias ubicaciones, pero cuentan con funcionalidades limitadas para lograr la automatización de la instalación de programas en los sistemas. Cabe recordar que Microsoft SMS ha mostrado el camino con el ancestro de Windows Installer (SMS Installer) que permitía "reempaquetar" los antiguos programas de instalación manuales en paquetes automatizados, sin ofrecer mayores funcionalidades tan adelantadas como las disponibles hoy con Windows Installer incluido en todas las versiones modernas de Windows. Por lo tanto, es el sistema mismo el que instala y hace el trabajo y no un módulo externo. Es lo que explica el carácter dinámico de la instalación de software en los puestos de trabajo que soportan Active Directory, los objetos GPO y la tecnología IntelliMirror.

Para más información sobre las diferentes versiones de Windows Installer en las diferentes versiones de Windows, consulte la sección Las diferentes versiones de Windows Installer más adelante en este capítulo.

La fase de distribución es importante ya que consiste en tener a disposición de los equipos y los usuarios todos los archivos necesarios para el correcto desarrollo de la instalación y las funciones de reparación cuando ello sea necesario.

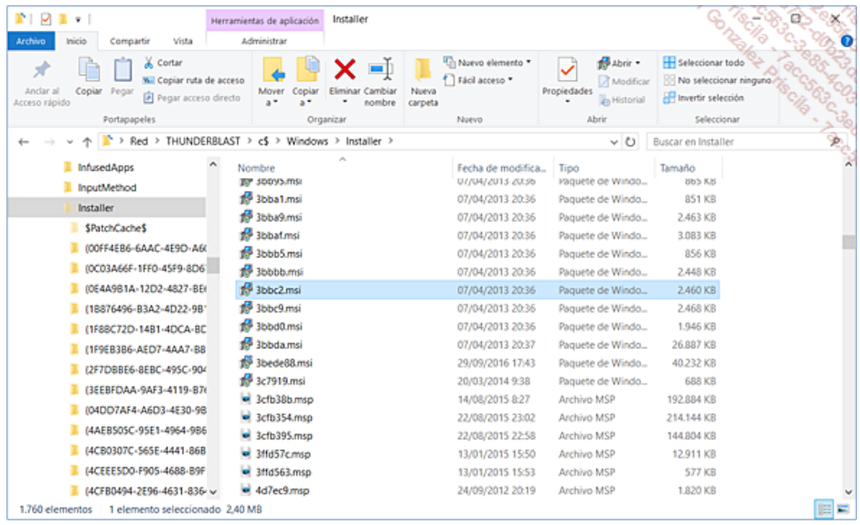
Recomendación: implementar una raíz DFS integrada en Active Directory.

La tecnología Windows Installer permite la reparación de los programas almacenando de forma local el archivo MSI de cada aplicación (directorio %Systemroot%\ y teniendo en cuenta la ubicación fuente que contiene los archivos.

Por lo tanto, para aprovechar plenamente las funciones de reparación automática, es obligatorio disponer de una fuente de red "fiable", tal como la ofrecida por una raíz DFS integrada en Active Directory. También podemos basarnos en servicios de distribución muy potentes como los incluidos en Microsoft SCCM y controlar de forma muy fina la forma de las replicaciones, las planificaciones horarias y el cumplimiento de algunos mínimos de ancho de banda disponible en la red.

Como información, las versiones de Microsoft Office ofrecen conservar en caché, en el directorio \Msocache, todos los archivos "útiles" para una reparación urgente de la aplicación cuando el ordenador está desconectado de la red. Microsoft SCCM propone también esta opción empleando el cache de aplicaciones. De esta forma, SCCM nos permite especificar que una aplicación estratégica específica puede ser puesta en caché local para fines de reparación, por ejemplo cuando un problema se produce y el usuario está trabajando en un sitio no conectado a la red de la empresa.

La imagen siguiente muestra la ubicación y los diferentes tipos de archivos contenidos en el directorio %Systemroot%\Installer.



Almacenamiento de archivos utilizables con fines de reparación de aplicaciones

Tenga en cuenta que para ver este directorio debemos activar la opción de visualización **Elementos ocultos**.

Además de los archivos MSI de cada aplicación, también encontraremos los archivos ETS (*Microsoft Transforms Files*) y los archivos que contienen los parches, es decir, los archivos MSP. Observamos también la presencia de un directorio cuyo nombre es el GUID de la aplicación. Así, para cada aplicación, algunos archivos de configuración del entorno de la aplicación están disponibles, pero de ninguna manera los archivos que contienen los programas y demás componentes necesarios para el buen funcionamiento de la aplicación. Como hemos descrito, debemos disponer del servidor de distribución que contenga todos los archivos necesarios para la instalación.

Por definición un recurso compartido de red utilizable en el marco de la gestión y mantenimiento de aplicaciones deberá contener los elementos listados a continuación:

- todos los archivos de la distribución de la aplicación,
- todos los archivos de transformación utilizados en el marco de los futuros despliegues,
- los service packs y otros parches que se quiera desplegar al mismo tiempo que la instalación.

En el caso de productos que solicitan una clave de instalación, debemos disponer de una adecuada distribución tal como las ofrecidas por Microsoft con los contratos de licencia por volumen que utilizan claves para productos de tipo VLK (*Volumen License Key*) o MAK (*Multiple Activation Key*). En este caso, procedemos a una instalación administrativa del producto. Observe que en el caso de la utilización de claves de cliente KMS, debemos aplicar un servidor KMS para el producto afectado, por ejemplo Windows 10 Profesional o Office 2016 Pro Plus.

Fase de definición del objetivo en función del ámbito de gestión (SOM - Scope Of Management) Sitio, Dominio y Unidades organizativas

La fase de definición del objetivo sirve para determinar que software debe ser ofrecido a que usuarios en función de sus necesidades.

Las funcionalidades de gestión y mantenimiento del software se basan cien por cien en las directivas de grupo y los servicios de directorio Active Directory. Los conceptos que ya hemos aprendido sobre los principios fundamentales de las directivas de grupo se aplicarán de manera íntegra para el nodo "Instalación de software (usuarios) y (equipos)", que es una extensión natural de las funciones de las directivas de grupo. Así, las funciones de despliegue de software podrán basarse en una extensión de gestión (*Scope of Management*) de tipo Sitios, Dominios y Unidades organizativas.

Como de costumbre, deberemos proceder de la siguiente manera:

- crear o modificar un objeto directiva de grupo, teniendo cuidado de darle un nombre basado en una política de nombres adaptada,
- definir un posible filtrado de seguridad en base a los permisos de **Lectura** y **Aplicar la directiva de grupo** para referirse a objetos equipo y usuario concretos,
- conectar el objeto directiva de grupo a uno o varios contenedores de Active Directory S,D,UO adecuados,
- asociar un posible filtro WMI para filtrar la aplicación de la directiva de grupo.
- en el caso en que la directiva de grupo esté desactivada por defecto, activar el vínculo de la directiva de grupo. Esta última operación puede realizarse de forma manual, o basada en un script. Esta última opción puede ser interesante para determinar el mejor momento de la puesta en disposición de la aplicación.

Por último, el software se instalará al arrancar el equipo o cuando un usuario inicia la aplicación.

En relación con los nombres de objetos de directivas de grupo y de la activación por defecto

Dos parámetros interesantes pueden ser definidos para simplificar algunas tareas de gestión de las directivas de grupo, en particular en relación con la gestión y mantenimiento de software.

- **Crear nuevos vínculos de objetos de directiva de grupo en estado deshabilitado de forma predeterminada**: este parámetro crea todos los nuevos vínculos a objetos de directivas de grupo en un estado deshabilitado por defecto. Después de haber configurado y probado los nuevos vínculos a los objetos, utilizando el componente Usuarios y equipos de Active Directory o el componente Sitios y Servicios de Active Directory, podemos activar los vínculos a los objetos para que estén operativos.

Este parámetro se recomienda para evitar que un error de vínculo tenga efectos «adversos» sobre los objetivos posibles presentes en el ámbito de gestión S,D,UO.

- **Nombre predeterminado para los nuevos objetos de directiva de grupo**: este parámetro nos permite especificar el nombre por defecto de los nuevos objetos de directiva de grupo creados a partir de herramientas como la consola de gestión MMC Directiva de grupo en las herramientas de Active Directory, y el Explorador de objetos de directiva de grupo. El nombre completo puede contener variables de entorno y puede contener hasta 255 caracteres como máximo.

Este parámetro es útil para ayudar a cumplir un esquema de nombres estándar para los objetos directivas de grupo definidos dentro del directorio Active Directory. En efecto, es posible que exista a largo plazo cientos o miles de objetos de directivas de grupo, para definir el conjunto de parámetros específicos de los equipos y usuarios de la empresa.

c. Garantizar el mantenimiento del software

Podemos proceder a la actualización de un software a una nueva versión, donde podremos reinstalar una aplicación provista de un nuevo Service Pack o de una actualización importante del software.

Mediante esta operación, la aplicación será actualizada o reinstalada de forma automática al arrancar el equipo o cuando el usuario arranque la aplicación en función de las opciones iniciales.

d. Eliminar el software

Podremos eliminar una aplicación cuyo ciclo de vida a alcanzado su término. Para esto podemos eliminar la declaración del software en el objeto directiva de grupo.

Mediante esta operación, la aplicación será eliminada de forma automática al arrancar el equipo o cuando el usuario abra una sesión en función de las opciones iniciales.

2. Tecnología Windows Installer y tipos de paquetes

a. Tecnología Windows Installer y tipos de paquetes

Los sistemas Windows emplean Windows Installer para permitir a la directiva de grupo el despliegue y la gestión del software. Este componente automatiza la instalación y la eliminación de las aplicaciones aplicando durante el proceso un juego de reglas de configuración definidas de forma centralizada. Windows Installer contiene dos componentes.

- **El Servicio Windows Installer**: este servicio por parte del cliente automatiza por completo el proceso de instalación y configuración del software. El Servicio Windows Installer también puede modificar o reparar una aplicación instalada existente. Se instala una aplicación directamente desde el CD-Rom o empleando la directiva de grupo. Para instalar una aplicación, el servicio Windows Installer necesita de un paquete Windows Installer.
- **El paquete Windows Installer**: este archivo de paquete contiene toda la información que el servicio Windows Installer necesita para instalar o desinstalar software. Un archivo de paquete contiene:
  - un archivo Windows Installer con extensión .msi,
  - cualquier archivo de origen externo requerido para instalar o desinstalar el software,
  - un resumen de la información relativa a normas del software y el paquete,
  - los archivos del producto o una referencia a un punto de instalación donde están estos archivos.

Las ventajas de la utilización de la tecnología Windows Installer son las siguientes:

- Instalaciones personalizadas: las funciones opcionales en una aplicación, tales como imágenes clipart, un tesauro, o la ayuda en línea pueden ser visibles en un programa sin que la característica sea realmente instalada. Aunque los comandos del menú sean accesibles, la funcionalidad no se instalará hasta que el usuario acceda al comando en el menú. Este método de instalación contribuye a reducir a la vez, la complejidad de la aplicación y la cantidad de espacio que ocupa en el disco duro.
- Aplicaciones tolerantes a fallos: si un archivo crítico se elimina o se corrompe, la aplicación recuperará de forma automática una nueva copia del archivo a partir de la fuente de instalación, sin que el usuario tenga que intervenir y sin requerir privilegios especiales.
- Eliminación misma: Windows Installer desinstala aplicaciones sin dejar archivos huérfanos ni dañar otra aplicación de forma inadvertida, por ejemplo, cuando un usuario borra un archivo compartido que otra aplicación necesita. Además, Windows Installer elimina todos los parámetros de registro relacionados con la aplicación y almacena en una base de datos las transacciones de instalación y los registros correspondientes. Cuando no es posible utilizar un software de recuperación para reparar una aplicación, o cuando un archivo de paquete Windows Installer no está disponible, use los archivos .zap (paquetes distintos de Windows Installer) para publicar las aplicaciones.

Las diferentes versiones de Windows Installer

En la medida que la tecnología Windows installer dispone de diferentes plataformas de sistema, se requiere disponer de una nueva versión adaptada a cada una de ellas.

A continuación listamos las diferentes versiones

Windows Installer 1.0: esta primera versión se implementó con Office 2000.

Windows Installer 1.1: esta versión se incluyó dentro de la familia de los sistemas operativos Windows 2000.

Windows Installer 2.0 (2.0.2600.0): esta versión fue incluida en Windows XP Profesional y soportada en sistemas Windows XP, Windows 2000, Windows NT 4.0 SP6 y también Windows Me.

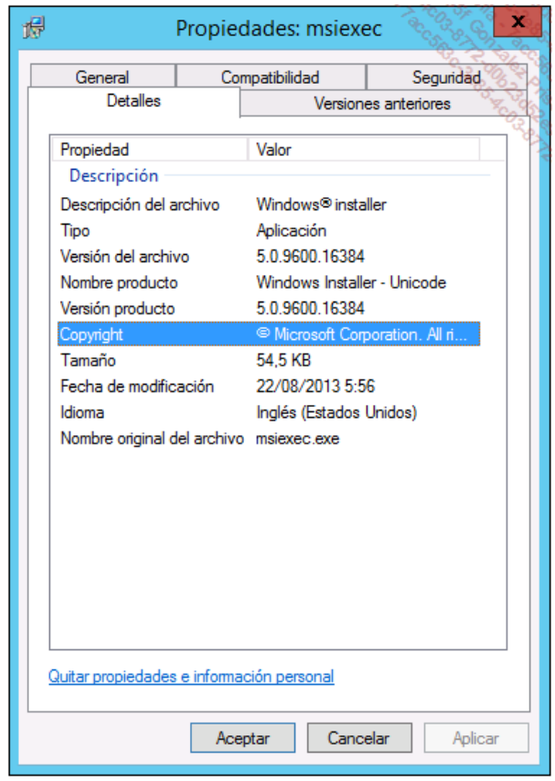
Windows Installer 3.0 (3.0.3790.2180): esta versión fue incluida en Windows XP Profesional SP2. El motor Windows Installer 3.0 es soportado por los sistemas Windows 2000 SP3 y SP4, Windows Server 2003 SP1 y SP2, Windows XP SP1 SP2 y SP3.

Windows Installer 3.1 (3.1.4001.5512): esta versión se distribuyó con Windows XP Profesional SP3.

Windows Installer 4.0: esta versión requiere de Windows Vista o Windows Server 2008. No hay ninguna versión redistribuible para poder instalar Windows Installer 4.0 en otras versiones de Windows. Una versión actualizada de Windows Installer 4.0, no añadirá ninguna nueva característica, se adaptó para su disponiblilidad para Windows Vista SP1 y Windows Server 2008 SP1 y SP2.

Windows Installer 4.5 (4.5.6001.22159): esta versión estuvo disponible como versión redistribuible para Windows Server 2008 SP2, Windows Vista SP2, Windows XP SP3, así como para Windows Server 2003 SP1 y SP2.

Windows Installer 5.0 (5.0.7600.16385): esta versión estuvo disponible con Windows Server 2008 R2 y Windows 7. También está disponible en las versiones posteriores, tales como Windows 10 y Windows Server 2016.



Versión de Windows Installer 5.0 en Windows 10 Professional

El desarrollador del paquete puede decidir que el paquete MSI en cuestión sólo funcione en una equipo que utilice tal o cual versión o nivel del sistema operativo. Cuando un mensaje de este tipo nos informa de dicha limitación, no se trata de un problema de incompatibilidad de Windows Installer, sino de una elección del desarrollador del paquete.

b. Aplicaciones reempaquetadas en formato MSI

En el caso de no disponer del software entregado en un archivo MSI, y si deseamos utilizar la tecnología de instalación y gestión de software, contamos con la posibilidad de crear el archivo MSI requerido.

Tan pronto como hayamos "transformado" una aplicación que se instala con un programa de instalación específico en una aplicación basada en la tecnología Windows Installer, podremos realizar, mantener o eliminar la aplicación utilizando la tecnología de gestión y mantenimiento de software empleando las directivas de grupo y los servicios de directorio Active Directory.

Los packages MSI disponen de funcionalidades avanzadas como la reparación automática de los componentes y la instalación de las funcionalidades bajo demanda. Como una aplicación reempaquetada como MSI no ha sido diseñada para soportar los conceptos de "features/components/resources", las aplicaciones reempaquetadas serán instaladas o reparadas en su totalidad y no en función de las opciones de funcionalidad bajo demanda.

Con Windows Server 2003, Microsoft entregaba la versión "light" de la herramienta de reempaquetado WinINSTALL LE (LE de *Limited Edition*) desarrollada por Microsoft y Seagate Software. Esta herramienta está hoy en día obsoleta para el uso con sistemas operativos como Windows 8.1 o Windows 10. Por lo tanto, podremos según nuestras necesidades adquirir un producto profesional como InstallShield distribuido por Flexera Software. Observe que InstallShield Limited Edition for Visual Studio está disponible de forma gratuita para los propietarios de Microsoft Visual Studio.

Encontraremos en el sitio Installsite.org, una comparación funcional de todos estos productos profesionales.

Un producto Windows que no utilice la tecnología de instalación Windows Installer no puede obtener el distintivo "Designed for Windows".

La creación de un archivo MSI para reempaquetar una aplicación se trata más adelante.

c. Archivos .Zap

Se trata del último tipo de archivo soportado capaz de utilizar la tecnología de instalación y mantenimiento de software.

Podemos crear un archivo .zap que contienen las instrucciones necesarias para la correcta publicación del software si no existe ninguna solución para disponer de un archivo MSI. Esta solución debe ser considerada como el último recurso, ya que en este caso, no se trata de una instalación realizada por el servicio de sistema empleando Windows Installer, sino por el shell de Windows en el contexto del usuario. Este último deberá disponer de los derechos de administrador del equipo local para que el software pueda ser instalado.

Podemos crear un archivo Zap empleando un editor de texto como el Bloc de notas. Este archivo está compuesto de las dos secciones siguientes:

- La sección dedicada a la aplicación `[Application]`,
- La sección dedicada a las extensiones de archivo de la aplicación `[Ext]`.

Configuración de la sección [Application]

Esta sección contiene los datos que especifican cómo instalar la aplicación, así como la información que se presentará a los usuarios en la sección del panel de control **Agregar o quitar programas**. El archivo Zap también deberá contener el nombre mostrado de la aplicación, denominada FriendlyName, así como los parámetros de instalación mediante el parámetro `SetupCommand`. Encontraremos a continuación la descripción de estos parámetros:

`FriendlyName`: muestra la descripción de la aplicación. Por ejemplo, para la aplicación App-Finance, declaramos "Aplicación Finanzas".

`SetupCommand`: contiene la ruta relativa a partir del punto de acceso al archivo. Si el archivo de comando a ejecutar está en el mismo directorio que el archivo Zap, entonces solo declaramos el nombre del comando acompañado de sus parámetros.

`DisplayVersion`: especifica el número de versión de la aplicación.

`Publisher`: especifica el fabricante de la aplicación.

`URL`: especcifica la ubicación de una URL que permite obtener información acerca de la aplicación.

Configuración de la sección [Ext]

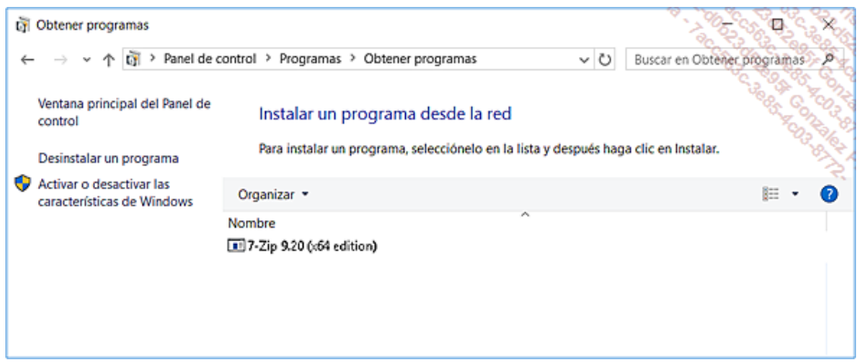
Esta sección no es obligatoria. Permite llegado el caso de publicar en Active Directory la naturaleza de las extensiones de archivos gestionados por esta aplicación. Para declarar las extensiones de archivos soportados por la aplicación, declare la sección `[Ext]`, luego agregue las distintas extensiones tal como se especifica en el ejemplo siguiente.

```
[Ext]

XLS=

XLC=
```

La pantalla de siguiente ilustra un ejemplo de archivo Zap para desplegar como aplicación publicada una antigua aplicación como el visualizador Microsoft PowerPoint 97.

Los dos parámetros necesarios dentro del archivo ZAP

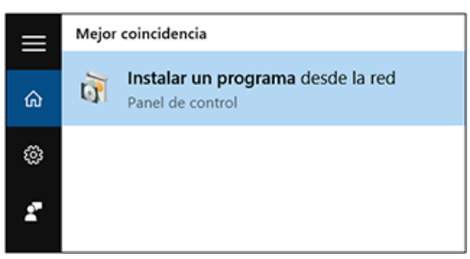
Una vez conectado, el usuario puede recorrer el almacén de aplicaciones administrado por Active Directory a través de los distintos despliegues que habremos efectuado.



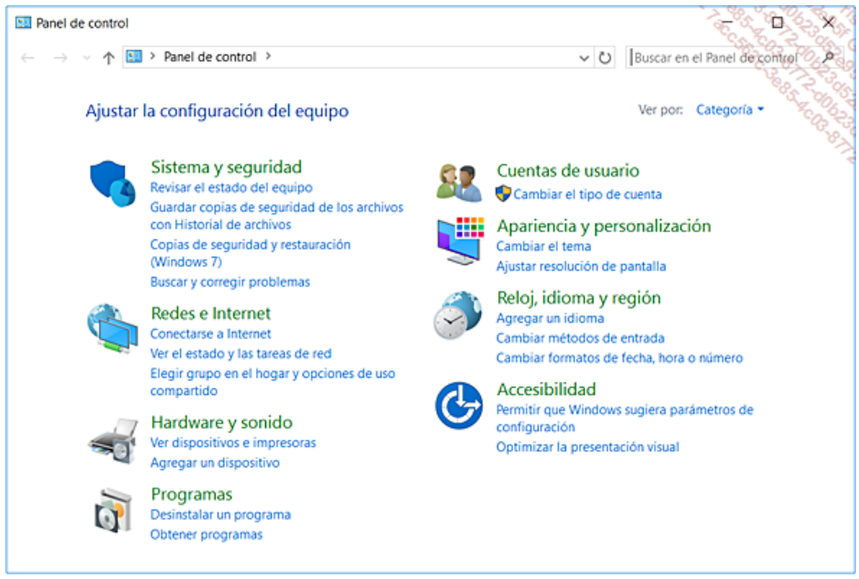
Acceso del usuario a las aplicaciones publicadas

En nuestro ejemplo, para utilizar la aplicación, el usuario podrá hace un sencillo doble clic en un archivo o bien optar por iniciar la instalación de forma automática. Para lograrlo, basta con examinar **Panel de control/Programas y características/Obtener programas**. Una vez mostrada la lista de los programas publicados, bastará con pulsar el botón **Añadir**.

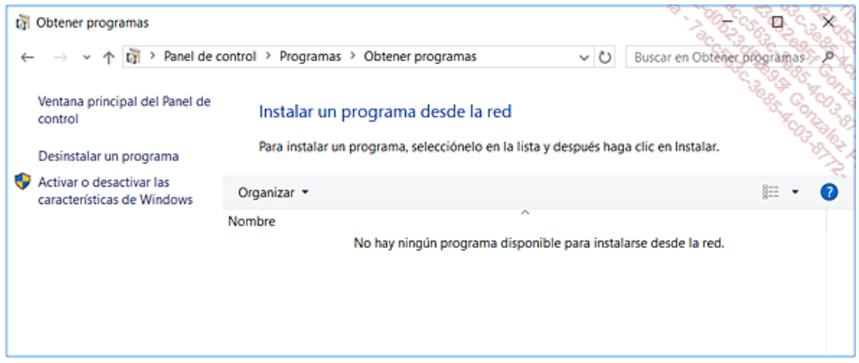
La interfaz de Windows 10 es totalmente intuitiva, el usuario podrá utilizar el menú **Inicio** y luego buscar con Cortana "Instalar un programa desde la red". También podremos utilizar el enlace **Panel de control / Programas y características / Instalar un programa desde la red**.



Búsqueda a través del menú Inicio y Cortana



Vínculo Programas / obtener programas



Opción "Instalar un programa desde la red ".

d. Observaciones generales sobre los diferentes formatos de instalación

Los puntos enumerados a continuación nos ayudarán a comprender las diferencias de fondo relacionadas con los diferentes métodos de instalación:

- Cuando el software es desplegado empleando un verdadero MSI, lo que es propio de cualquier aplicación "Compatible con Windows", todas las funcionalidades ofrecidas por el motor de instalación Windows Installer están disponibles, es decir, la instalación bajo demanda, la reparación automática y la eliminación misma y total del software.
- Las instalaciones realizadas en el contexto del servicio Windows Installer utilizan la cuenta de sistema local, por lo tanto cuentan con todas las autorizaciones para poder instalar, reparar, actualizar o eliminar el software en el equipo local.
- Los accesos a red utilizados por el Servicio Windows Installer para acceder a los archivos fuente de la aplicación explotan una autenticación de red que utiliza el contexto del equipo cuando se trata de una instalación que se refiere al equipo, o al usuario conectado si se trata de una instalación que se refiere al usuario. No puede tratarse de la cuenta sistema ya que esta cuenta debe contar con privilegios de acceso válidos a través de la red.
- Un archivo Zap no ofrece ninguna de las funcionalidades del servicio Windows Installer. Permite solo ejecutar el programa de instalación de forma independiente de la aplicación que se encarga del proceso de instalación o desinstalación en el contexto del usuario conectado.
- Una aplicación desplegada empleando una directiva de grupo y un archivo Zap será publicada solo en el panel de control en la sección**Programas y características**.

Configuración del despliegue de software

1. Creación de un nuevo despliegue de aplicaciones

a. Creación o modificación de una directiva de grupo

Una vez que tenemos un software que puede desplegarse empleando directivas de grupo, el procedimiento consiste en hacer disponibles uno o varios puntos de distribución.

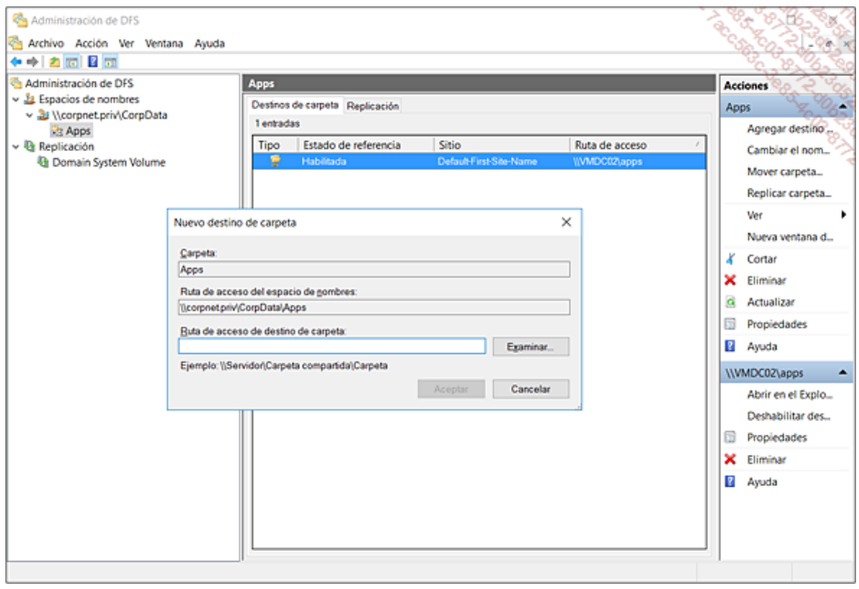
Podemos utilizar uno o varios recursos compartidos de red o una raíz DFS tolerante a fallos integrada en Active Directory para ofrecer un acceso mixto de alta disponibilidad. Una raíz DFS de dominio permite tener en cuenta la infraestructura de los sitios Active Directory.

Por ejemplo, podemos realizar las operaciones siguientes:

- crear una raíz DFS de dominio en la cual la raíz dispondrá de réplicas situadas en varios controladores de dominio ubicados en diferentes lugares,
- crear uno o varios vínculos dentro de la estructura DFS
- crear destinos adicionales para cada uno de los vínculos para apuntar a los servidores disponibles en cada uno de los sitios,
- replicar de forma manual los datos hacia los distintos vínculos de cada uno de los sitios.

La imagen siguiente ilustra la opción que permite añadir varios destinos en el nivel de una raíz DFS para un vínculo dado. Como información, los servidores DFS Windows Server ofrecen la posibilidad de incluir varias raíces DFS por servidor, así como la localización de los destinos en función de la topología de sitios Active Directory.

El número de destinos adicionales por vínculo DFS puede alcanzar treinta y dos como máximo. Con Windows Server 2012 R2 y Windows Server 2016, sabemos que las ediciones estándar y Datacenter son idénticas a nivel funcional. Observe no obstante que con Windows Server 2003 R2 y 2008 R2, este no era el caso. Por ejemplo, para soportar múltiples raíces DFS con servidores Windows Server 2008 R2, era necesario utilizar una edición de tipo empresarial o Datacenter.



Añadido de destinos de carpetas en la Consola Gestión del sistema de archivos distribuidos DFS

Una vez preparados los puntos de distribución, podemos declarar el software en una directiva de grupo procediendo como se especifica a continuación:

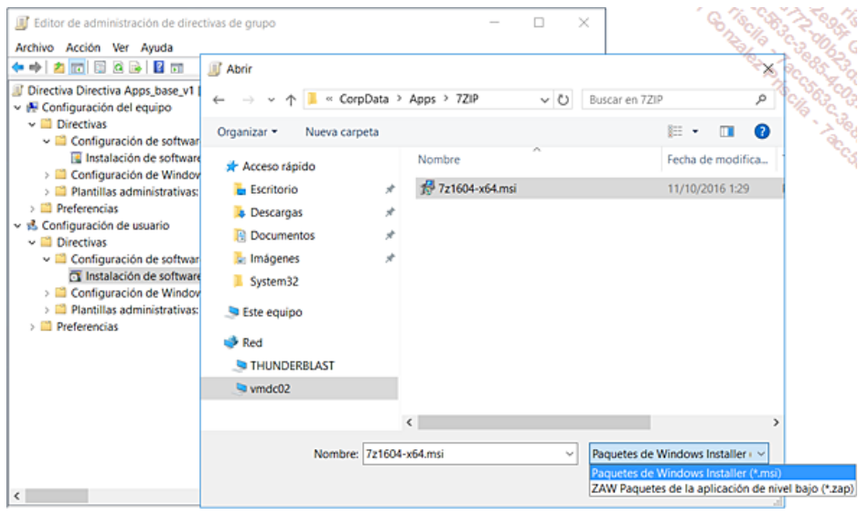
En una directiva de grupo, seleccionamos los nodos **Configuración del equipo** o **Configuración del usuario**.

Declaramos el nuevo software indicando la ruta de red donde se encuentra el archivo MSI.

La ventana de selección ofrecerá de forma exclusiva dos tipos de archivo:

- para el despliegue de aplicaciones a los equipos, podemos seleccionar solo archivos de tipo MSI,
- para el despliegue de aplicaciones a los usuarios, podemos seleccionar los archivos de tipo MSI o bien los archivos de tipo ZAP.

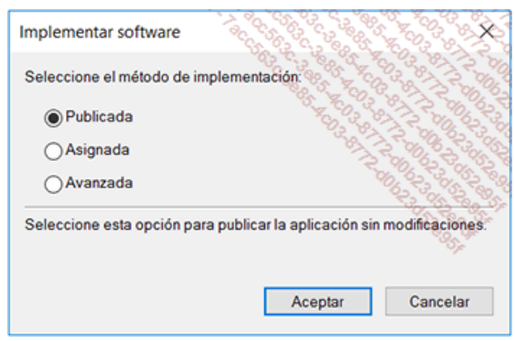
La imagen siguiente ilustra estos tipos de figura. La razón es que los archivos Zap sólo se refieren a aplicaciones que se instalan en el contexto del usuario y no a través del servicio Windows Installer. Estas aplicaciones no pueden aparecer en el Panel de control en el applet Programas y Características / Instalar un programa a partir de la red como aplicaciones publicadas.



Selección de un archivo MSI para las aplicaciones que aparecen publicadas para los usuarios

Por último, seleccionamos el método de despliegue adecuado.

Una aplicación puede ser publicada o asignada. Pero podemos también optar por seleccionar el modo avanzado que permite ajustar los detalles del despliegue.



Selección del tipo de despliegue

b. Configuración de las opciones de despliegue

Cada directiva de grupo puede contener varias aplicaciones. Cada aplicación dispondrá de sus propios parámetros de despliegue que especificarán cómo la aplicación se instalará, actualizará o eliminará. Podemos declarar estos parámetros en el momento de la declaración del software dentro de la directiva de grupo o más tarde, editando la directiva.

Como se muestra en la imagen anterior, tenemos dos grandes modos de despliegue.

Atribución de aplicaciones

Cuando asignamos aplicaciones a usuarios o equipos, éstas serán de forma automática instaladas en el equipo de inicio de sesión, para las aplicaciones asignadas a los usuarios, o bien para el inicio de aplicaciones asignadas a los equipos.

Cuando asigne una aplicación a un usuario, el comportamiento por defecto será su anuncio en el equipo la próxima vez que el usuario inicie sesión.

Esto significa que el método abreviado de la aplicación aparecerá en el menú **Inicio**, y que el registro se actualiza con los datos relativos a la aplicación, en particular, la ubicación de los paquetes de aplicación y de los archivos fuente de la instalación. Una vez publicados estos datos en el equipo del usuario, la aplicación será instalada por primera vez cuando el usuario la intente usar, es decir, en el último momento.

Aparte de este comportamiento por defecto, los clientes Windows XP hasta Windows 10 profesional cuentan con una opción para la instalación completa del paquete al iniciar la sesión, en lugar de una instalación durante el primer uso.

Debemos tener en cuenta que en el caso de que esta opción se encuentre definida, será ignorada por los equipos que funcionen con Windows 2000 que seguirán instalando las aplicaciones asignadas a un usuario solo en su primer uso.

Cuando una aplicación se asigna a un equipo, será instalada durante el próximo arranque del equipo. Las aplicaciones asignadas a los equipos no serán enunciadas, sino instaladas con la serie de características por defecto configuradas para el paquete.

La atribución de aplicaciones a través de una directiva de grupo requiere el uso exclusivo de archivos MSI. En efecto, los archivos Zap solo son utilizables como último recurso para los despliegues de tipo usuario por equipo.

Publicación de aplicaciones

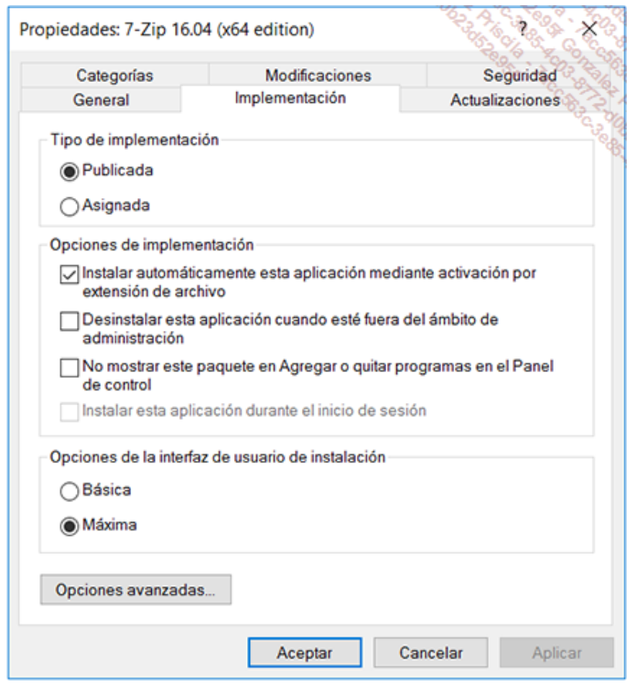
Podemos a su vez publicar las aplicaciones para los usuarios, que así las podrán instalar.

Para instalar una aplicación publicada, los usuarios pueden emplear **Programas y características** en el **Panel de control**. Éste contiene una lista de todas las aplicaciones publicadas accesibles por los destinatarios.

Si el administrador selecciona la característica **Instalar automáticamente esta aplicación mediante activación por extensión de archivo**, los usuarios pueden también abrir un archivo de documento asociado a la aplicación publicada.

Por ejemplo, si un usuario abre un archivo Zip, y el programa no está instalado, entonces la instalación de la aplicación asociada a esta extensión se pondrá en marcha.

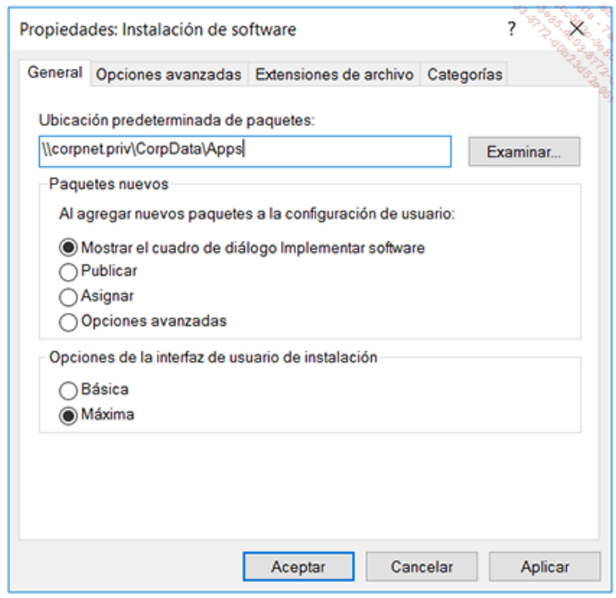
Observe que el modo Publicación de aplicaciones solo se aplica a la directiva de un usuario. No es posible publicar aplicaciones para un equipo.



Opciones de despliegue de software mediante GPO

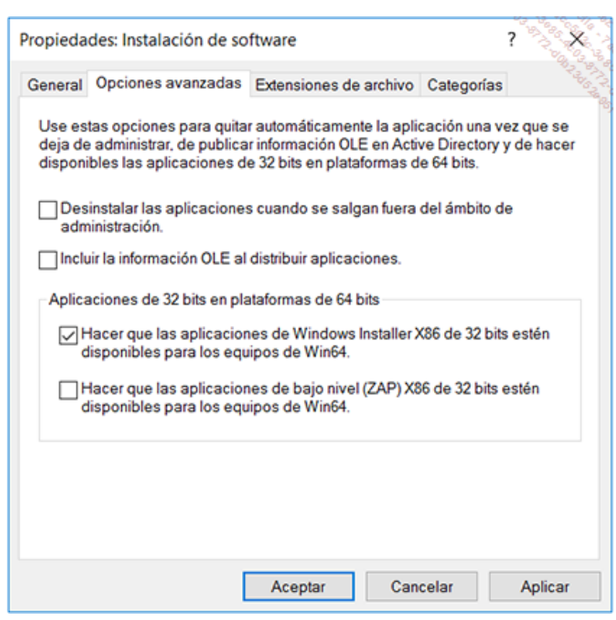
La imagen anterior muestra las diferentes opciones de despliegue disponibles. Podemos constatar que las aplicaciones atribuidas se instalan de forma automática empleando la extensión de la aplicación. De la misma forma, una aplicación asignada a un usuario es, por defecto, publicada de forma automática en el panel de control bajo el epígrafe **Programas y características**. La opción **No mostrar este paquete en Agregar o quitar programas en el Panel de control** le permitirá "ocultar" la publicación de la aplicación.

Parámetros del nodo "Instalación de software".



Ubicación de las opciones por defecto para el despliegue del software

Esta ventana nos permitirá declarar las opciones por defecto de todos los nuevos paquetes declarados dentro de una directiva de grupo. Esta ventana es muy práctica en la medida en que permite declarar los valores en función de nuestras preferencias.



Opciones OLE y compatibilidad de las aplicaciones Win64

La pestaña **Opciones avanzadas** permite gestionar ciertos comportamientos específicos tales como la compatibilidad de las aplicaciones de 32 bits en los equipos de tipo Windows 64 bits.

c. Asociación de extensiones de archivo

Podemos controlar qué aplicaciones están asociadas con qué extensiones. Por ejemplo, podemos desplegar la aplicación Winzip pero también Winrar para el mismo grupo de equipos o usuarios.

Con respecto al despliegue de estas dos aplicaciones en los equipos, no hay ningún problema, ya que se instalarán una tras otra durante el arranque del equipo.

Por el contrario, ¿quién puede decidir el despliegue empleado por los usuarios?

De hecho, el problema se refiere a la selección de la aplicación a instalar. En efecto, ¿qué aplicación debemos instalar al abrir un archivo zip sabiendo que dos aplicaciones gestionan este tipo de archivos? Podemos declarar el orden de selección preferido de instalación de la aplicación cuando un usuario invoca la extensión conflictiva accediendo a las propiedades del nodo **Instalación de software**. Los botones**Subir** y **Bajar** nos permitirán gestionar la prioridad de instalación de una aplicación en relación con las demás.

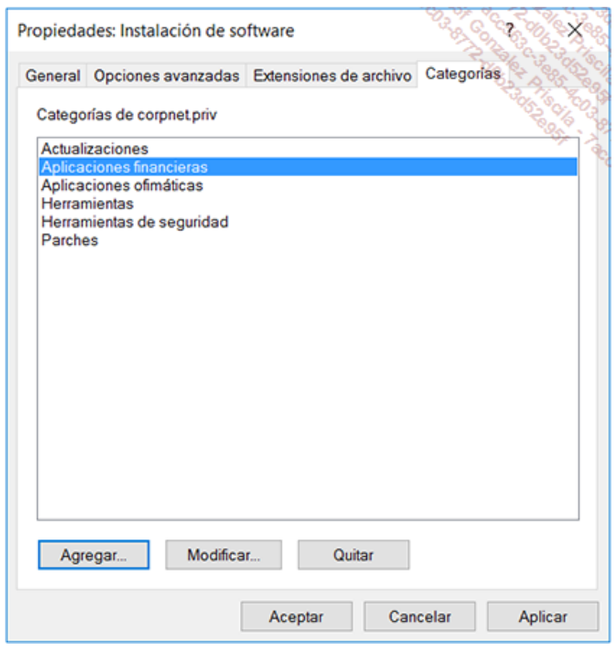
En nuestro primer ejemplo, si la aplicación preferida para los ficheros Zip es WinZip, entonces la aplicación Winzip se instalará de forma automática. El usuario puede también iniciar la instalación del programa de su elección, pasando por la opción del Panel de control **Programas y características**, o bien pulsando directamente en el icono del programa mostrado en el escritorio o bien en el menú **Inicio**.

d. Creación de las categorías de aplicaciones publicadas

La publicación de muchas aplicaciones requiere un cierto nivel de organización. Puedes organizar todas las aplicaciones publicadas en varias categorías para facilitar su selección por los usuarios de la red Active Directory.

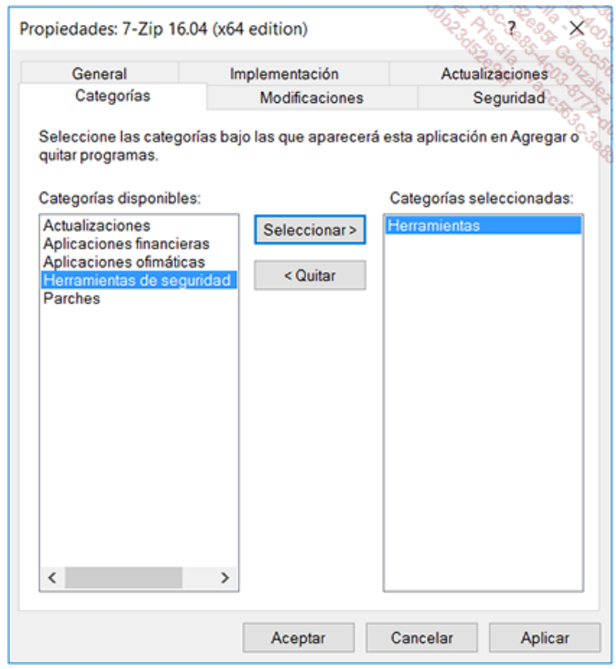
Podemos considerar la creación de varias categorías en función de los criterios especificados a continuación:

- **La naturaleza del software**: un modelo de organización es muy útil cuando la empresa dispone de muchas aplicaciones de un mismo tipo. Podemos, por ejemplo, agrupar todas las aplicaciones de ofimática en la categoría **Aplicaciones de ofimática** y todas las aplicaciones financieras en la categoría **Aplicaciones financieras**.
- **El modelo organizativo**: también podemos agrupar las aplicaciones en función de los diferentes departamentos. Por ejemplo, todas las aplicaciones de negocio necesarias para los usuarios del departamento de contabilidad podrían agruparse en una categoría llamada Aplicaciones Contabilidad.
- **Los tipos de actividades de los usuarios de la empresa**: también podemos agrupar las aplicaciones en función de los roles desempeñados en la empresa. Por ejemplo, todas las aplicaciones requeridas para la actividad de los directores podrían agruparse en una categoría llamada Aplicaciones - Dirección.



Creación de las categorías de programas

Una vez establecidas las categorías en función de los criterios que consideremos más relevantes, asociamos cada aplicación desplegada a las categorías.



Asignación de una aplicación a una o varias categorías

Mantenimiento de Software desplegado

1. Actualización de aplicaciones

Una aplicación desplegada empleando la tecnología de gestión y mantenimiento de software podrá ser objeto de una actualización opcional o una actualización obligatoria.

Una actualización opcional permite a los usuarios elegir si desea o no proceder a la actualización de dicha aplicación. A la inversa, una actualización obligatoria actualizará la aplicación de forma automática.

- En una actualización opcional, el usuario siempre tendrá la posibilidad de instalar la nueva versión, pasando por la opción del Panel de control **Programas y características**.

- Si la aplicación se actualiza de forma obligatoria, entonces la nueva versión se instalará de forma automática en su próxima ejecución.

Cuando una aplicación reempaquetada se actualiza, ¡el proceso de actualización no lo es en realidad! La aplicación desplegada en primer lugar es suprimida, y luego la nueva es instalada por completo.

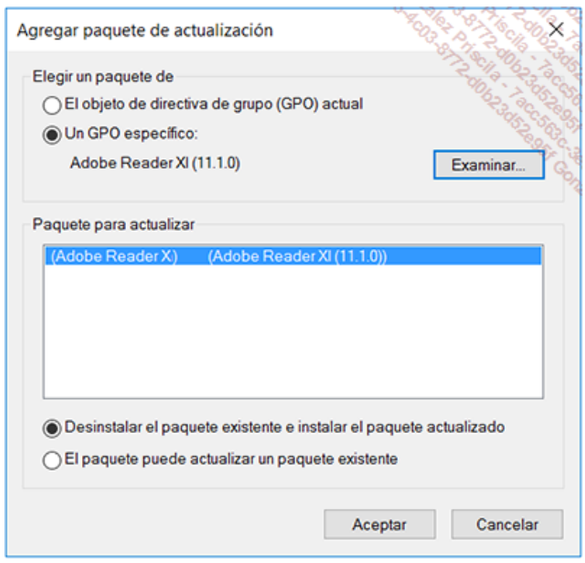
En general, el inconveniente de este método, además de sus efectos en términos de tráfico en la red, será la pérdida de todos los parámetros y preferencias del usuario, teniendo en cuenta que este comportamiento puede ser diferente de una aplicación a otra.

Este fenómeno no se producirá en el caso de la actualización de un producto de la misma familia. En este caso, el código de actualización se incluye en el archivo MSI mismo con el fin de considerar el estado inicial antes de la actualización.

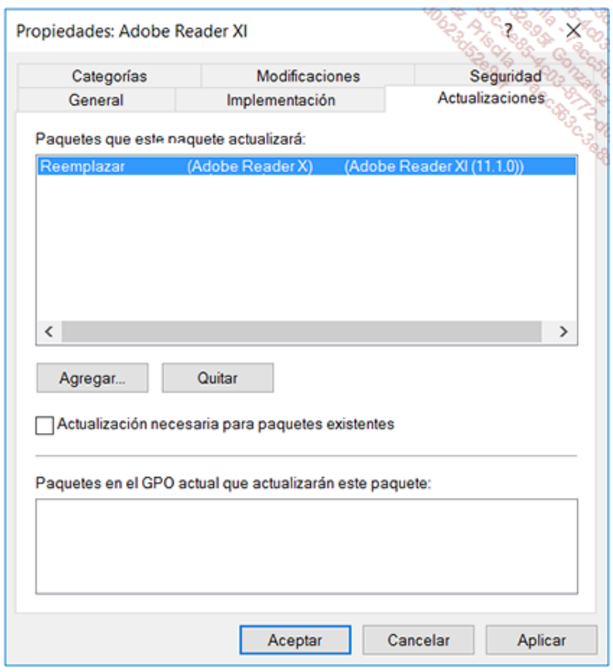
Para crear un software que desempeña el papel de actualización, seguimos el siguiente procedimiento:

Creamos una nueva directiva de grupo o agregamos a una directiva existente, el nuevo software que actuará como actualización,

En la pestaña **Actualizaciones**, declaramos los paquetes que serán actualizados por el que acabamos de declarar.



El paquete Adobe Acrobat Reader XI es la actualización del paquete Adobe Acrobat Reader X



La aplicación Adobe Acrobat Reader XI reemplazará Adobe Acrobat Reader X, si el usuario lo desea

Las dos pantallas muestran que la aplicación Adobe Acrobat Reader XI reemplazará de forma opcional, a la versión de Adobe Acrobat Reader X.

Tenga en cuenta que la consola de gestión de directivas de grupo es capaz de determinar de forma automática si dos aplicaciones son capaces de lograr una verdadera operación de actualización.

También observaremos que la primera imagen muestra que el paquete para actualizar es seleccionado a partir de una directiva de grupo

diferente de la que contiene la actualización. Esto significa que cualquier software de cualquier directiva puede ser visto como una aplicación que puede ser actualizada. En otras palabras, y aunque no sea obligatorio, un software no debería ser declarado más que una sola vez.

2. Despliegue de Service Packs y actualizaciones

El despliegue de un Service Pack o de una actualización de aplicación provocará la redistribución de la aplicación de tal manera que los equipos y/o usuarios que cuenten con la aplicación podrán disponer de la nueva versión.

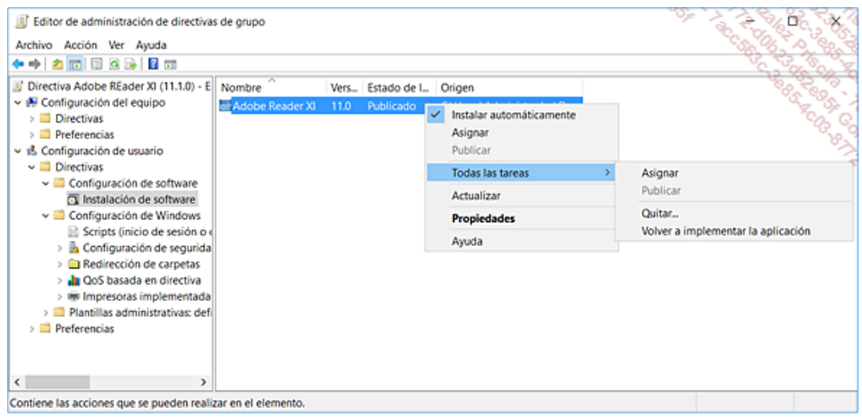
Los nuevos equipos o usuarios instalarán de forma directa la versión más actualizada. La pantalla siguiente ilustra el hecho de que es su responsabilidad prevenir a la infraestructura de que el software ha "cambiado". Esta operación se denomina "redespliegue de aplicaciones".

Para realizar una operación de despliegue de un Service Pack o de una actualización de software, podemos proceder como sigue:

Obtenga el Service Pack o la actualización de software, la cual es proporcionada por el fabricante del sistema o de la aplicación.

Coloque los archivos del Service Pack en la misma ubicación que los archivos fuente originales. Entre los archivos entregados, debemos por necesidad contar como mínimo con archivos .MSP y un nuevo archivo MSI. Un archivo en formato MSP es un archivo estándar definido en las especificaciones Windows Installer. Este archivo describe en detalle las operaciones a realizar como los archivos a sustituir y las posibles modificaciones de parámetros a introducir en el registro del sistema.

Ejecutamos la tarea **Volver a implementar la aplicación**.



*La opción **Volver a implementar la aplicación** permite "refrescar" el software ya desplegado*

Un mensaje de advertencia avisará de la importancia de la operación.

En efecto, en función de la importancia de la actualización, podemos considerar que se trata casi de una verdadera nueva instalación, con la salvedad de que todos los parámetros se recuperarán.

Si durante la descarga de un Service Pack o de una actualización, los archivos MSP y MSI no son "visibles", es probable que el archivo descargado sea un archivo ejecutable auto expandible.

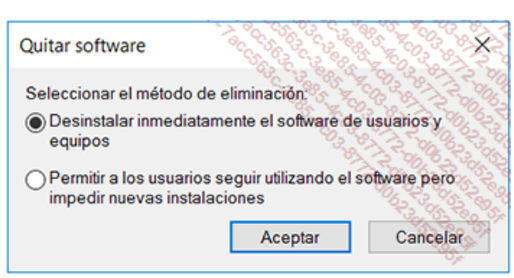
Informe a los posibles usuarios utilizar para extraer el conjunto de archivos e integrarlos en el directorio de la aplicación (por lo general, la extracción se obtiene empleando el parámetro /X). Este procedimiento suele estar documentado en el sitio del proveedor de la aplicación y nos permitirá preparar de forma correcta al servidor de distribución en previsión de una próxima redistribución.

En sentido amplio, en función del software, las actualizaciones de software pueden ser objeto de un despliegue de tipo equipo y/o usuario.

3. Eliminación de software

La supresión de un software puede ser forzada. En este caso, tan pronto como se verifique la directiva de grupo, el software será eliminado por completo, ya sea durante el arranque del equipo en el caso de una directiva de grupo aplicada al equipo o durante el inicio de sesión del usuario en el caso de una estrategia aplicada al usuario.

La pantalla siguiente muestra la simplicidad de la operación y también el impacto devastador en caso de error de manipulación. Podemos además señalar que no es posible acceder a esta operación tocando sobre la tecla [Supr].



Eliminación de un software en modo obligatorio.

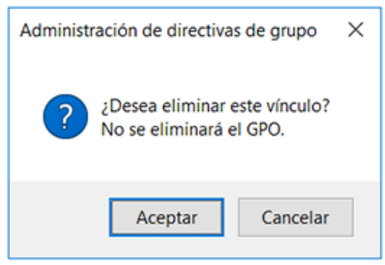
Si no deseamos que la aplicación sea eliminada, en este caso, escogeremos la opción: **Permitir a los usuarios seguir utilizando el software pero impedir nuevas instalaciones** que permite a los usuarios conservar la aplicación.

Observe que podemos obtener el mismo efecto manteniendo el software en la directiva de grupo, pero desactivando la directiva de grupo que permitió el despliegue inicial.

Recuerde anotar el nombre de la directiva de grupo utilizada durante la operación de eliminación. En efecto, cuando declaramos en una directiva de grupo dada que el software debe eliminarse, este software no aparecerá más en la lista de aplicaciones. Además, no será posible "ver" la operación todavía en curso.

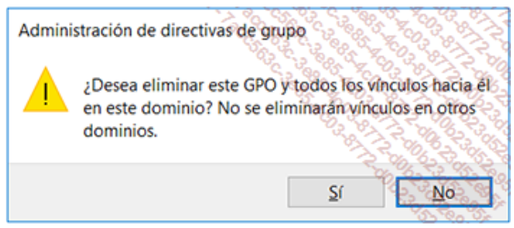
Con respecto a las operaciones de eliminación: éstas pueden ser peligrosas, la interfaz gráfica de las diferentes herramientas de administración de Active Directory fue diseñada con cuidado. Sus puntos diferentes se explican de forma breve a continuación:

- En caso de una eliminación de una aplicación dentro de una directiva de grupo: esta operación no puede realizarse con ayuda de la tecla [Supr]. Debemos por necesidad usar el menú **Todas las tareas .../Eliminar ...**.
- En caso de eliminar un vínculo de la directiva del grupo en la consola de administración MMC directivas de grupo: esta operación puede realizarse usando la tecla [Supr]. Sin embargo, los daños ocasionados son limitados, ya que siempre es fácil crear un vínculo destruido por error.



Confirmación de la eliminación de un vínculo de GPO en una UO

- En caso de eliminar un objeto de directiva de grupo en la consola de administración MMC directivas de grupo: esta operación puede realizarse usando la tecla [Supr]. Sin embargo, los daños ocasionados serán más limitados que en el caso anterior si hemos guardado los objetos directivas de grupo, por ejemplo empleando uno de los scripts que vienen con la consola de gestión de directivas de grupo.



Eliminación de un objeto GPO empleando la consola de gestión de directivas de grupo

Introducción

Los servicios de directorio Active Directory y sus diferentes componentes centrales forman el corazón de los sistemas de información implementados utilizando la plataforma Windows Server. Aparecido con Windows 2000 Server, los servicios de directorio Active Directory se impusieron de forma veloz como una plataforma central capaz de incluir servicios de seguridad avanzada y muchas aplicaciones capaces de usarlo como referencia. Uno de los puntos más importantes que contribuyó a este éxito es por supuesto la gran compatibilidad con el conjunto de los protocolos entre diferentes versiones de controladores de dominio Windows y sistemas operativos cliente. En efecto, es frecuente la necesidad de soportar infraestructuras compuestas por servidores y controladores de dominio que funcionan con diferentes versiones de Windows Server y con puestos de trabajo Windows y no Windows tales como Mac OS y diferentes versiones de Unix y de Linux.

Este importante éxito permitió a los equipos de desarrollo de Microsoft extender de forma significativa los servicios integrados en Active Directory para que estos servicios sean el soporte de una plataforma completa de gestión de identidades y de gestión de acceso a escala empresarial.

1. Servicios de directorio Windows Server y servicios asociados

Los servicios fundamentales de los servicios Active Directory fueron introducidos con Windows 2000 Server. De partida, se hizo énfasis en la adopción de los estándares de industria. En efecto, se escogieron los protocolos LDAP v2 y v3, Kerberos v4 y v5, los servicios DNS modernos y el servicio de tiempo NTP (*Network Time Protocol*). Los mecanismos de replicación son potentes y permiten desplegar infraestructuras de dominio que incluyen varias centenas de controladores. En este punto, el énfasis fue enfocado a la gestión de los objetos más importantes tales como los objetos equipo, grupo, usuario, impresora y carpetas compartidas. Uno de los objetivos principales es permitir mediante un único inicio de sesión un acceso al conjunto de recursos de la empresa. De esta forma, los usuarios pueden ubicar y acceder de forma sencilla a los recursos necesarios para el ejercicio de su actividad. Por su parte, el personal a cargo de la administración dispondrá de una infraestructura de directorio coherente e intuitiva basada en un modelo organizado y jerárquico de la red y los elementos que la integran. Desde este punto vista, el más notable será sin duda alguna la tecnología IntelliMirror la cual se apoya en el modelo de administración basado en sitios, dominios y unidades organizativas (modelo de gestión S,D,UO) y las directivas de grupo (objetos GPO, *Group Policy Object*) y preferencias de directivas de grupo (GPP,*Group Policy Preferences*).

Una versión resultado de los servicios de certificados

Los servicios de certificados de Windows Server 2016 forman parte de los servicios de infraestructura de Active Directory. De esta forma es posible instalar una Autoridad de certificación (CA, *Certification Authority*), para emitir y gestionar certificados digitales. Estos certificados podrán ser utilizados para la autenticación de usuarios y equipos y para el uso de aplicaciones tales como el acceso a sitios Web seguros via SSL (*Secure Socket Layer*) o el correo electrónico. Si bien es cierto que las autoridades de certificación Windows Server no están íntimamente integradas en los servicios de dominio de Active Directory, las autoridades de certificación de tipo Raíz de la empresa, por lo tanto, integradas dentro de la configuración Active Directory, soportan las funcionalidades modernas como la grabación automática de certificados para los equipos, los usuarios, así como la autenticación de Active Directory empleando una tarjeta inteligente, llamada Smart Logon.

Administrador de autorizaciones y particiones del directorio de aplicaciones

Del lado de los servicios de directorio, Microsoft continua su trabajo de ampliación de la plataforma Windows Server. La idea es extender los servicios de seguridad Active Directory para que las aplicaciones puedan llamarlos de forma más eficaz. Para lograrlo, se implementan dos grandes novedades: el administrador de licencias (*Authorization Manager*) y las particiones del directorio de aplicaciones. El primer componente proporciona un conjunto de interfaces de programación COM (*Component Object Model*) que permite a una aplicación administrar y controlar las demandas iniciadas por los usuarios en base a una gestión "aplicativa" de los roles. El segundo componente esta integrado de forma directa en Active Directory. En efecto, las particiones del directorio de aplicaciones están soportados por los controladores de dominio Windows Server 2003 y las versiones posteriores. Los datos almacenados en la partición de aplicaciones se destinan a los casos donde los datos deben ser replicados, pero no por necesidad a escala empresarial. Es entonces posible crear particiones del directorio replicadas solo en los controladores seleccionados de forma específica en el bosque Active Directory.

Las aplicaciones o servicios utilizan el protocolo LDAP y autenticaciones Kerberos como métodos estándar para acceder a la información de la aplicación. De esta forma, los servicios de directorio Active Directory juegan un papel de federador de forma total.

2. Servicios de gestión de los derechos digitales AD RMS

Windows Server 2016 ofrece también otro componente asociado a Active Directory, los servicios de gestión de derechos digitales Windows AD RMS para Windows Server 2016. La primera versión de esta tecnología se introdujo desde Windows Server 2003, a través de una descarga a partir del sitio de Microsoft. Desde entonces, la tecnología ha ido evolucionando de forma progresiva con Windows Server 2012 R2 y esta nueva versión 2016. Estos servicios de seguridad de documentos garantizan la protección de la información y funcionan con las aplicaciones y navegadores compatibles con la tecnología AD RMS. De esta forma, los datos digitales controlados a través de la tecnología AD RMS están protegidos contra cualquier uso no autorizado o indebido. En efecto, cada vez más, la fuga de información confidencial puede provocar una pérdida de volumen de negocio, afectar la competitividad de una empresa, y mucho más. Los métodos de seguridad como cortafuegos y listas de control de acceso (ACL) impiden el acceso no autorizado a la información en el perímetro de almacenamiento controlado, pero en absoluto cuando las personas habilitadas acceden y "toman posesión" de datos de carácter sensible o confidencial.

Securización de la información con AD RMS

El cifrado de datos protege la información durante el tránsito en la red. ¿Pero que ocurre cuando el documento se copia en una llave USB o se transmite por e-mail a una persona situada en el exterior del perímetro de seguridad de la empresa?

RMS protege la información confidencial del uso no autorizado, ya sea en línea, sin conexión, dentro o fuera de la red de la empresa. De forma práctica, los desarrolladores definen las condiciones en las que el destinatario puede utilizar uno u otro tipo de datos, mientras que el autor de un documento podrá utilizar estas mismas condiciones. Por ejemplo, la gestión de derechos digitales incluida en Microsoft Office profesional a partir de la versión 2003 y hasta la más reciente versión 2016, soporta operaciones seguras "abrir, modificar, imprimir y transferir". Por ejemplo, ¡puede que un usuario que utiliza Microsoft Outlook reciba un mensaje confidencial de su dirección y no pueda imprimirlo, ni copiar o transferir a otro destinatario!

Desde el punto de vista técnico, la plataforma AD RMS combinan las funciones, herramientas de desarrollo y las tecnologías de seguridad incluidas en Windows Server, tales como los servicios de cifrado, los certificados XrML (*eXtensible rights Markup Language*) y los mecanismos de autenticación fuerte capaces de garantizar la aplicación de una solución fiable de protección de la información. Para desplegar una solución AD RMS, es necesario disponer de los servicios de dominio de Active Directory, servicios IIS, los servicios de Microsoft Message Queuing así como de Microsoft SQL Server o Windows Internal Database (WID).

3. Ofrecer una conexión unificada SSO a los servicios Web mediante ADFS

Los servicios de la Federación de Active Directory (ADFS) aparecieron en primera instancia con Windows Server 2003 R2. Desde entonces, se han visto mejorados de forma considerable a lo largo de las versiones de Windows Server y empleados con mayor frecuencia por los productos de Microsoft que recurren a servicios de autenticación abiertos hacia el exterior, pero no solo. En efecto, estos servicios permiten hacerse cargo de escenarios de autenticación en empresas que amplían el acceso de sus aplicaciones Web internas a socios externos o filiales situadas fuera del perímetro de la empresa o directamente en Internet. Por lo tanto, para proporcionar acceso seguro y medios de gestión coherentes, la gestión de los servicios de la Federación se han convertido poco a poco en un elemento clave de la implementación de servicios Web. Los servicios de la Federación de Active Directory AD FS se basan en la especificación Web Services Architecture (o WS-*) y permiten el acceso a los servicios de seguridad de Active Directory. De esta manera los mecanismos de autenticación son utilizables, mediante ADFS, con otras organizaciones, permitiendo así una ampliación de la infraestructura de Active Directory existente con los mecanismos de acceso único de tipo SSO (*Single Sign On*).

Así, los usuarios aprobados y declarados una sola vez pueden acceder. Este principio fundamental permite reducir el número de ubicaciones donde una cuenta debe crearse y al mismo tiempo simplifica la administración. Otro aspecto importante es la seguridad, ya que la unicidad de la identidad del usuario reduce el riesgo de errores causados por posibles conflictos o confusiones en el nivel de cuentas, es decir, las identidades.

Por último, la arquitectura de ADFS se basa en los standards WS-*, desde un punto de vista técnico es posible soportar comunicaciones con sistemas diferentes. ADFS se integra de cerca con los servicios de directorio Active Directory y ADAM, de tal manera que es fácil acceder a los atributos de usuarios y proceder a la autenticación de usuarios en los dominios Active Directory o las instancias de tipo ADAM. Si se utilizan estos, la autenticación será de tipo BIND LDAP, mientras que en el caso de los dominios Active Directory o entornos basados en Unix o Linux, ADFS podrá utilizar todos los métodos soportados a saber, Kerberos, certificados digitales X.509 v3 y la autenticación mediante tarjetas inteligentes de tipo Smart Logon. Veremos más adelante que Windows Server 2016 incorpora una evolución de los servicios AD FS con muchas características nuevas.

4. Gestión de identidades con Active Directory, Azure AD y MIM 2016

Por último, Active Directory es en verdad el corazón de la gestión de identidades. Una buena gestión de los servicios de dominio Active Directory debe permitir estandarizar y simplificar todo lo que afecta a la gestión de identidades, por lo tanto, los usuarios y contraseñas. Los servidores de aplicaciones no-Windows deben tender hacia una utilización del protocolo Kerberos, del cual conocemos su robustez, para mejor coordinar la gestión de identidades. Por último, la última versión de Microsoft Identity Manager 2016 puede servir para sincronizar los múltiples espacios de almacenamiento de cuentas de usuario.

Microsoft Identity Manager 2016

MIM 2016 recoge las poderosas funcionalidades de gestión de identidades ya presentes en FIM 2010 R2 (*Forefront Identity Manager*). Esta nueva versión soporta, en particular, los escenarios híbridos y el soporte de nuevas plataformas. Así, Microsoft Identity Manager 2016 permite, por ejemplo, la creación de informes incluyendo Azure AD. Del mismo modo, el portal de autoservicio de restablecimiento de contraseñas soporta autenticación multifactor ofrecida con Azure Active Directory en su versión Premium (autenticación MFA, *Multi Factor Authentication*).

Privileged Identity Management

Una nueva funcionalidad llamada PIM *Privileged Identity Management*, nos permite también gestionar los accesos de alto poder de administración a través de un acceso temporal basado en las tareas relacionadas con los recursos. De esta manera, no es necesario conceder accesos de tipo "Administrador" -siempre problemáticos en términos de seguridad. Además de este marco de uso, la funcionalidad PIM permite extraer y aislar a las cuentas de administración de los bosques de Active Directory existentes.

MIM, gestión de certificados, tarjetas inteligentes y portal de autoservicio

Para las empresas que empiezan a hacer un uso importante de certificados, esta nueva versión Microsoft Identity Manager 2016 asegura una gestión de certificados a través de una API de tipo REST. Esta implementación permite soportar escenarios complejos compuestos de varios bosques Active Directory, propone una nueva aplicación publicada en la tienda Windows Store para la gestión del ciclo de vida de los certificados, tarjetas inteligentes virtuales (Virtual RPM) y también una gestión de eventos. Por último, para mejorar aún más la experiencia del usuario, los escenarios de autoservicio incluyen ya el desbloqueo de cuenta y la posibilidad de reiniciar la contraseña a través de una autenticación multifactor.

Observe que esta nueva versión de Microsoft Identity Manager 2016 soporta las últimas versiones de los entornos Microsoft Office, Windows Server y System Center.

5. Servicios de directorio Windows Server 2016 y servicios asociados

Windows Server 2016 es la base que permite la aplicación de todos los servicios que acabamos de descubrir. Así, con el mismo espíritu que Windows Server 2008 R2, y luego Windows Server 2012 y 2012 R2, Windows Server 2016 mejora el conjunto de estos diferentes bloques, que presentamos de forma rápida a continuación:

- Los servicios AD DS, de *Active Directory Domain Services*, y los servicios AD LDS, para *Active Directory Lightweight Directory Services*, ofrecen los servicios y componentes fundamentales de tipo dominio y de tipo autónomo.
- Los servicios AD CS, de *Active Directory Certificate Services*, aportan certificados digitales X.509 v3 necesarios para la aplicación de todos los mecanismos criptográficos actuales, así como el conjunto de servicios ofrecidos por una infraestructura de claves públicas PKI (*Public Key Infrastructure*).
- Los servicios AD RMS de *Active Directory Rights Management Services*, proporcionan una infraestructura capaz de proteger la información crítica y confidencial contenida en documentos y otros mensajes electrónicos.
- Los servicios AD FS, de *Active Directory Federation Services*, proporcionan la infraestructura y los mecanismos capaces de ofrecer un inicio de sesión único de tipo SSO a aplicaciones y servicios Web eliminando la necesidad de crear varias identidades para el mismo usuario.

Características de los servicios de dominio AD DS de Windows Server 2016

1. Introducción

El conjunto de capítulos anteriores planteó los conceptos y características de los servicios de dominio Active Directory ofrecidos por Windows Server. Hemos abordado de forma amplia los puntos sensibles en materia de servicios DNS, en particular la integración de las zonas DNS en Active Directory, la estructura de los bosques y los servicios de administración tales como las directivas de grupo. Las páginas siguientes permiten poner de relieve las características más notables implementadas en Windows Server 2016.

Vamos pues, a tratar los puntos siguientes:

- El fortalecimiento de la seguridad de los controladores de dominio instalados en sucursales mediante la instalación en modo Server Core.
- El fortalecimiento de la seguridad de los controladores de dominio instalados en sucursales con el nuevo rol de controlador de tipo sólo lectura (en inglés RODC de *Read Only Domain Controller*).
- La creación de nuevas directivas de contraseña granulares aplicables de forma directa a los usuarios o grupos de dominio, además de la habitual directiva de contraseña aplicada en todo el dominio. Aunque esta característica fue aportada por Windows Server 2008, es bueno revisar este tema en el momento en que la seguridad y la securización de las plataformas se encuentra en el corazón de las preocupaciones de muchas empresas.
- La posibilidad de activar en caso necesario las nuevas funciones de auditoría disponibles en los controladores de dominio Windows Server, a partir de Windows Server 2008 R2 y en las versiones posteriores, tales como Windows Server 2016.
- La posibilidad de proteger los objetos de Active Directory contra el borrado utilizando las nuevas herramientas de administración Active Directory de Windows Server.

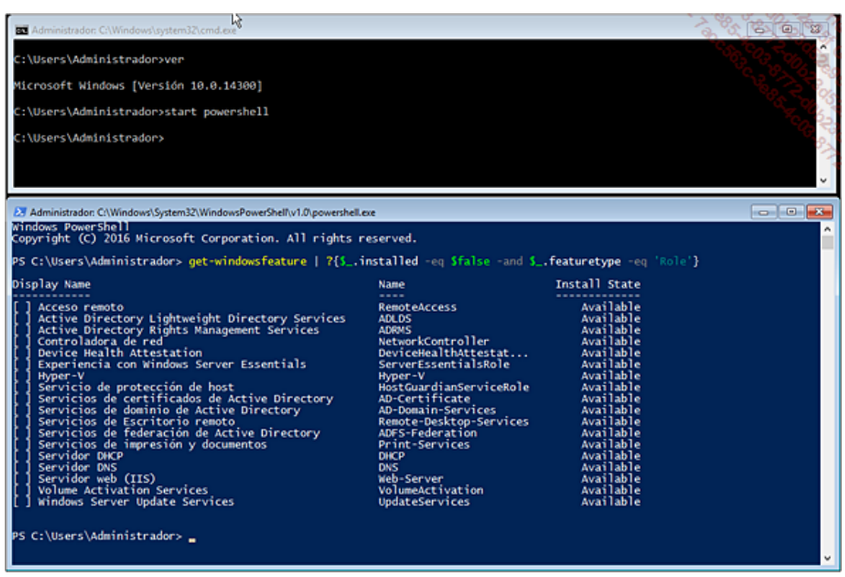
2. Rol de controlador de dominio y modo Server Core

a. Acerca del modo Server Core

De partida, el concepto de Server Core parece una señal de un paso atrás, hacia algo anodino, pobre o limitado. Este no es el caso porque la mayoría de los roles y funcionalidades aportadas por Windows Server 2016 están -casi todas- disponibles en modo Core. De hecho, se podría decir que Windows Server 2016 en modo Server Core ofrece toda la potencia de Windows Server, ¡pero sin la interfaz gráfica de Windows!

Este enfoque no es negativo, está lejos de serlo. En efecto, aunque se entiende que la modernidad de las interfaces y los asistentes de configuración y administración de Windows Server 2016 se han realmente perfeccionado, y si durante los últimos quince años todo fue hecho para hacer los sistemas operativos más asequibles y por lo tanto más fáciles de controlar, también es cierto que la línea de comandos permite a los administradores experimentados ganar tiempo y capacidad de limitar los errores a veces imputables a algunas imperfecciones de una determinada interfaz. Veremos más adelante que no se trata solo de estos beneficios por supuesto.

Así, la instalación en modo Server Core disponible con Windows Server 2016 soporta todos los servicios disponibles en una versión de tipo Standard o Datacenter. La imagen siguiente lista los roles disponibles con Windows Server 2016 en modo Core -sin mostrar la lista de todas las funcionalidades:



Lista de roles disponibles en Windows Server 2016 en modo core

Para ver la lista de todos los roles, sin mostrar la lista de innumerables funcionalidades, podemos usar el comando Windows PowerShell siguiente: `get-windowsfeature | ?{$_.installed -eq $false -and $_.featuretype -eq 'Role'}`

Observe que las instalaciones de Windows Server 2016 en modo Server Core soportan la seguridad de los discos empleando BitLocker, así como la protección anti-virus Microsoft Windows Defender.

Tenga en cuenta que Windows Defender integrado en las versiones de Windows 8.1 y Windows 10 ya está disponible con Windows Server 2016, incluso en sus versiones Core y Nano Server.

Reducir las operaciones de mantenimiento

Es evidente que un sistema operativo está compuesto principalmente de archivos centrales esenciales que implementan el corazón del SO. La interfaz gráfica que le acompaña solo tiene una importancia relativa con respecto al papel que desempeñará el equipo en la red de la empresa.

Por último, en función de la criticidad del servidor, podremos mediante una instalación en modo Server Core, disponer de un servidor "aligerado" y totalmente funcional para los roles importantes de la empresa. Observe que algunos programas adicionales de terceros o Microsoft podrían requerir la presencia de la interfaz gráfica (con posibilidad de añadir a posteriori).

Reducir la exposición, la superficie de ataque, los bugs y también las operaciones de mantenimiento y soporte

Ya que una instalación en modo Server Core es mínima, muchos componentes no están presentes y la superficie de ataque se ve reducida. Por

consiguiente, la reducción del número de componentes y servicios reduce el volumen de código, lo que tendrá el efecto de reducir de forma considerable el número de parches necesarios.

Reducir el espacio del disco

La instalación de Windows Server 2016 en modo Core permite ahorrar alrededor de 4 GB en comparación con una instalación convencional con la interfaz gráfica. Este punto puede ser interesante para las empresas que disponen de salas de máquinas formadas por cientos o miles de servidores. A este nivel, las economías de escala en el espacio en disco consumido por el sistema operativo pueden ser importantes representando cientos de gigabytes.

Recuerde que los sistemas equipados con más de 16 GB de RAM necesitan disponer de más espacio en disco (Archivos de paginación, hibernación y crash dump).

b. Limitaciones de una instalación en modo Server Core

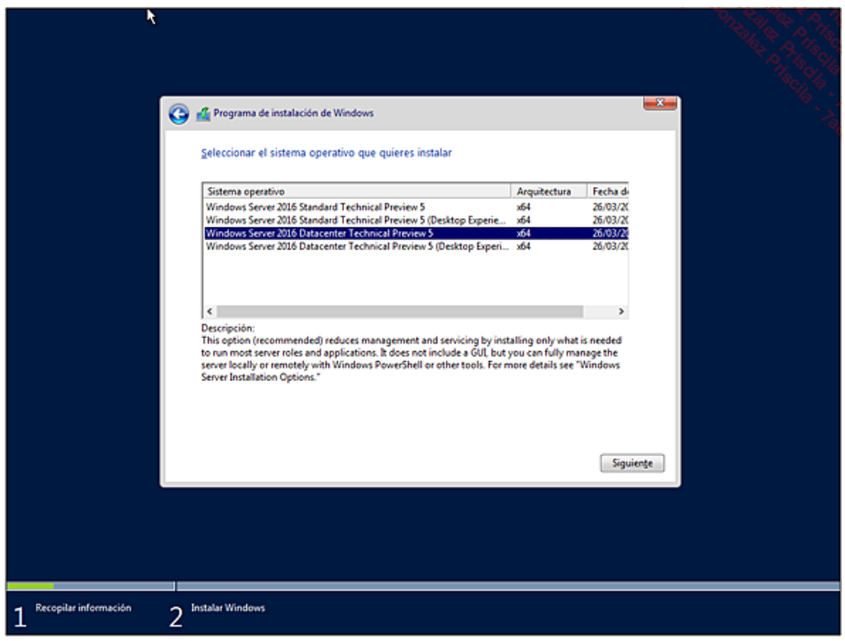
A pesar de las ventajas de este tipo de instalación, la instalación en modo Server Core es muy específica e introduce las limitaciones siguientes:

- Sólo se soporta una instalación "nueva". Esto significa que no se puede realizar una actualización a partir de una versión anterior.
- Como ocurría con Windows Server 2012 R2, el administrador tiene la posibilidad de pasar de una versión estándar a una versión Core.
- Observe que no es posible realizar una actualización de Windows Server 2012 o 2012 R2 en modo Core a Windows Server 2016 en modo Core. En este caso, tendremos que efectuar por necesidad una nueva instalación de Windows.

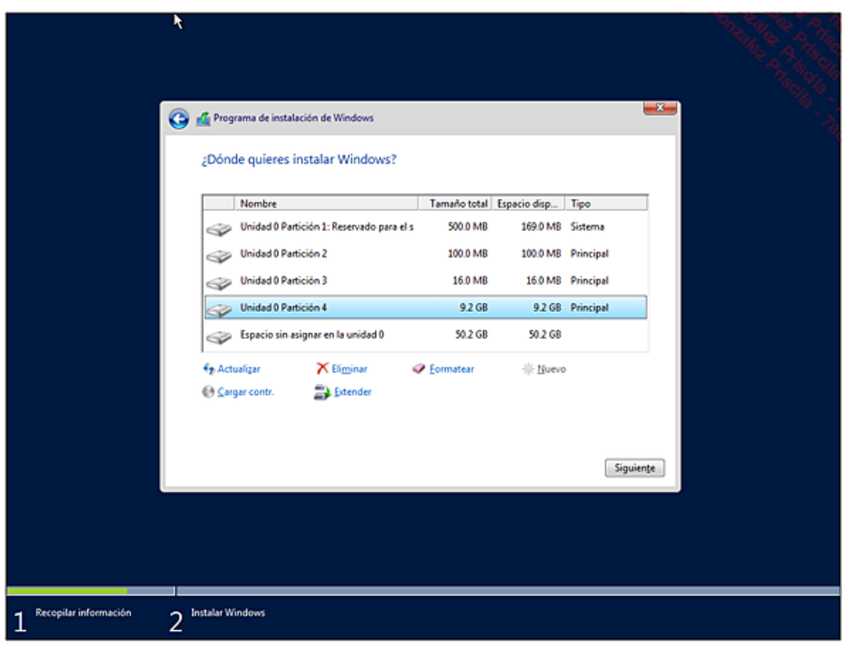
c. Server Core y roles de Windows Server 2016

La instalación en modo Server Core de Windows Server 2016 se selecciona en el momento de la instalación y permite instalar un entorno de producción mínimo. Como hemos visto antes, este tipo de instalación proporciona como punto principal la ventaja de fortalecer la seguridad y reducir las tareas de mantenimiento y gestión.

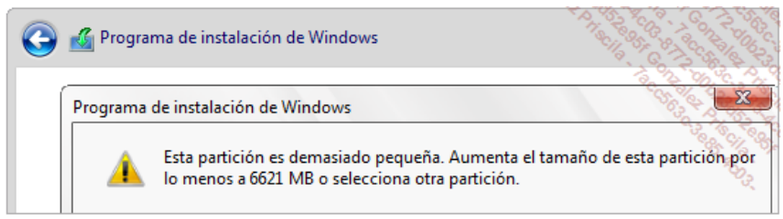
d. Instalación de Windows Server 2016 en modo Server Core



Instalación de Windows Server 2016 por defecto en modo Server Core o instalación con la interfaz gráfica (Desktop Experience)



Partición de 10240 MB (10 GB) y particiones adicionales creadas de forma automática por el asistente (Partición de recuperación, partición del sistema y partición Microsoft reservada - MSR)

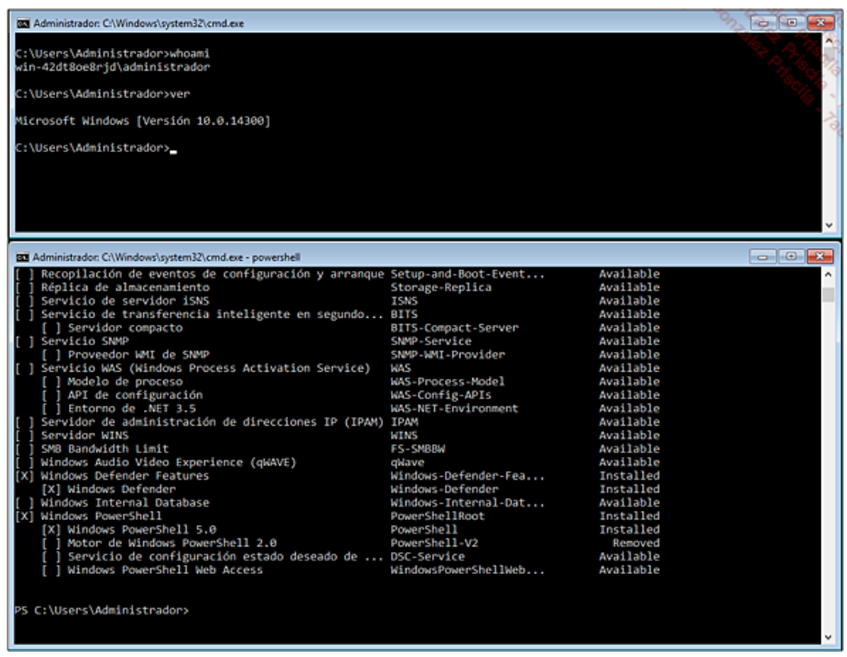


Espacio mínimo para una instalación en modo Core

Para realizar una instalación en modo Server Core, la partición de Instalación mínima debe contar con un espacio igual o superior a unos 7 GB. Para este tipo de configuración, se recomienda un tamaño mínimo de entorno a 10 GB.

Al término de la instalación, el servidor se reinicia y en el primer inicio de sesión debemos cambiar la contraseña del administrador. Una vez efectuada esta operación, el intérprete de comandos cmd.exe se pone en marcha.

La imagen siguiente muestra con la ejecución del comando Windows PowerShell Get-WindowsFeature los diferentes roles y características, así como los componentes instalables con su estado, instalado o no instalado.

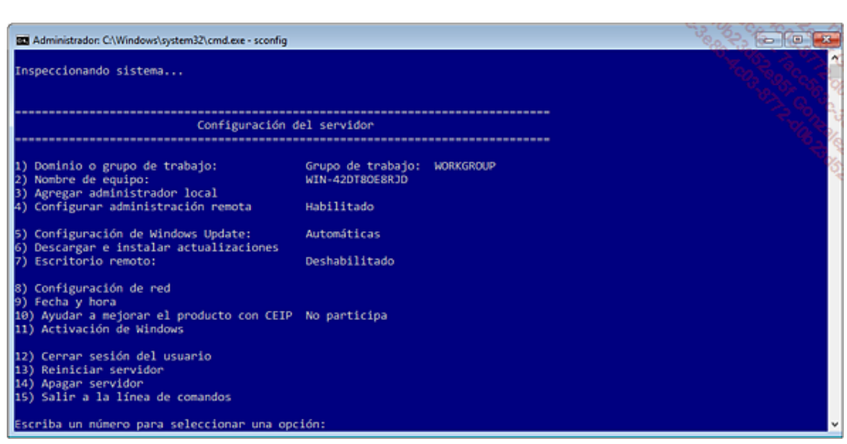


Roles y características instaladas y disponibles en modo Server Core

Como ocurría con Windows Server 2012 R2, Windows Server 2016 podrá ser configurado empleando el comando SCONFIG. Podremos en pocos minutos configurar la totalidad de los parámetros básicos de una instalación de Windows Server 2016 en el modo Core. El comando SCONFIG permite gestionar los parámetros listados a continuación:

- cambio de nombre del equipo;
- integración al dominio de Active Directory;
- configuración de la administración remota y el firewall;
- configuración de Windows Update;
- configuración del escritorio remoto;
- configuración de las capas de red (IP estática o dinámica, mismas tarjetas...)

Para utilizar esta herramienta, teclee SCONFIG en el intérprete de comandos y utilice las instrucciones mostradas.

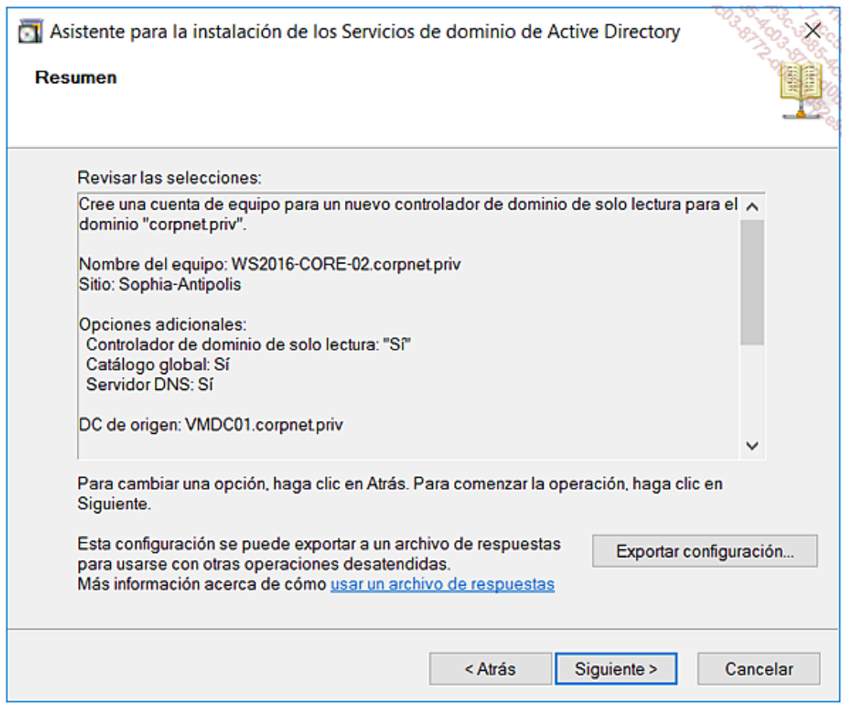


Configuración del servidor con la herramienta sconfig

e. Instalación del rol de controlador de dominio AD DS en modo Server Core

En esta etapa de la configuración, el servidor está listo para añadir el rol de controlador de dominio, o cualquier otro rol soportado. La instalación del rol de controlador de dominio no podrá efectuarse con el asistente de instalación de Active Directory ofrecido por el administrador del servidor. El procedimiento debe basarse en la utilización de un archivo de comandos de Windows. El archivo script puede ser utilizado para instalar el rol de controlador de dominio Active Directory, y también eliminarlo, en caso de necesidad. Tenga en cuenta que al final de la instalación automática (en modo Server Core), el asistente efectuará un reinicio de forma automática.

Tenemos la posibilidad de utilizar el asistente de instalación de Active Directory en modo gráfico en un equipo Windows Server 2016 y utilizar el asistente para guardar un archivo unattend para su utilización en el servidor instalado en modo Server Core.



Export de los parámetros en un archivo de respuestas

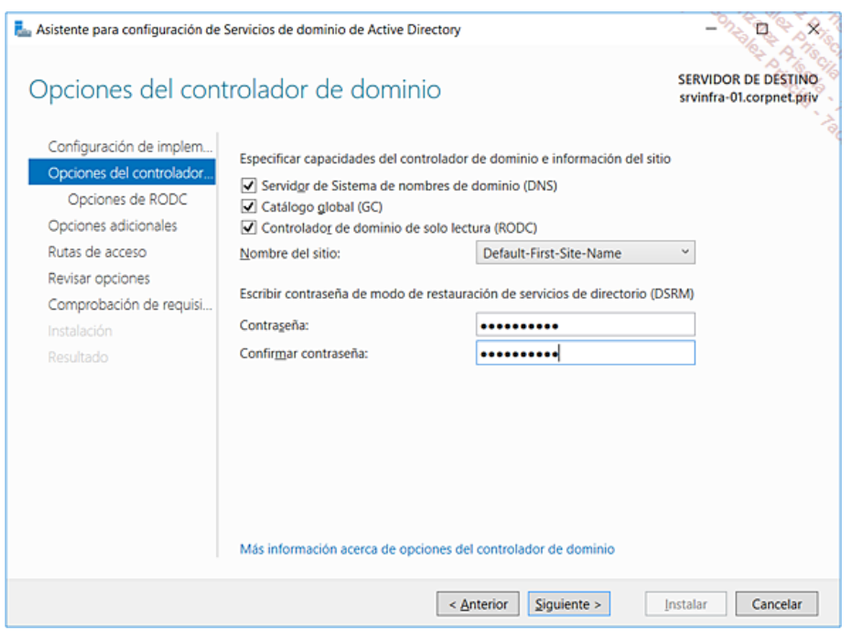
Borrado automático de contraseña: el archivo de respuesta contiene la contraseña del administrador del dominio necesaria para la aplicación del nuevo controlador de dominio. Con el fin de preservar la seguridad de la cuenta utilizada para la operación de promoción, una vez utilizado el archivo de respuestas por DCpromo, la contraseña será borrada de forma automática. Por lo tanto, si necesitamos utilizar de nuevo dicho archivo, tendremos que modificarlo para incluir de nuevo la contraseña.

f. Instalación de un controlador RODC en modo Server Core

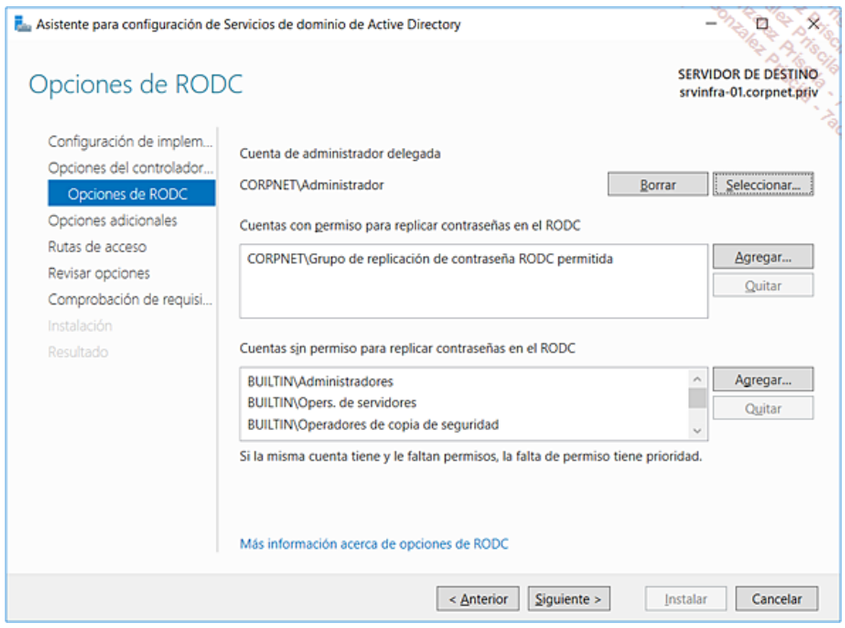
El archivo generado a continuación permite instalar un nuevo controlador de dominio de tipo RODC (*Read Only Domain Controller*) dentro de un dominio llamado corpnet.priv. El parámetro ReplicaOrNewDomain permite crear un nuevo dominio, un nuevo controlador de dominio dentro de un dominio existente o el nuevo rol de controlador de dominio en solo lectura, RODC. En nuestra configuración, el controlador corresponderá al dominio Active Directory corpnet.priv y tendrá también el rol de servidor DNS y de Catálogo Global en el sitio Active Directory de Default-First-Site-Name. La cuenta de dominio utilizada para realizar la promoción es la cuenta administrador en el dominio corpnet.priv, sin que la contraseña de este administrador esté registrada en el archivo, mientras que la contraseña de la cuenta de reparación de emergencia (arranque e inicio de sesión en modo DSRM) será también definida.

La primera etapa consiste en generar el archivo Windows PowerShell que permitirá realizar las distintas operaciones. Para lograrlo, podemos crearlo desde cero o, por ejemplo, utilizar el administrador de servidor de Windows Server 2016 a partir de un servidor ya instalado en el modo de Experiencia de Usuario.

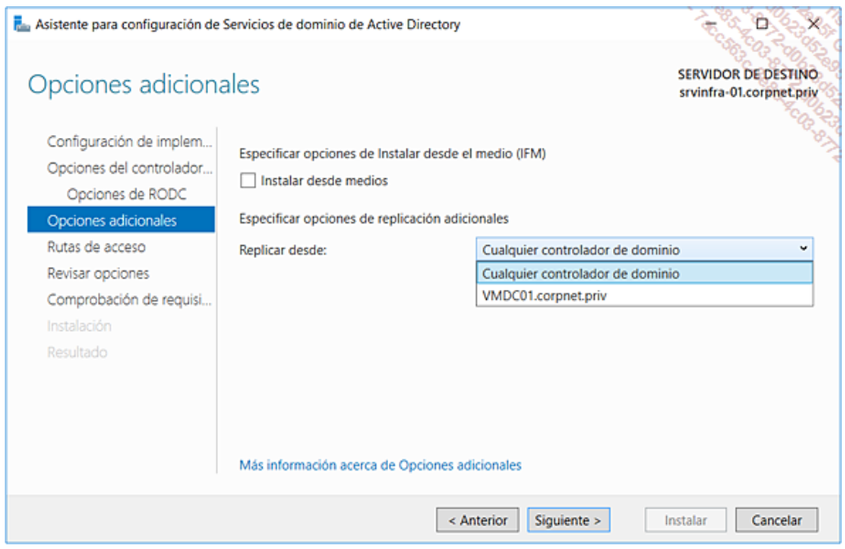
Archivo de comandos Windows PowerShell: para más información acerca de la creación de un archivo de respuestas para desplegar un controlador de dominio empleando Windows PowerShell, busque en el sitio Microsoft Technet en la dirección:https://technet.microsoft.com « Install a Windows Server 2016 Active Directory Read-Only Domain Controller » o utilice el siguiente enlace:https://technet.microsoft.com/en-us/library/jj574152.aspx



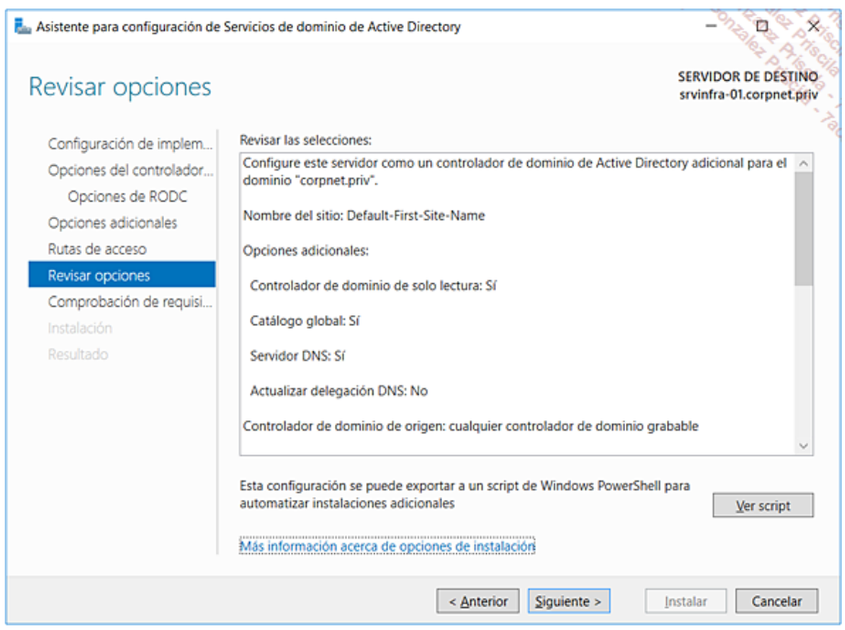
Agregar un nuevo controlador de tipo RODC



Configuración de las opciones de un nuevo RODC



Opciones adicionales: selección del controlador de dominio fuente



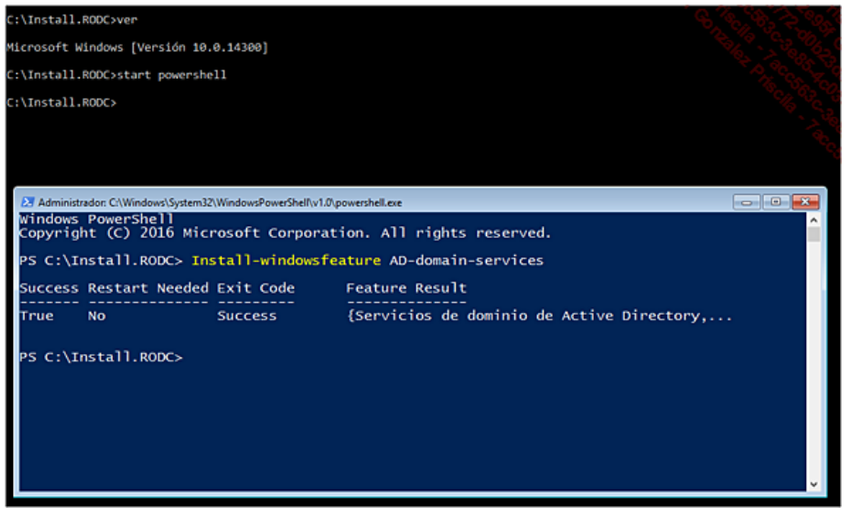
Verificación de las selecciones con el arranque de la instalación, o export del script PowerShell para su uso en otro servidor Windows Server 2016

```
#

# Script de Windows PowerShell para implementación de AD DS

#



Import-Module ADDSDeployment

Install-ADDSDomainController `
```

```
-AllowPasswordReplicationAccountName @("CORPNET\Grupo de replicación
de contraseña RODC permitida") `

-NoGlobalCatalog:$false `
-Credential (Get-Credential) `

-CriticalReplicationOnly:$false `

-DatabasePath "C:\Windows\NTDS" `

-DelegatedAdministratorAccountName "CORPNET\Administrador" `

-DenyPasswordReplicationAccountName @("BUILTIN\Administradores",
"BUILTIN\Opers. de servidores", "BUILTIN\Operadores de copia
de seguridad", "BUILTIN\Opers. de cuentas", "CORPNET\Grupo
de replicación de contraseña RODC denegada") `

-DomainName "corpnet.priv" `

-InstallDns:$true `

-LogPath "C:\Windows\NTDS" `

-NoRebootOnCompletion:$false `

-ReadOnlyReplica:$true `

-SiteName "Default-First-Site-Name" `

-SysvolPath "C:\Windows\SYSVOL" `

-Force:$true
```

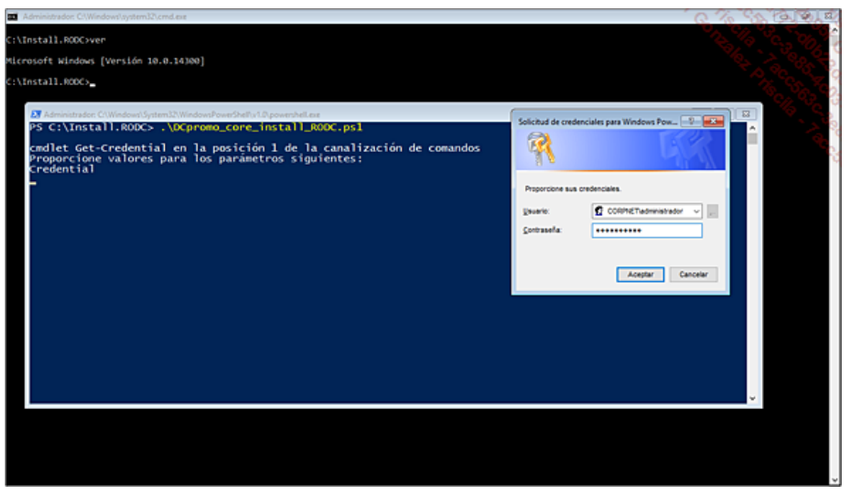
Observación importante: como hemos visto antes al promover un servidor a Controlador de dominio, cada vez que un archivo Unattend se utiliza, las contraseñas incluidas son eliminadas. Recuerde modificar el archivo para añadir las contraseñas a emplear en caso de reutilizarlo.

La imagen siguiente ilustra la etapa que consiste en agregar el rol AD DS a la instalación antes realizada en modo Core.

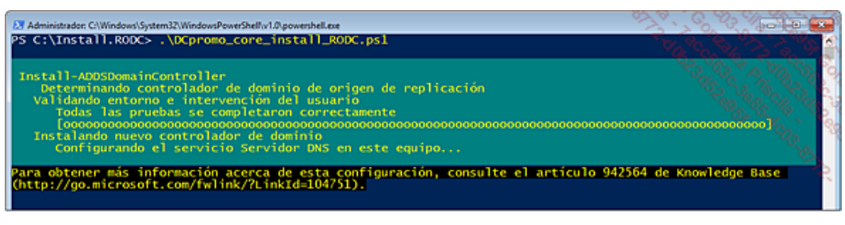


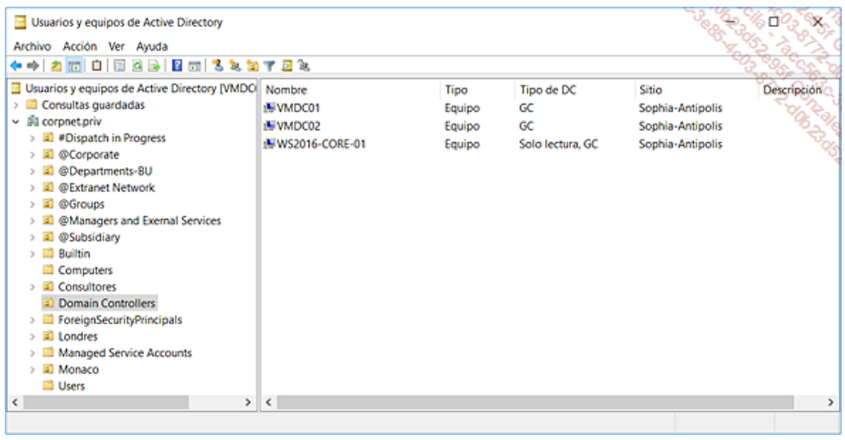
Autenticación durante la instalación de un servidor RODC en modo Server Core.

Una vez instalados los archivos binarios de los servicios de dominio Active Directory, el proceso de instalación automático del nuevo controlador de dominio RODC puede arrancar. Para lograrlo, solo falta ejecutar el archivo de script Windows PowerShell creado de forma previa y autenticarse en el dominio que incluirá el nuevo controlador de dominio de solo lectura.



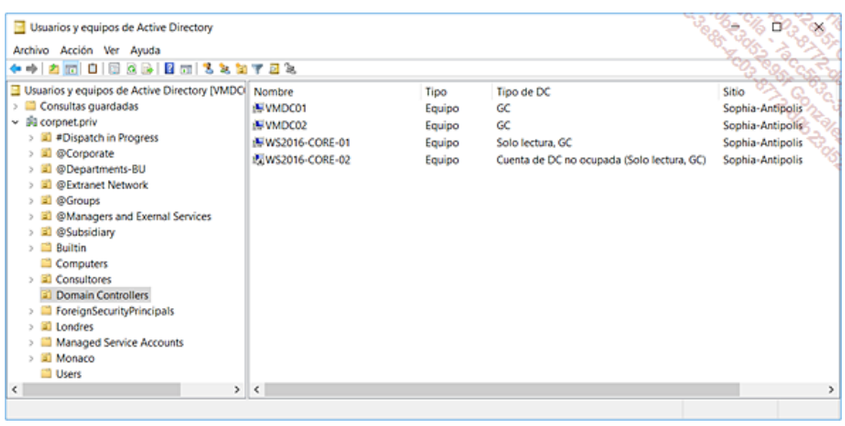
Ejecución del script Windows PowerShell





Fin de la instalación y estado del nuevo RODC WS2016-CORE-01

En este punto, el nuevo controlador de dominio RODC funcionando en Windows Server 2016 en modo Core está operativo.



La imagen anterior muestra los controladores de dominio del dominio corpnet.priv Observe que el servidor WS2016-CORE-01 está visto como "Cuenta de DC en solo lectura", mientras que el servidor WS2016-CORE-02 está declarado como "Cuenta de DC no ocupada (sólo lectura, DC)". En este ejemplo, este estado es normal porque -en este punto, el segundo controlador de dominio RODC ha sido pre-creado pero todavía no está instalado.

En este ejemplo, hemos instalado y configurado los parámetros generales de un servidor Windows Server 2016 en modo Server Core. Ahora crearemos el archivo Unattend para su utilización mediante Windows PowerShell para añadir dentro del dominio Active Directory una nueva réplica de tipo RODC con el rol de servidor DNS y Catálogo global. La continuación del capítulo detalla el nuevo rol de controlador de dominio en modo solo lectura.

3. Rol de controlador de dominio en modo solo lectura

Se trata de un nuevo tipo de controlador de dominio que permite a las empresas que requieren desplegar controladores en ubicaciones no seguras hacerlo limitando su exposición. El principio de un controlador de dominio en modo solo lectura (RODC de *Read Only Domain Controller*) consiste en marcar las particiones Active Directory (NC, *Naming contexts*) en modo solo lectura. Veremos más adelante que esta modificación entraña muchos cambios.

Recordemos que las particiones de tipo Global Catalog funcionan ya bajo este principio. En efecto un controlador de dominio de tipo catálogo global en un dominio dado posee una copia de solo lectura de todas las particiones de los dominios miembros del bosque. Este tipo de partición se conoce como Read Only PAS, de Partial Replica Set. Es por principio imposible modificar el contenido de forma directa.

El funcionamiento de un controlador de tipo RODC es un poco diferente. En efecto, cuando el controlador recibe una operación de escritura LDAP, entonces recibirá una referencia de un controlador disponible para su escritura. La operación de escritura dirigida al RODC es solo redirigida. Una vez efectuada la operación de escritura en el controlador remoto disponible para escritura, tendrá lugar una replicación unidireccional en el controlador RODC. Este enfoque garantiza que no se pueda producir ninguna corrupción del Active Directory en la ubicación donde reside el RODC. Así, toda la infraestructura está protegida. Por último, es un poco como con la replicación de los antiguos controladores de dominio Windows NT, donde el controlador de dominio principal del dominio, el PDC de *Primary Domain Controller*, ¡era al centro de la infraestructura!

Es muy recomendable usar servidores RODC para prestar servicios de infraestructura en sitios remotos difíciles de proteger (lugares públicos, universidades, etc.). Esto puede ser también el caso de aplicaciones de terceros instaladas de forma local en el controlador de dominio cuando estas aplicaciones se administran utilizando una sesión de terminal. El empleo del modo RODC, asegura los datos de Active Directory del Contralor local y minimiza los riesgos de seguridad en el conjunto del bosque.

Este principio garantiza que ni la base de datos Active Directory, ni los objetos que se almacenan, pueden ser modificados en local de forma directa.

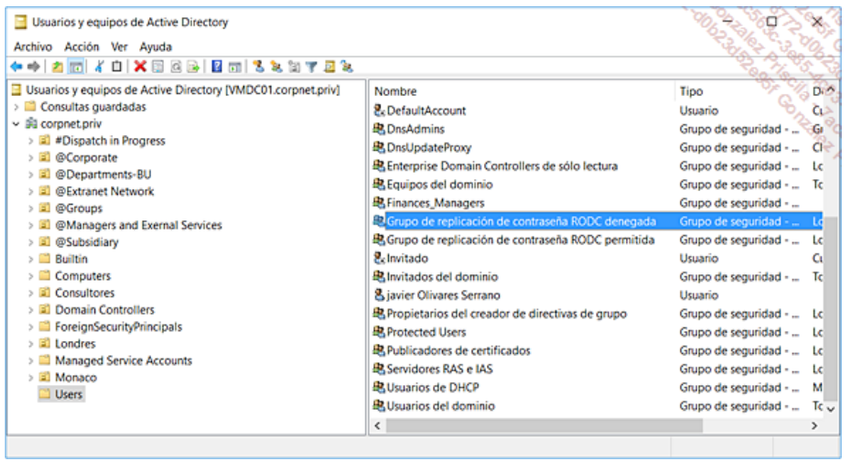
a. Securización de las contraseñas en los controladores RODC

La securización de las contraseñas depende de la directiva de replicación de las contraseñas de los controladores de tipo RODC. Los controladores de dominio Windows Server 2016 -así como las versiones anteriores como Windows Server 2012 R2 o 2008 R2, que funcionan en modo RODC, disponen de un mecanismo de gestión de contraseñas de usuarios y equipos muy específico. La idea es lograr que en caso de robo de un controlador de dominio RODC remoto, no exista en el equipo ninguna contraseña de cuentas "críticas" que pueda ser descifrada. Este método radical garantiza que será imposible lanzar, incluso sustrayendo el equipo de forma física, un ataque de fuerza bruta contra la base de datos Active Directory.

¡Observe! Como ocurre con los controladores de dominio que utilizan versiones anteriores de Windows Server, es necesario que los controladores de dominio de solo lectura puedan ponerse en contacto con un servidor maestro de operaciones que ostente el rol PDC Emulator con la misma versión de Windows Server. Así, con respecto a los controladores de dominio RODC Windows Server 2016, el maestro FSMO PDC Emulator también debería utilizar Windows Server 2016.

En la práctica, el controlador de dominio RODC del sitio transmitirá la consulta de autenticación de un puesto cliente a un controlador de

dominio disponible en lectura y escritura que funcione a su vez con Windows Server 2016. Una vez autenticado el usuario, el Contralor RODC solicita que se le envíe una copia de la información de seguridad del usuario. El controlador de dominio disponible en escritura reconoce que la consulta es iniciada por un RODC y, en este caso, consulta la RODC Password Replication Policy. Ésta determinará si la información de seguridad puede ser replicadas al contralor RODC -o bien sólo en caché de memoria.



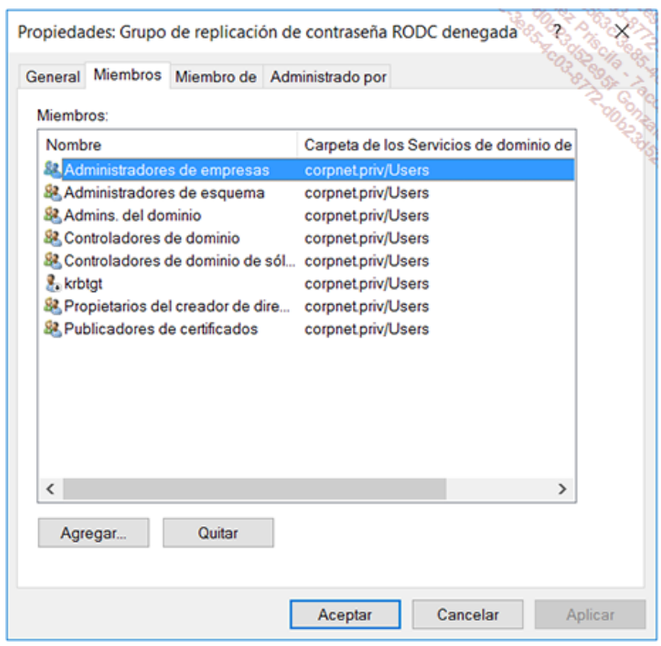
Directiva de replicación en la cual se denegará la contraseña RODC

Queda a discreción del administrador definir una directiva de replicación de las contraseñas sabiendo que, por defecto, ninguna contraseña de usuario o de equipo se almacena en el RODC.

Microsoft recomienda mantener la directiva por defecto (RODC Password Replication policy) para preservar la seguridad de las cuentas de usuarios y de equipos en estos controladores. Conviene verificar que el tráfico de red de las consultas de autenticación transmitidas hacia un controlador Windows Server 2016 disponible en escritura son aceptables.

Controladores RODC y almacenamiento de contraseñas… A excepción de todas las contraseñas, la base de datos Active Directory de un controlador de tipo RODC contiene la totalidad de los objetos de las diferentes particiones del directorio. Los únicas contraseñas almacenadas por defecto son aquellos asociados a la cuenta del equipo mismo, así como la de la cuenta krbtgt específica del controlador de tipo RODC.

Como podemos constatar, dos grupos de dominio local son creados de forma automática durante la actualización del esquema, sabiendo que el grupo que autoriza la reproducción de las contraseñas es nulo y que el grupo niega de forma explícita la replicación de contraseñas que contengan los miembros de los grupos más importantes, como los Administradores de empresas, Administradores del esquema, los Admins. del dominio, los controladores de dominio RW y RODC, así como los miembros de los grupos editores de certificados y propietarios de creadores de la directiva de grupo.



Cuentas críticas cuyas contraseñas no se replican en los RODC

b. Replicación de las contraseñas en los controladores RODC

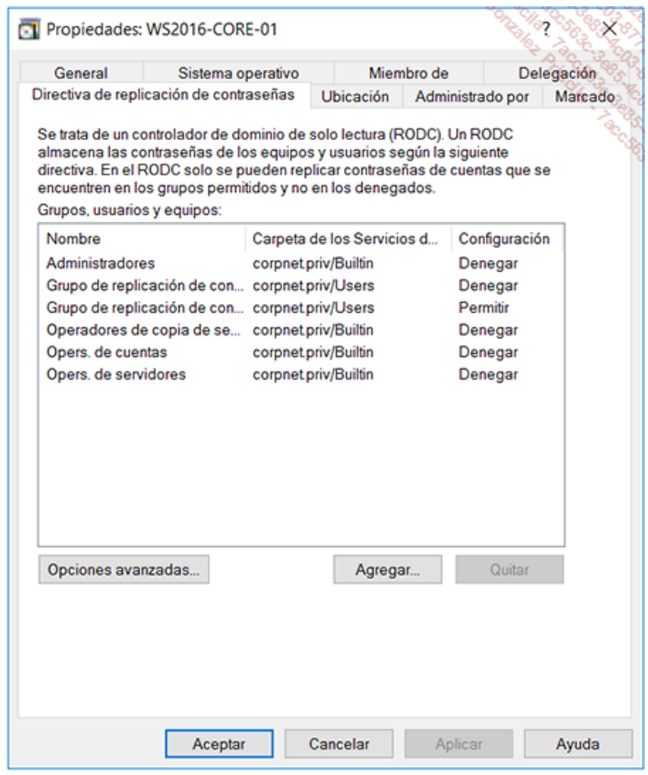
La securización de las contraseñas depende pues de la directiva de replicación de las contraseñas definida en los objetos de tipo controladores RODC.

Para implementar este funcionamiento, los controladores de dominio de tipo RODC utilizan un mecanismo que permite poner en caché los secretos LSA utilizados para la autenticación de usuarios y equipos. Este atributo, insertado en el esquema durante su actualización se llama RO PAS - *Read Only Partial Attribute Set*. Soporta los secretos de usuarios y equipos mediante el soporte de los condensados de contraseñas, y también otros datos sensibles tales como clave de recuperación BitLocker.

Aunque los valores definidos por Microsoft convienen a la mayoría de las implementaciones, es interesante señalar que es posible modificar la lista de atributos no replicados modificando el contenido del Partial Attribute Set.

Por defecto, la base local de un contralor RODC contiene solamente dos condensados de contraseñas: el condensado de la contraseña de cuenta de administrador local de la máquina y el de la cuenta máquina. Luego, en función de la directiva de replicación de las contraseñas, otros condensados pueden almacenarse durante un período configurable cuando la autenticación haya sido realizada con éxito.

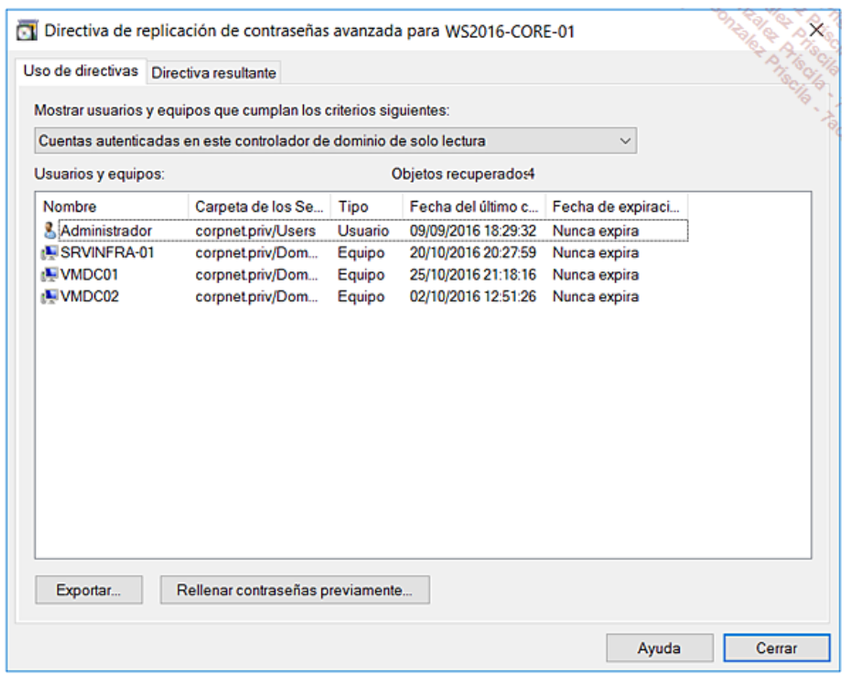
La política definida permite, gracias a la pertenencia a los dos grupos de seguridad vistos antes, controlar cuáles son los usuarios para que la puesta en caché y la replicación sean posibles y cuáles son aquellos para los que la replicación está prohibida.



Directiva de replicación de contraseñas sobre los objetos grupos, usuarios y equipos en los modos de Permitir o Denegar

Así, cuando un usuario es autenticado a través de un RODC, la pertenencia a estos dos grupos se verificará, sabiendo que la pertenencia al grupo donde la replicación de las contraseñas es denegada se tendrá en cuenta de manera prioritaria. De esta forma se soporta la caché en caso de conflicto.

Los dos atributos Active Directory utilizados para implementar esta política son msDS-Reveal-OnDemandGroup y msDS-NeverRevealedList. El primero es un parámetro global que permite la replicación de la contraseña, mientras que el segundo, siempre prioritario, es un parámetro orientado de forma específica para cada controlador RODC y para cada identidad.



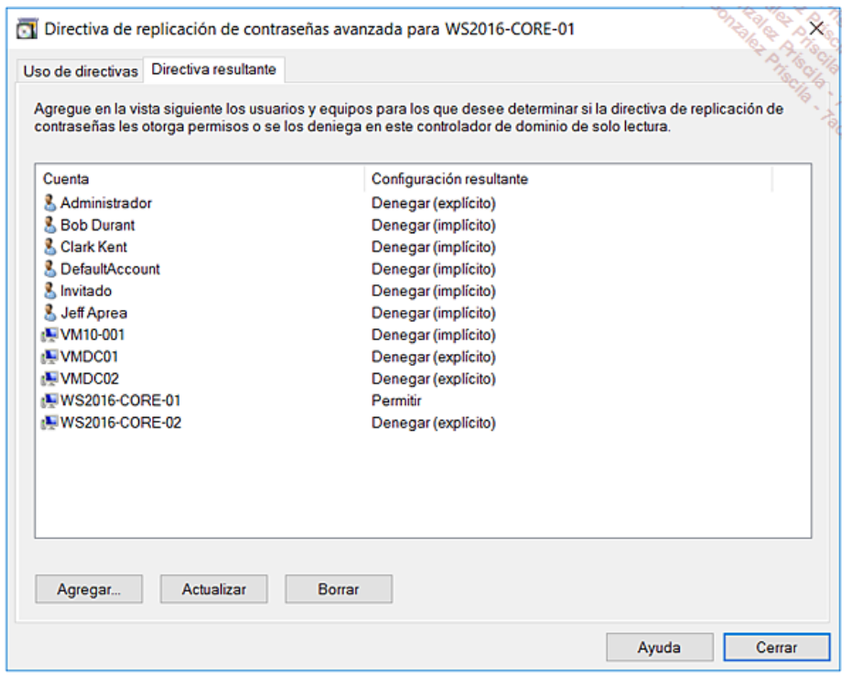
Cuentas autenticadas y en caché, pero no replicadas

Observe que la consola de gestión MMC Usuarios y equipos de Active Directory de Windows Server 2016 permite ver todas las propiedades de los nuevos tipos de controladores de dominio en modo sólo lectura.

El botón **Opciones avanzadas...**, disponible en la pestaña **Directiva de replicación de contraseñas** de un objeto controlador de dominio en modo sólo lectura, nos permite consultar en tiempo real la lista de cuentas ya autenticadas en el controlador de dominio seleccionado.

Así, la interfaz ofrece la posibilidad de mostrar los usuarios y equipos que responden a criterios importantes correspondientes a las cuentas de las contraseñas almacenadas físicamente en este controlador de dominio en modo sólo lectura o bien solo las cuentas autenticadas y en caché del mencionado controlador de dominio de solo lectura

¡Observe! Debemos revisar de forma periódica las cuentas que hayan sido autenticadas en un controlador de dominio en modo sólo lectura (RODC). Esta información puede ayudarle a planificar la evolución de la directiva de replicación de contraseñas existente. Por ejemplo, comprobar las cuentas de usuarios y equipos ya autenticados en un controlador de dominio en modo sólo lectura (RODC) para rellenar de forma previa la cache de contraseñas con dichas cuentas.



Control de cuentas autorizados o denegadas para replicar su contraseña en el controlador de dominio en modo sólo lectura empleando la función de "Directiva resultante"

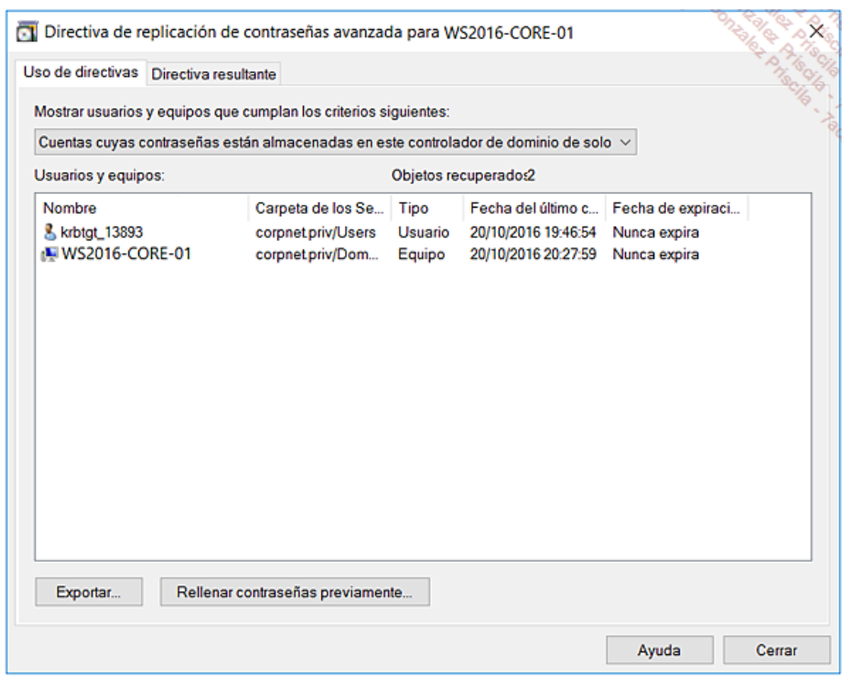
Por último, la ventana anterior pone de manifiesto que es fácil "consultar" al controlador de dominio en modo sólo lectura tal o cual cuenta de usuario o equipo disponen de información de contraseñas en la actualidad en caché en el controlador.

Por ejemplo, las cuentas de tipo administrador Bob Durand y Jean-Francois Aprea están rechazadas de forma explícita en la replicación de este controlador de dominio de solo lectura única, al ser miembros del grupo de los Admins. del dominio, este grupo forma parte él mismo del grupo denegado de forma explícita para la replicación de las contraseñas en todos los controladores en modo sólo lectura del dominio.

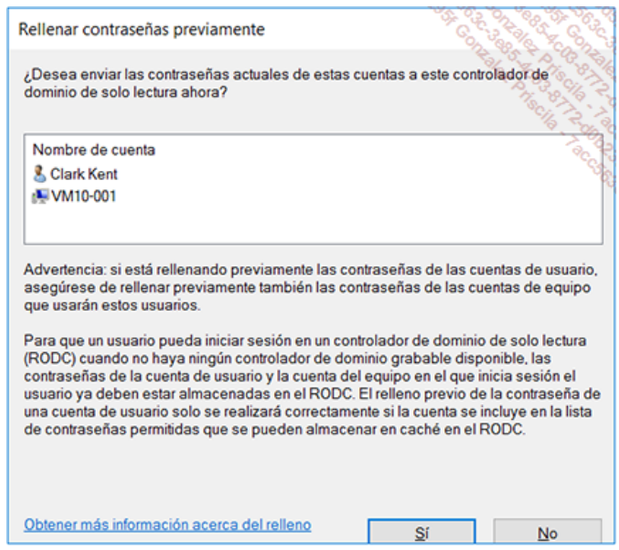
c. Llenado previo de las contraseñas en un controlador de sólo lectura

La interfaz de administración de los controladores de dominio de solo lectura también permiten rellenar la caché para los usuarios y/o equipos para los que se autoriza la replicación de las contraseñas y no haya sido de forma explicita prohibida.

Esta operación, realizada empleando el botón **Rellenar contraseñas previamente**, permite al administrador rellenar las contraseñas que se consideran como esenciales en caso de problema de contacto entre el controlador RODC y un controlador fuente disponible en lectura y escritura -que, recordemos debe funcionar con la misma versión de Windows, es decir, en nuestro caso Windows Server 2016.

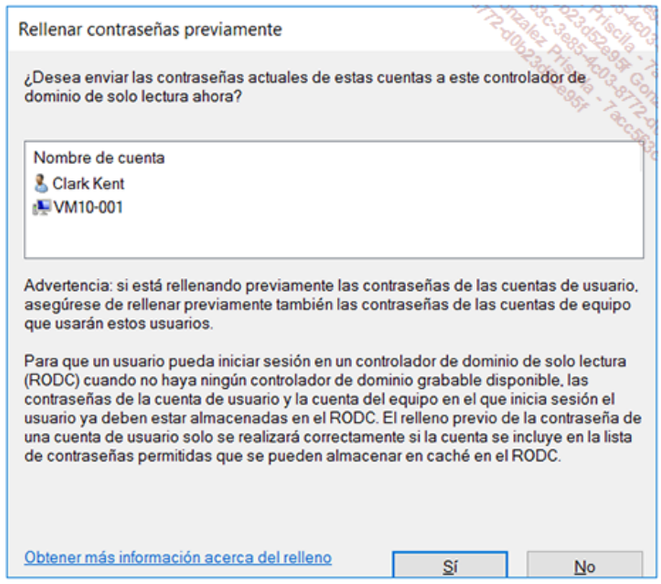


Operación de llenado previo de cache de contraseñas.

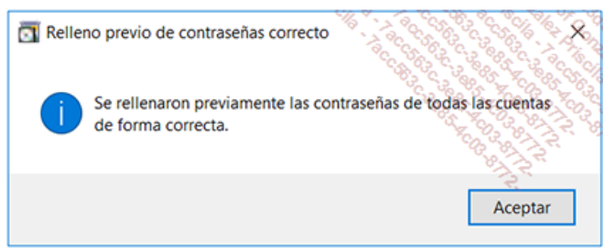


Selección de las cuentas de usuarios y equipos a replicar en el equipo RODC

La operación de llenado previo es muy simple de realizar: hacemos clic en **Rellenar contraseñas previamente** y seleccionamos las cuentas deseadas. Serán replicadas y almacenadas en el controlador de dominio en modo sólo lectura (RODC) de forma automática.



Añadir las cuentas seleccionados de forma previa

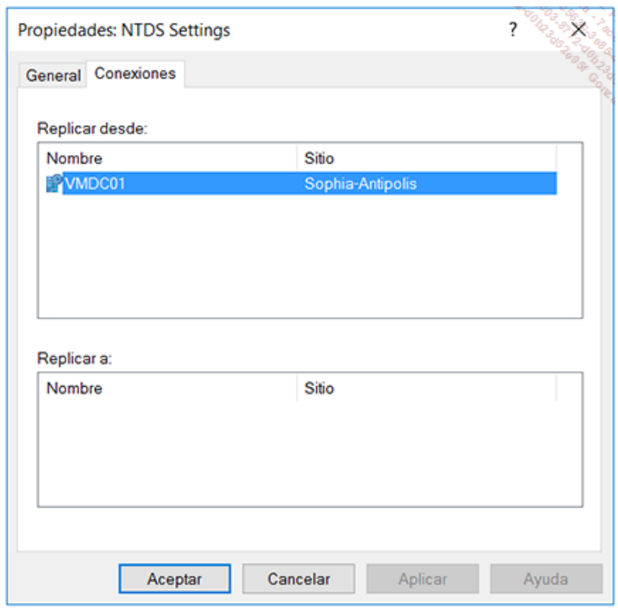


Operación de llenado previo de contraseñas exitosa

¡Observe! Conviene recordar replicar las contraseñas de los equipos y los usuarios. En efecto, si la cuenta del equipo debe ser utilizada para autenticar el equipo cliente en el contralor local, o incluso en otro servidor, será necesario contactar con un controlador de dominio RW en otro sitio Windows Server 2016. Si este controlador no puede localizarse, entonces la autenticación solo podrá llevarse a cabo con éxito si la cuenta de equipo, y la contraseña asociada, ya está incluida en la caché, o mejor, grabada de forma previa de forma proactiva.

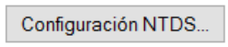
d. Condiciones requeridas para desplegar un controlador en modo sólo lectura (RODC) y limitaciones

Para desplegar un servidor Windows Server 2016 que desempeña el rol RODC, el rol FSMO de tipo PDC Emulator debe ser mantenido por un controlador que funcione a su vez con Windows Server 2016. También habrá que asegurarse que el nivel funcional del dominio es, como mínimo, de tipo Windows Server 2008, sabiendo que se recomienda por supuesto una versión posterior de Windows Server. El funcionamiento del controlador RODC es muy habitual, ya que la replicación unidireccional del servidor RODC se aplica a nivel AD DS y también a nivel de la replicación de SYSVOL empleando DFS-R, punto esencial para que el contralor incluya los objetos de directivas de grupo.



Replicación unidireccional desde un controlador disponible en lectura y escritura funcionando con Windows Server 2016

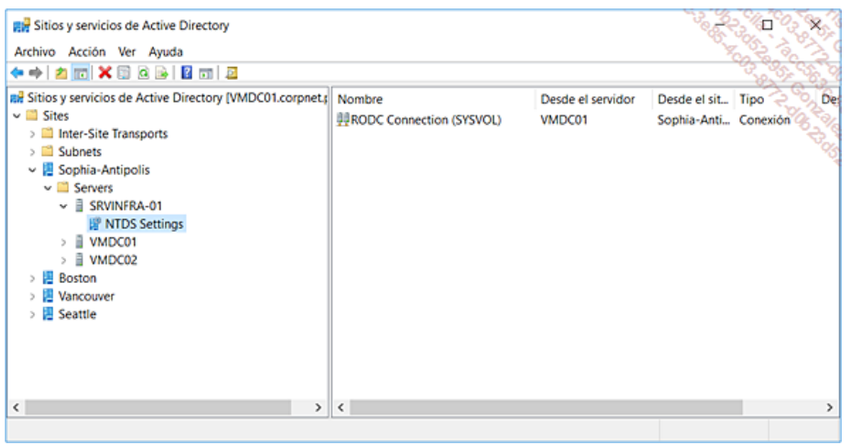
La imagen anterior se obtiene al acceder a las propiedades del objeto servidor en la consola de administración MMC Usuarios y equipos de Active Directory. Esta ofrece una vista de resumen de las conexiones de Active Directory que puedan existir entre varios controladores de dominio.



Nuevo acceso a la configuración NTDS vía la consola Usuarios y equipos de Active Directory de Windows Server 2008 y Windows Server 2008 R2.

Por último, cabe señalar que por razones obvias en relación con la seguridad de la infraestructura de Active Directory, un controlador de dominio de tipo RODC no podrá desempeñar ningún rol FSMO (*Flexible Simple Master Operations*). Ocurrirá lo mismo para el rol de servidor cabeza de puente dentro de la topología de replicación de Active Directory (servidor BHS, Bridgehead Server).

La figura siguiente muestra que empleando la consola de administración MMC Sitios y servicios de Active Directory, el objeto conexión se llamará RODC Connection (SYSVOL), que significa este también será utilizado para la replicación del volumen SYSVOL en el sentido "controlador de dominio RW hacia un controlador de dominio RODC".



Objeto Conexión de tipo RODC - SYSVOL

Como se muestra arriba, el controlador de dominio en solo lectura SRVINFRA-01 solo acepta la replicación de datos Active Directory desde el controlador de dominio VMDC01. Los controladores de dominio RODC Windows Server 2016 solo aceptan las replicaciones entrantes. No existe ninguna replicación saliente desde un controlador de dominio RODC hacia otro Controlador de la empresa.

4. ¿Por qué y cómo evolucionar hacia el nivel funcional de dominio Windows Server 2016?

Desde hace varios años, los servicios de dominio Active Directory suelen estar operativos en el nivel funcional Windows 2003 o con mayor frecuencia hoy en día en Windows Server 2012 o 2012 R2.

Hoy los servicios de dominios AD DS de Windows Server 2016 no aportan funcionalidades adicionales a los niveles funcionales de dominio y de bosque ya conocidos con Windows Server 2012 R2. Estos últimos años, la evolución más destacable concierne a los niveles funcionales de dominio y bosque de Windows Server 2008. Conviene recordar cuáles son los valores añadidos aportados por estos modos "2008".

En efecto, el nivel funcional de dominio Windows Server 2008 permite conservar todas las funcionalidades aportadas por los modos anteriores y añadir el soporte de funcionalidades siguientes:

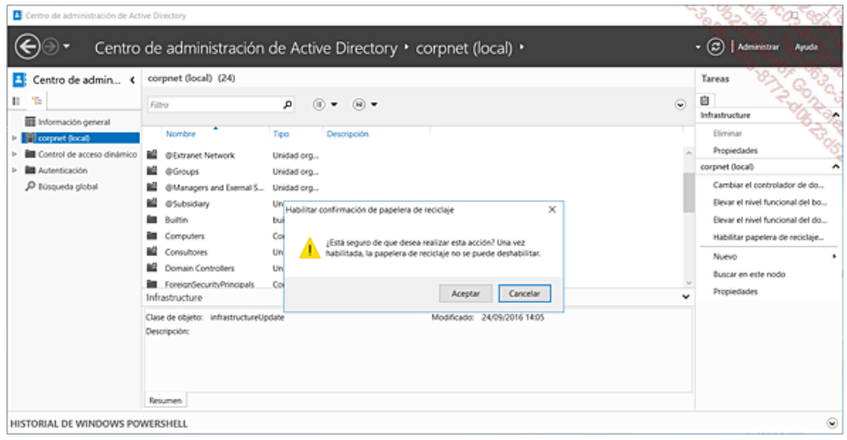
- La replicación del volumen de sistema SYSVOL se soporta mediante la replicación DFS-R. El Servicio de replicación DFS-R es sin duda más eficaz y robusto que el anterior motor NTFRS. Este punto interesará en particular a los directores que deben gestionar un gran número de directivas de grupo o también que se enfrentan a un bajo rendimiento de la replicación NTFRS.
- El protocolo Kerberos v5 soporta los algoritmos AES 128 y AES 256 - *Advanced Encryption Standard*.
- El soporte de información del último Inicio de sesión interactiva. Los registros de seguridad que contendrán los datos importantes como la hora del último inicio de sesión interactiva ejecutado con éxito.
- El nombre del puesto de trabajo desde el cual el usuario inició la sesión.
- El número de inicio de sesiones rechazadas desde el último Inicio de sesión efectuado con éxito.
- Las directivas de contraseña granulares. Estas nuevas directivas de contraseña permiten a los administradores especificar las directivas de contraseña y bloqueo de cuenta al nivel de los usuarios y grupos globales de seguridad dentro del dominio Active Directory que funcionan en el nivel funcional en Windows Server 2008 o posterior.

Para más información sobre las nuevas directivas de cuentas granulares de Windows Server 2008, podemos consultar el documento "step-by-step Guide for Fine-Grained Password and Account Lockout Policy Configuration" disponible para su descarga en el sitio de Microsoft en la dirección: http://go.microsoft.com/fwlink/?LinkID=91477

Ahora que las empresas tratan de alcanzar un mayor nivel de seguridad, cabe señalar que las diferentes herramientas de administración de Windows Server prohíben aumentar el nivel funcional cuando no se cumplen todas las condiciones.

En relación a los bosques Windows Server 2008, 2012, 2012 R2 y 2016: estos bosques Windows Server soportan todas las funcionalidades de las versiones posteriores y ninguna otra funcionalidad específica. El hecho de que un bosque determinado sea objeto de una elevación del nivel funcional a un nivel superior tal como Windows Server 2016 se asegurará de que cualquier nuevo dominio será operativo de forma automática en el nivel funcional de Windows Server 2016.

Con respecto a los bosques Windows Server 2008 R2: se trata del único nivel funcional de bosque que aporta una nueva funcionalidad muy apreciada por los administradores de Active Directory. En efecto, este nivel y los niveles posteriores, permiten la activación de la Papelera Acitve Directory disponible en la consola Centro de administración de Active Directory.

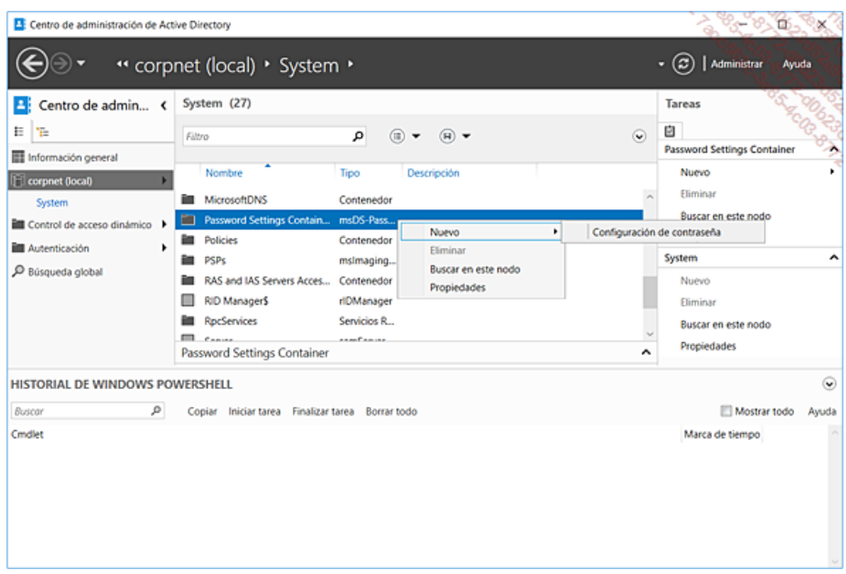


Activación de la Papelera de Active Directory empleando el Centro de administración de Active Directory

5. Administración de directivas de contraseñas granulares

Se trata de una pequeña revolución, ¡introducida una vez más por Windows Server 2008! En efecto, esta versión de Windows Server hace posible la declaración dentro del mismo dominio de diferentes directivas de gestión y bloqueo de contraseñas. Recordemos que esta operación nunca ha sido posible, ni en el caso de los dominios LAN Manager con UNIX o con OS/2, ni con los dominio Windows NT o Active Directory -antes de esta versión de Windows Server 2008. Las únicas soluciones para evitar esta limitación histórica consistían en poner en práctica uno o varios dominios Active Directory adicionales o bien desarrollar una DLL de filtrado de contraseñas, tal como se especifica en el SDK de Active Directory. Por supuesto, estas dos soluciones crean limitaciones, tanto en términos de arquitectura como en términos de sobrecarga de administración.

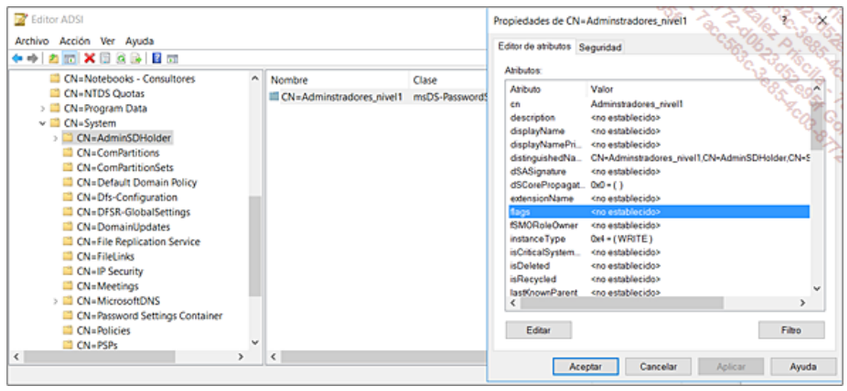
La aplicación de directivas de contraseñas granuladas dentro de un mismo dominio Active Directory emplea la nueva clase de objeto PSO - *Password Settings Object*. El Administrador podrá luego crear nuevas directivas de contraseña granulares y destinarlas a los diferentes grupos de usuarios y/o usuarios que deban estar sujetos a restricciones de Gestión de contraseñas empleando la consola Centro de administración de Active Directory de Windows Server 2012 R2 o Windows Server 2016.



Creación de un objeto PSO y nuevos parámetros de gestión de contraseñas.

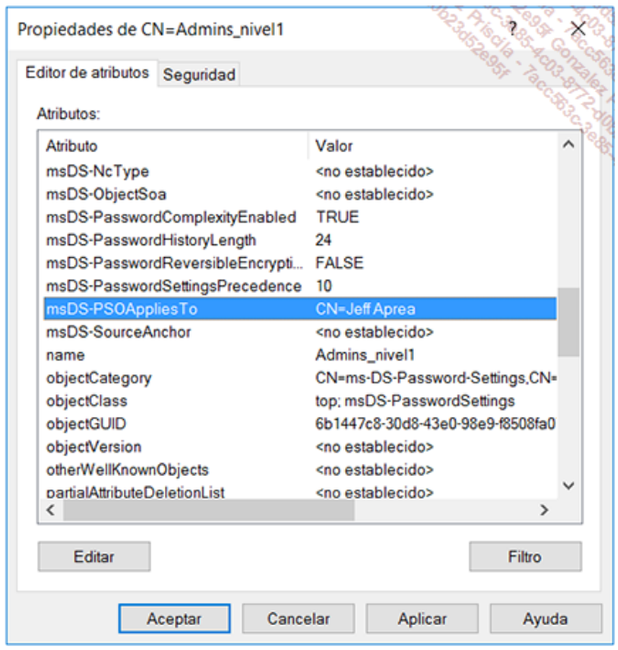
Tenga en cuenta que con Windows Server 2008 y 2008 R2, Microsoft no suministra una interfaz gráfica, ni herramienta de línea de comandos para crear, modificar o suprimir objetos PSO. La solución, también vigente hoy en día, consiste en emplear la herramienta ADSI Edit. Podemos pensar que su uso debe considerarse excepcional.

Tendremos que utilizar ADSI Edit, o un script Ldif, para realizar las operaciones de creación, eliminación, modificación de los objetos PSO, así como para refinar el orden de aplicación y las conexiones de los objetos en los destinos de objetos usuarios o grupos globales de seguridad objeto de estas características.



Visualización y modificación de un objeto PSO con ADSI Edit

La figura anterior muestra que la partición del campo contiene ahora el nuevo contenedor Password Settings Container, el cual contiene un objeto de la clase msDS-PasswordSettings llamado Adminitradores_Nivel1.



Valor del atributo msDS-PSOAppliesTo

Observaremos que la consola MMC Usuarios y equipos de Active Directory permite manipular los atributos de los objetos a través de la nueva pestaña Attribute Editor. Esta mejora de la interfaz es muy útil porque permite un acceso rápido a todos los atributos de todos los objetos de Active Directory, ya se trate de consultar o bien cambiar algunos valores especiales. Por ejemplo, controlando el valor del atributo msDS-PSOAppliesTo, podemos de forma sencilla comprobar las cuentas de usuario y/o de grupos objeto PSO donde Administradores_Nivel1 está vinculado. - o aplicado.

Como siempre con los directorios LDAP, otra alternativa es utilizar el comando Ldifde. Esto nos permitirá aplicar en una sola operación un objeto PSO para múltiples usuarios o grupos de usuarios.

Recordatorio con respecto a Ldifde: LDIF es un estándar de Internet que define un formato de archivo específico para realizar operaciones en modo batch en los directorios respetando las normas LDAP. El Protocolo LDIF puede ser útil para las operaciones de importación y exportación de datos. Para más información sobre la utilización de LDIFDE con Active Directory, consulte el siguiente enlace:http://go.microsoft.com/fwlink/?LinkId=87487

Atributos de Active Directory de objetos PSO - Password SettingsObjects

La tabla siguiente lista los atributos que nos permitirán definir los detalles de un objeto PSO (*Password Settings Object*) declarando los distintos atributos obligatorios y opcionales.

Nombre del atributo	Descripción	Ejemplo de valor
msDS-PasswordSettingsPrecedence	Permite gestionar la prioridad de aplicación de los objetos PSO con un concepto de peso.	10
MsDS-PasswordReversibleEncryption- Enabled	Permite la activación del cifrado reversible de las contraseñas.	FALSE
msDS-PasswordHistoryLength	Número de contraseñas soportadas.	24
msDS-PasswordComplexityEnabled	Permite la activación de las contraseñas complejas.	TRUE
msDS-MinimumPasswordLength	Longitud mínima de las contraseñas.	8
msDS-MinimumPasswordAge	Duración mínima de la contraseña (el valor debe ser negativo).	-864000000000 (1 día)
msDS-MaximumPasswordAge	Duración mínima de la contraseña (el valor debe ser negativo).	-17280000000000 (20 días)
msDS-LockoutThreshold	Umbral de bloqueo de cuenta de usuario.	0
msDS-LockoutObservationWindow	Umbral del período de bloqueo de cuentas de usuarios bloqueados (el valor debe ser negativo).	-18000000000 (30 minutos)
msDS-LockoutDuration	Duración del período de bloqueo de cuentas de usuarios bloqueados (el valor debe ser negativo).	-18000000000 (30 minutos)
msDS-PSOAppliesTo	Vínculos a los que este objeto PSO se aplica. Puede tratarse de usuarios y grupos de usuarios.	CN=u1,CN= Users,DC=DC1, DC=

		corp net,DC=priv

Debemos especificar que se puede "vincular" varios objetos PSO al mismo usuario o grupo de usuarios. También es posible que un usuario sea miembro de varios grupos de usuarios con conexiones a varios objetos PSO.

Por razones evidentes de gestión de las normas de seguridad relativas a las contraseñas, se acordó que los objetos PSO no serán fusionados. El atributo msDS-PSOAppliesTo de un objeto PSO garantiza el vínculo a las cuentas de usuario o grupo de destino.

Por último, pueden existir dos tipos de enlaces: una conexión directa, donde el objeto PSO está vinculado con el objeto de usuario, o una conexión indirecta basada en los objetos PSO vinculados a los grupos a los que pertenece el usuario. Por último, si varios objetos PSO existen para un usuario, entonces un arbitraje tendrá lugar para solo seleccionar uno de los atributos msDS-PasswordSettingsPrecedence definido en los distintos objetos PSO.

Con respecto al esquema de Active Directory y objetos Usuarios InetOrgPerson y grupos: a partir de Windows Server 2008, el esquema de Active Directory añade el atributo msDS-PSOApplied como vínculo inverso sirviendo de enlace entre el objeto destino y el objeto PSO. Este atributo permite al Protocolo RSOP resolver los vínculos entre los objetos Usuarios y grupos y los objetos PSO. En resumen, recuerde que existe el atributo msDS-PSOApplied y también el atributo msDS-PSOAppliesTo.

El objeto PSO que disponga del valor de preeminencia más bajo será aplicado. Para poder gestionar los posibles conflictos, si varios objetos PSO tienen el mismo nivel de preeminencia, el objeto PSO con el GUID menor será elegido y aplicado de manera arbitraria. Este tipo de problema no se producirá si el valor de preeminencia de cada objeto PSO se define de forma correcta.

Objetos de directiva granulares y nivel funcional del dominio Active Directory

El único punto oscuro a tener en cuenta para aprovechar esta nueva funcionalidad de Gestión de contraseñas granulares, es que el dominio debe utilizar el nivel funcional Windows Server 2008 como mínimo. Este punto es en particular importante de destacar, ya que significa que todos los controladores de dominio de dicho dominio deberán haber sido actualizados a Windows Server 2008 como mínimo.

Para más información sobre esta característica, busque en el sitio de Microsoft Technet "step-by-step Guide for Fine-Grained Password and Account Lockout Policy Configuration".

Soporte del Protocolo RSoP y determinación de la estrategia granular a aplicar

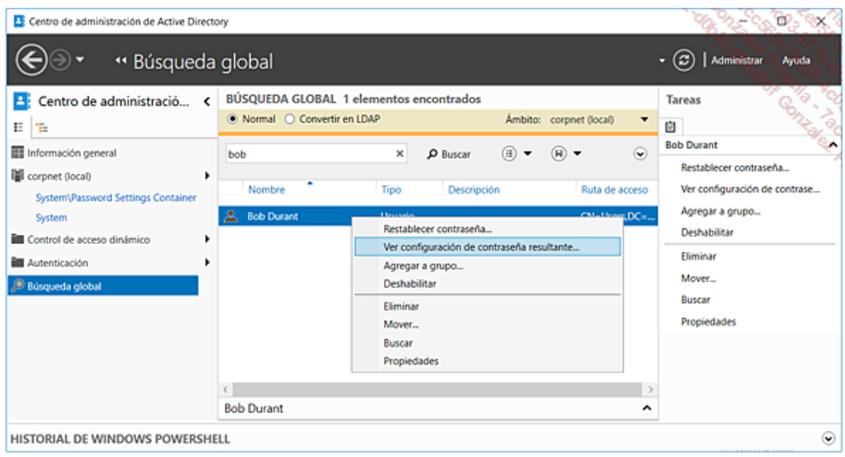
La implementación de las nuevas directivas de contraseña granulares está muy cuidada, ya que el protocolo RSoP (*Resultant Set of Policy*), será soportado para investigar los inevitables problemas de aplicación de las directivas de contraseña granulares.

En efecto, un usuario o un grupo de usuarios puede disponer de varios objetos PSO vinculados, ya sea porque el usuario pertenece a varios grupos, donde cada grupo dispone de uno o varios objetos PSO, o bien porque varios objetos PSO están vinculados al objeto usuario de forma directa.

Sin embargo, al final, solo se aplicará un objeto PSO para el usuario en cuestión. En otras palabras esto significa que cuando varios objetos PSO se refieren a un usuario, los parámetros contenidos en los demás objetos PSO nunca se aplicarán. El problema es determinar qué objeto PSO será aplicado al usuario. Para esto, los mecanismos RSoP permiten evaluar, para un usuario, qué directiva de contraseña granular será aplicada de forma efectiva.

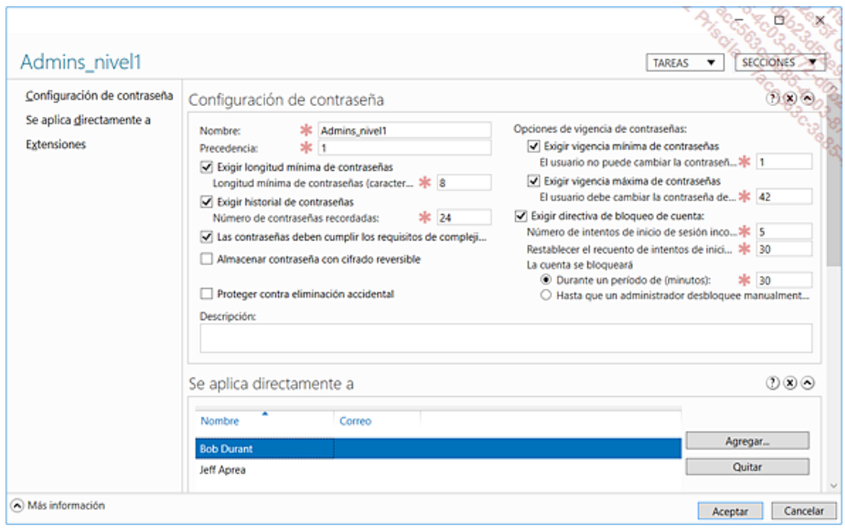
Con respecto a la aplicación de los objetos PSO: los objetos PSO pueden estar relacionados de forma directa con el usuario o de forma indirecta, cuando el objeto PSO está vinculado a un grupo del que el usuario es miembro. Cuando varios objetos PSO están vinculados a un usuario o a un grupo, entonces el objeto PSO resultante se determinará de la siguiente manera: por definición, el objeto PSO resultante es siempre el que está vinculado de forma directa con el usuario. Si varios objetos PSO están vinculados de forma directa con el usuario entonces el objeto PSO cuyo valor de preeminencia es el más bajo será el objeto PSO resultante. Si ningún objeto PSO está directamente vinculado con el usuario, entonces los objetos PSO vinculados a los diferentes grupos de los que el usuario es miembro se seleccionan. El objeto PSO con el valor de preeminencia más bajo se aplicará. Por último, si ningún objeto PSO es seleccionado por el Controlador de Dominio Windows Server 2008 o Windows Server 2008 R2, entonces éste aplicará la directiva por defecto del dominio.

Gestionar las directivas de contraseña granulares con la consola central de administración de Active Directory de Windows Server 2016



Análisis RSOP vía la opción ***Ver configuración de contraseña resultante...***

La figura ilustra el hecho de que el objeto PSO "Admins_Nivel1" se asocia a dos usuarios. El soporte del protocolo RSoP sobre los objetos PSO nos permitirá resolver los posibles errores o conflictos de gestión de directivas de contraseña granulares sobre los usuarios y grupos de usuarios. La búsqueda del objeto PSO resultante se muestra en la pantalla de la siguiente manera:



Vínculos declarados en un objeto de tipo PSO

6. Servicio de Auditoría de Active Directory

Microsoft ha implementado nuevas subcategorías dentro de la categoría **Auditoría directory service access**, las cuales están organizadas de la siguiente manera: Directory Service Access, Directory Service Changes, Directory Service Replication, Detailed Directory Service Replication. En nuestro caso, la subcategoría **Directory Services Changes** es la más atractiva porque registra los eventos de modificaciones de los valores de atributos de objetos sujetos a la auditoría. Se recopilan tanto los valores antiguos como los nuevos. Esta nueva funcionalidad es muy útil en caso de un error de procedimiento, ya que la operación y los detalles de los valores son registrados.

El administrador de un dominio Active Directory puede controlar la directiva de auditoría de la misma manera que en un entorno más antiguo, como Windows Server 2003, editando la directiva por defecto de los controladores de dominio.

Por defecto, los controladores de dominio Windows Server implementan una directiva de auditoría integral que activa la subcategoría **Directory Service Changes**. Por último, los nuevos eventos relativos a estas operaciones se registrarán en el registro de seguridad de los controladores de dominio.

Eventos vinculados a las operaciones de modificación de los objetos de Active Directory:

- Event ID 5136: operaciones de modificación de un atributo.

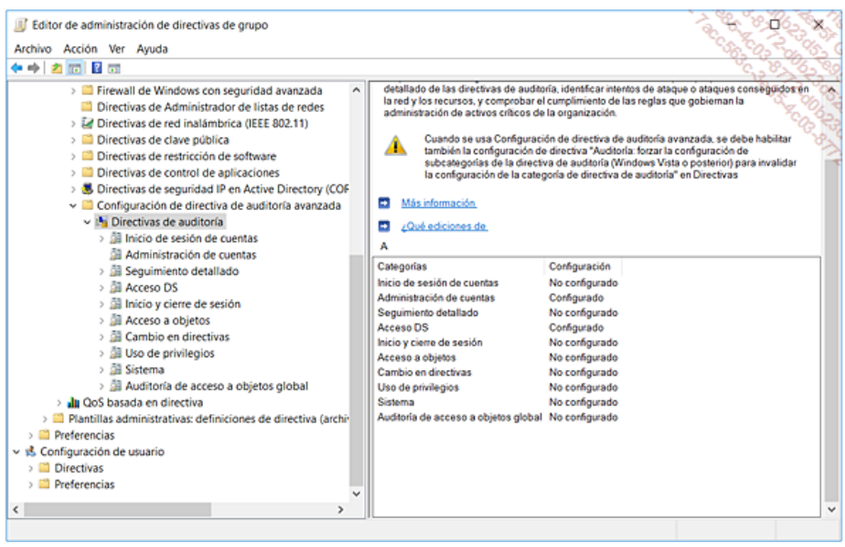
- Event ID 5137: operaciones de modificación de un objeto.

- Event ID 5138: operaciones de recuperación de un objeto.

- Event ID 5139: operaciones de desplazamiento de un objeto dentro del dominio.

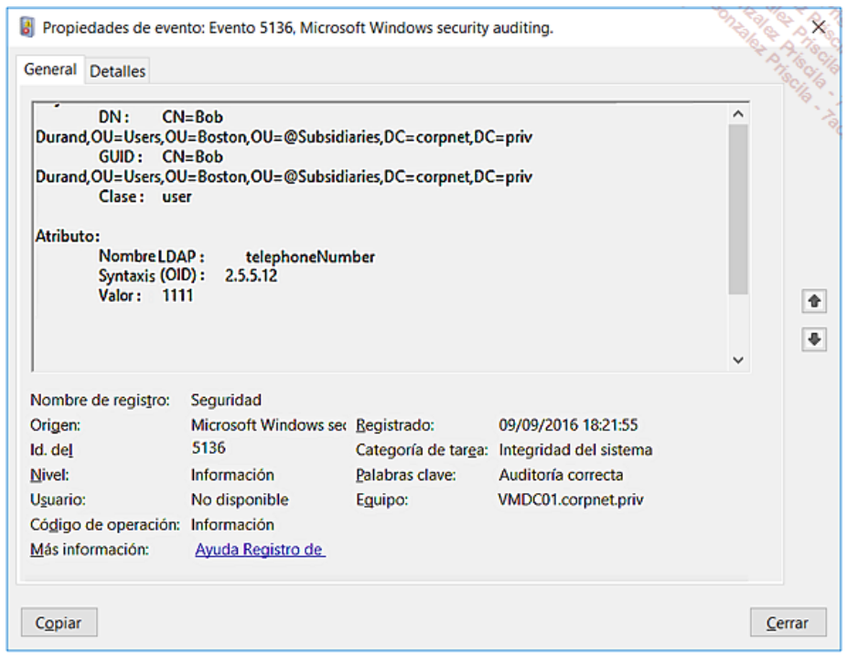
Por ejemplo, el comando `auditpol /set /user:corpnet\Bob.Durand /Category:"System" /success:enable /include`define la auditoría de éxitos para el usuario Bob Durand en los objetos de la categoría System.

Windows Server 2016 tiene una interfaz gráfica de configuración para definir las normas de auditoría de tipo AD DS Auditing. Es interesante notar que estas funcionalidades de auditoría avanzada son introducidas por el rol de controlador de dominio a partir de las versiones de Windows Server 2008 hasta Windows Server 2016 sin que sea necesario elevar el nivel funcional del dominio. Las nuevas funciones de auditoría AD DS están disponibles a partir de la instalación del primer Controlador de Dominio Windows Server 2008 o una versión posterior.



Configuración avanzada de las directivas de auditoría

La figura siguiente muestra como un valor ha sido modificado y por lo tanto reemplazado por otro, provocando la pérdida del valor inicial. El nuevo valor se muestra por supuesto, pero el mensaje anterior precisa la acción "Value deleted" señalando el antiguo valor.



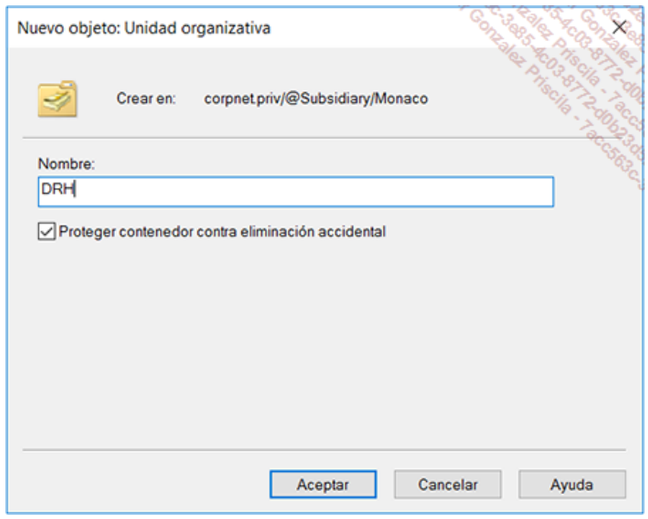
Modificación del atributo LDAP " telephoneNumber "

Para más información sobre las funcionalidades de auditoría de Active Directory, busque "Audit Policy Recommendations" en el sitio Microsoft Technet: https://technet.microsoft.com o siga el enlace siguiente: https://technet.microsoft.com/en-us/library/dn487457.aspx

Para acceder a las mejores recomendaciones de Microsoft en materia de auditoría y seguridad, consulte la herramienta gratuita Microsoft Security Compliance Manager disponible en el sitio de Microsoft a través del enlace: https://technet.microsoft.com/library/cc677002.aspx

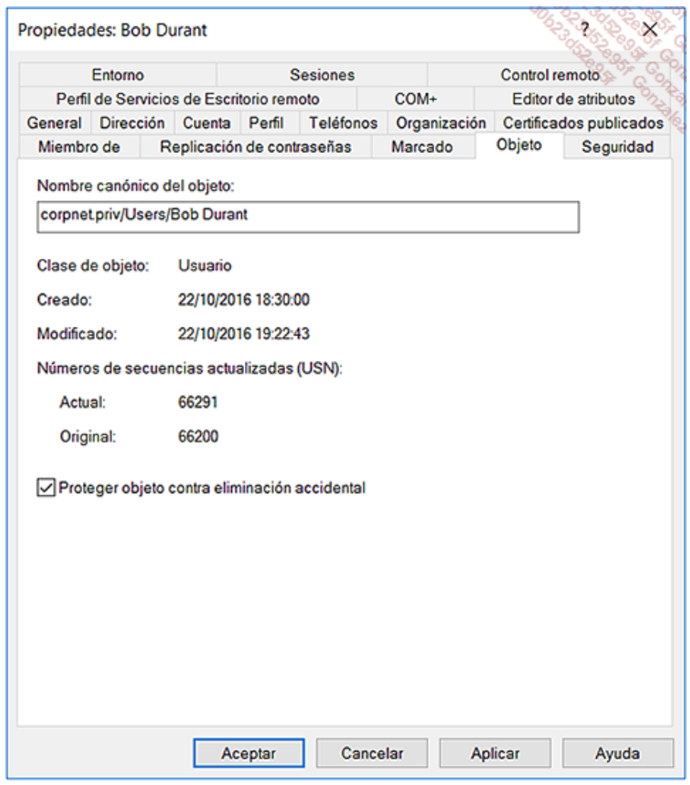
7. Protección de los objetos Active Directory contra el borrado

Las nuevas herramientas de administración de Active Directory permiten proteger los objetos como equipos, controladores de dominio, unidades organizativas, sitios Active Directory... contra una posible operación de borrado por parte de una persona que disponga de estos permisos.

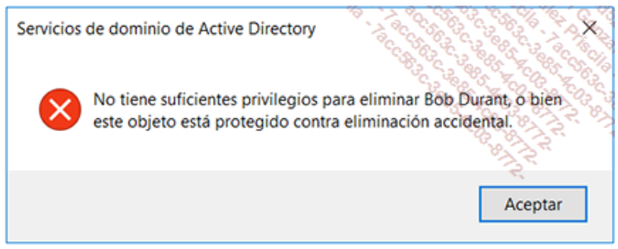


Protección de los objetos contra las eliminaciones accidentales

De esta forma, una gran parte de los incidentes Active Directory causados por errores de manipulación o scripts en especial peligrosos serán eliminados. ¡Esta nueva característica prestará, sin duda, muchos servicios!



Empleo de la pestaña Objeto para activar/desactivar la opción de protección



Mensaje de error que aparece al intentar una eliminación

Active Directory Certificate Services (AD CS)

1. Introducción a la infraestructura de claves públicas (PKI)

Las infraestructuras de claves públicas (PKI, *Public Key Infrastructure*) permiten a las empresas de cualquier tamaño disponer de los elementos técnicos que permiten asegurar las comunicaciones de red, así como las transacciones electrónicas.

Una infraestructura de claves públicas implica el uso de certificados digitales, el uso de mecanismos criptográficos basados en la utilización de claves públicas, así como la puesta a disposición de los equipos, aplicaciones y usuarios de una o varias entidades de certificación. Debido a la utilización generalizada de los certificados para los equipos, aplicaciones y usuarios, los servicios de certificados de Windows Server son un elemento fundamental de una arquitectura segura.

Los mecanismos basados en los certificados digitales requieren comprobaciones en varios niveles. Es así que es posible verificar y autenticar la validez de cada una de las entidades implicadas en una transacción electrónica.

Más allá de la tecnología y en razón de su papel central en términos de seguridad, una infraestructura de claves públicas introduce de forma inevitable la necesidad de publicar dentro de la organización todas las prácticas relativas a la utilización de los certificados digitales.

Desde el punto de vista de los elementos fundamentales que componen una infraestructura de claves públicas, conviene poner de relieve los elementos siguientes:

- Los certificados que serán utilizados por las distintas entidades representadas en el sistema de información.
- Los servicios de certificados que garanticen la emisión de dichos certificados y de forma más amplia la gestión de éstos.
- Las plantillas de certificados adaptadas a las diferentes necesidades y usos.
- Las entidades a utilizar los certificados (usuarios, equipos, aplicaciones y servicios).
- Los procesos y métodos de gestión de los certificados dentro de la empresa.

2. Los diferentes tipos de certificados

a. Introducción

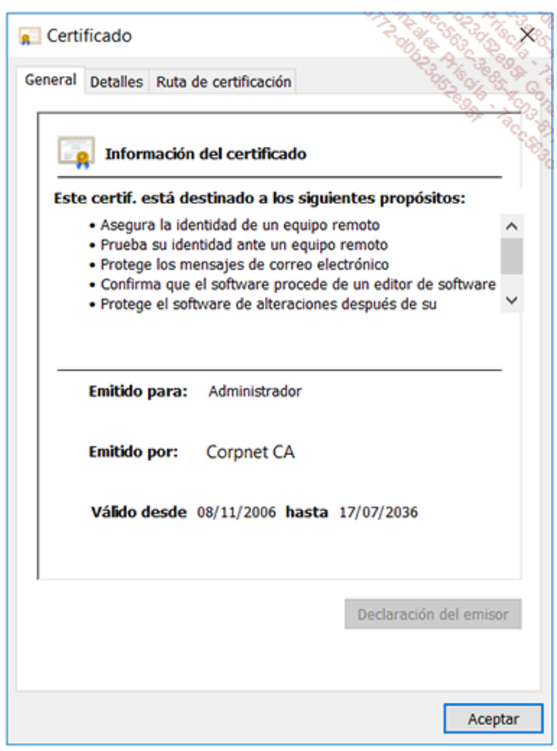
Los certificados están definidos a nivel técnico por la especificación X.509v3. Esta especificación describe los diferentes formatos, opciones y métodos relativos a su uso. Se utilizan por lo general en los sistemas de información modernos donde los elementos activos requieren su utilización. Así, los conmutadores de red, los puntos de conexión Wi-Fi, cortafuegos y otros dispositivos móviles pueden utilizar los certificados para proteger sus comunicaciones de red y operaciones en Internet. Por supuesto, esta lista no es exhaustiva y, por último, cualquier dispositivo, aplicación o entidad activa en la red, pública o privada, podrá usarlos.

Un certificado es una estructura firmada digitalmente por una autoridad emisora; dicho certificado es emitido y entregado a una persona, a un equipo o a una aplicación. Esta estructura digital crea la relación entre la identidad que se examina, el valor de la clave pública asociada y la clave privada correspondiente.

Con respecto a la especificación X.509v3: Se trata de la versión 3 de la recomendación X.509 de la ITU-T que especifica la sintaxis y el formato de los certificados digitales. Este formato es el formato estándar de los certificados utilizados en los sistemas operativos modernos, así como todos los dispositivos físicos de la red.

Además de la clave pública, un certificado X.509 contiene información que permite reconocer la entidad que emite el certificado, así como información sobre el certificado mismo. Por último, en función del tipo de certificado, también habrá información sobre la entidad de certificación que expide el certificado.

Una de las características más interesantes contenida en un certificado atañe a las funciones otorgadas a éste y por lo tanto, a la entidad que lo posee.

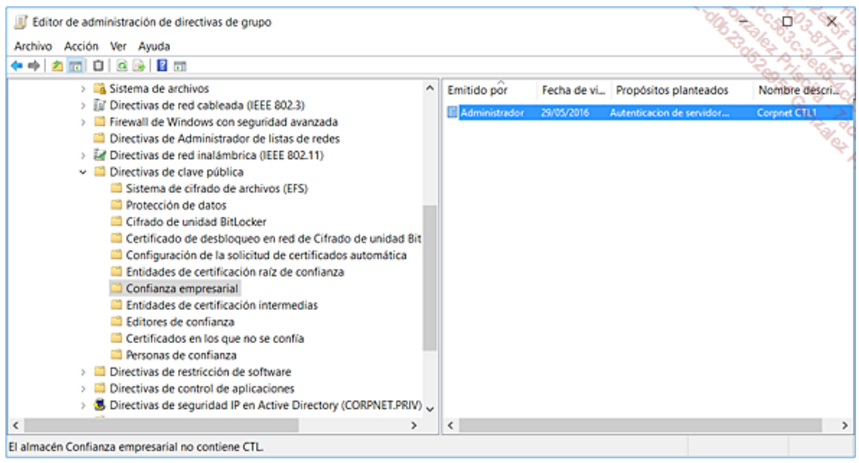


Certificado basado en el modelo oficial entregado a la cuenta Administrador del dominio Corpnet.priv y roles asociados

Los servicios de certificados incluidos en la familia de sistemas operativos Windows Server implementan el concepto de plantilla, que permite la emisión de certificados formateados y adaptados a usos específicos. En este ejemplo, el certificado se ha construido sobre la base de la plantilla Administrador, la cual contiene varias funciones.

Un ejemplo notable es el rol "firma de la lista de aprobación Microsoft", que permite firmar los objetos de tipo "Lista de confianza empresarial". La figura siguiente ilustra esta posibilidad a través de un objeto de directiva de grupo. La interfaz pone de relieve el hecho de

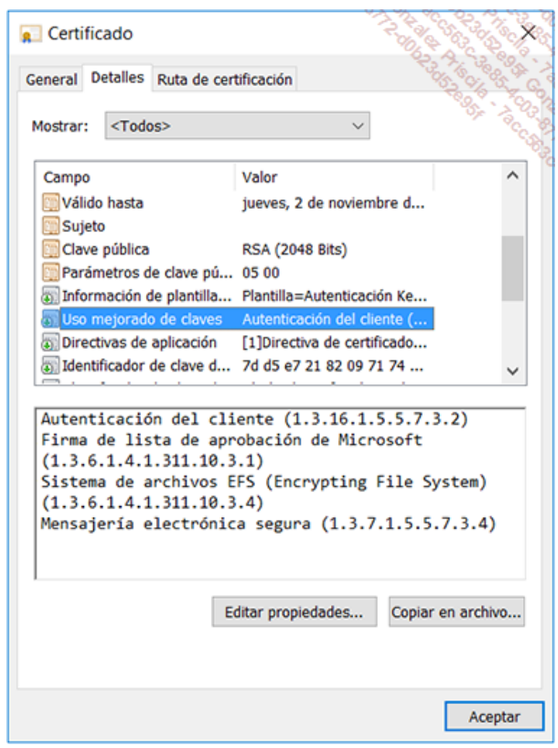
que la lista cuyo nombre cotidiano es "Lista de CA adicionales" fue expedido por una persona "con esta responsabilidad especial" a través de la función "Firma de la lista de aprobación".



Agregar autoridades raíz de confianza aprobadas por una CTL (Certificate Trust List), firmada por la cuenta administrador

Firma de listas de confianza: como es el caso de las operaciones de firma, es indispensable que la persona que efectúe la operación disponga del certificado con la capacidad de firmar una lista de confianza en el almacén de certificados personales, así como la clave privada asociada. En el ejemplo anterior, la cuenta administrador del dominio tiene un certificado basado en la plantilla de certificado Administrador que le permite firmar este tipo de objetos

La figura siguiente muestra el conjunto de roles contenidos en el certificado. El rol **Sistema de archivos EFS** (*Encrypted File System*) permite al usuario que disponga del certificado utilizar los servicios de cifrado de archivos disponibles en las plataformas Windows Client, Windows 2000 hasta Windows 10. En este ejemplo, la clave pública del usuario se utiliza para cifrar la clave de cifrado simétrica que permite cifrar un archivo particular. Luego, la clave privada del usuario es la única clave capaz de descifrar la clave de cifrado simétrica que permitirá descifrar el archivo. Otro ejemplo clásico se refiere a la mensajería segura. El rol **correo seguro** permite firmar y cifrar los mensajes electrónicos a través del protocolo S/MIME (*Secure Multipurpose Internet Mail Extensions*) el cual es soportado por los productos de correo como Microsoft Outlook y Microsoft Exchange Server. Por último, el rol **Autenticación del cliente** permite al usuario autenticarse demostrando su identidad a un servidor que soporte, también, el uso de certificados X.509v3.

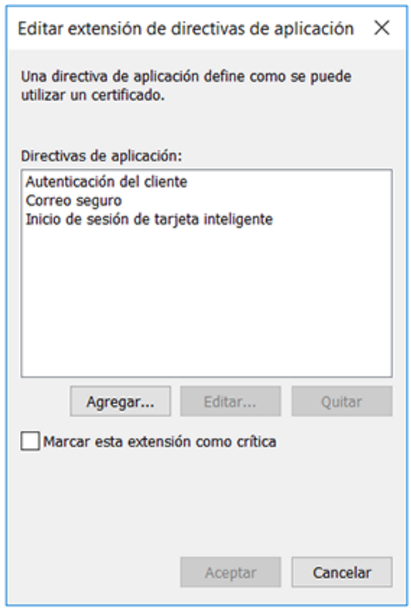


Certificado de la cuenta Administrador y funciones asociadas: firma de los CTL, cifrado de archivos EFS, correo electrónico S/MIME y autenticación del cliente

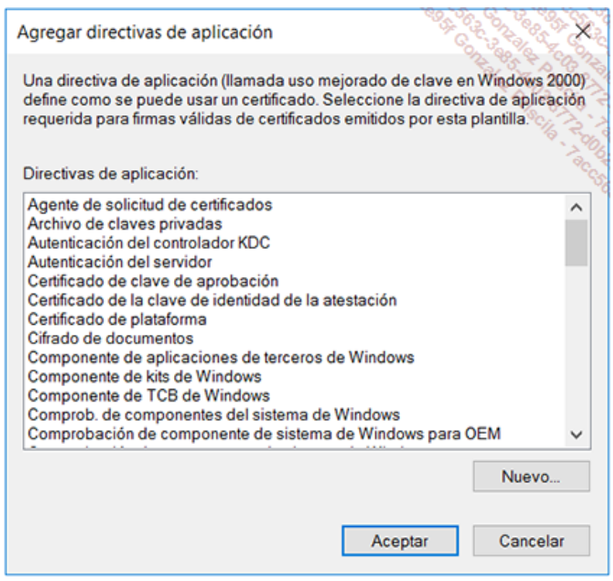
Con respecto a la utilización de la clave: un certificado permite a su poseedor, el cual se denomina el "sujeto", realizar una o varias tareas específicas. Para implementar el control del uso de certificados en función de las funciones, las restricciones se encuentran por supuesto incluidas en cada certificado. El campo **Uso de la clave** permite definir el marco de la utilización del certificado, es decir, los roles soportados. También es posible emitir certificados en función de las necesidades de los usuarios, equipos, dispositivos de red o aplicaciones.

Así, como acabamos de ver, los certificados podrán ser expedidos para múltiples funciones tales como la autenticación de usuarios accediendo a un sitio web empleando su navegador, la autenticación de servidores Web con los clientes, la seguridad de los mensajes electrónicos empleando el protocolo S/MIME, la seguridad de los datagramas IP empleando el protocolo IPSec. Por último, el uso de certificados no tiene límites reales. La gestión de derechos digitales empleando los servicios DRM (*Digital Rights Management*) es un ejemplo muy significativo.

Gracias a los certificados, es posible asumir una gestión avanzada de los derechos digitales sobre los datos y las identidades situadas dentro y fuera de la red empresarial. La figura siguiente ilustra las muchas funciones soportadas por las autoridades de certificación Windows Server, así como la posibilidad de crear nuevas.



Modificación de las directivas de aplicación sobre un nuevo modelo de certificado basado en la plantilla "Usuario de tarjeta inteligente ".



Lista de directivas de aplicación que definen la manera en que un certificado puede ser utilizado

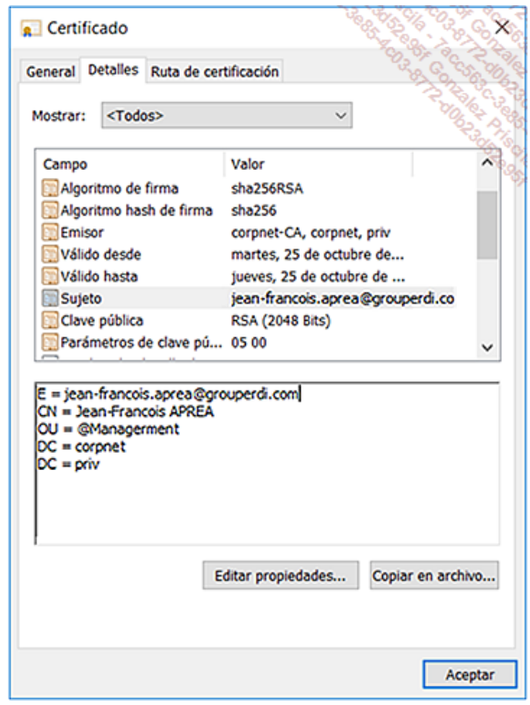
Las autoridades de certificación soportadas por las diferentes versiones de Windows Server se suministran con diferentes plantillas de certificado diseñadas para satisfacer las necesidades de la mayoría de las organizaciones. Tenga en cuenta que con las autoridades de certificación de Windows Server 2003 y posteriores, a diferencia de Windows 2000, los roles aparecen en las plantillas de certificados bajo el texto **Directiva de aplicación**.

Personalización de las plantillas de certificados: las entidades de certificación Windows Server 2003 Edición Enterprise y Datacenter soportan dos modelos de certificado: los modelos versión 1 y los modelos versión 2. Las plantillas Versión 2 correrán solo con autoridades Windows Server 2003 y posteriores hasta Windows Server 2016. A diferencia de los permisos Windows 2000 Server, que permiten personalizar la mayoría de los parámetros contenidos en una plantilla. Una de las tareas más importantes de los administradores de certificados se refiere a la definición de plantillas adicionales adaptadas a las necesidades específicas de la organización. Las entidades de certificación Windows Server 2008 y Windows Server 2008 R2 soportan también los certificados basados en los modelos versión 3. Estas nuevas plantillas soportan los algoritmos de encriptación del tipo ECC (*Elliptic Curve Cryptography*) para los equipos Windows 7 y versiones posteriores hasta Windows 10 y Windows Server 2016.

Por último, es importante señalar que cada entidad del tipo usuario, equipo o aplicación, con uno o varios certificados se conoce bajo la denominación de "Asunto de certificado". Por su parte, la autoridad de certificación será considerada como "la autoridad emisora y firmante" del certificado emitido.

b. Naturaleza y contenido de un certificado digital

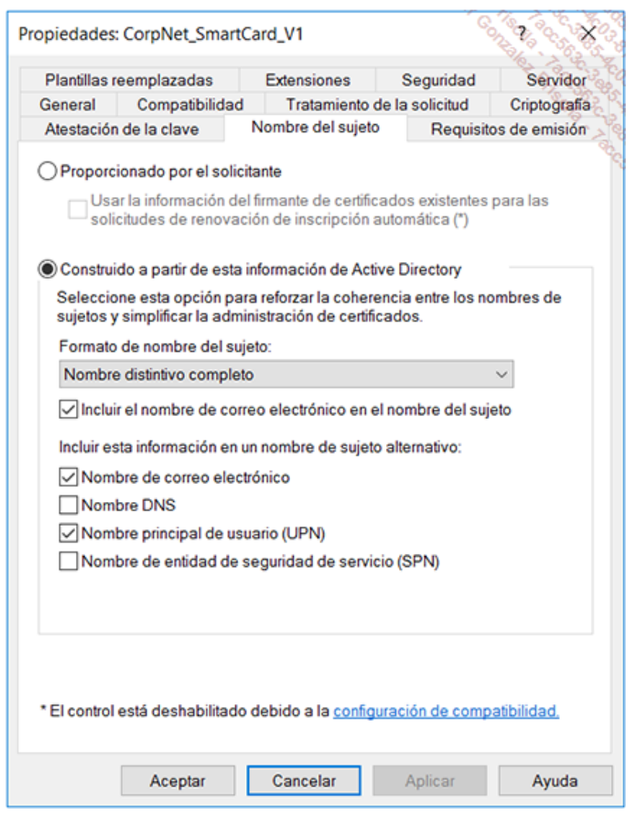
Un certificado digital contiene muchos datos técnicos y lógicos. En primer lugar, el certificado digital proporciona información "clara" que permite identificar el objeto del certificado. La figura siguiente muestra que se trata del certificado de un usuario (y no de un equipo o una aplicación) y que el valor del campo objeto contiene el DN (*Distinguished Name*) de éste dentro del sistema de directorio de Active Directory. Es interesante notar que el campo objeto contiene el valor del DN es decir: CN=Jean-Francois Jeff. APREA, OU=@Management,DC=Corpnet,DC=net al igual que la dirección de correo de dicho usuario.



Construcción del nombre del sujeto a partir de la información contenida en Active Directory

Valor del campo **Objeto**: cuando una solicitud de certificado se envía utilizando las plantillas entregadas por defecto, la inclusión del tema tiene lugar sin exigir ninguna entrada por parte del usuario.

La imagen siguiente muestra los diferentes parámetros que pueden ser combinados en las plantillas de certificados para construir de forma automática el nombre del tema en base a la información contenida en el directorio de Active Directory.



*Creación de una plantilla de certificado y pestaña **Nombre de sujeto** para establecer una coherencia entre los nombres y simplificar la administración de los certificados*

Además del campo **Objeto** que identifica el tema, los certificados contendrán los siguientes datos:

- El valor de la clave pública del sujeto.
- El período de validez que define el período durante el cual el certificado es válido.
- La información que identifica a la autoridad de certificación que expide el certificado.
- La firma digital de la autoridad emisora. De esta forma, podemos confirmar la relación que une la clave pública del sujeto con sus datos de identificación.

El período de validez de un certificado permite limitar en el tiempo el uso de un certificado. Una vez alcanzado el período de validez de un certificado, dicho certificado no podrá ser utilizado y un nuevo certificado deberá ser solicitado por el sujeto.

Podemos encontrar una analogía de este principio fundamental con documentos tales como la tarjeta de identidad o pasaporte. El documento oficial permite demostrar la identidad de la persona, ya que la prefectura del departamento es la autoridad que emitió el documento de identidad, esta última es de confianza ya que ha firmado empleando el sello de la prefectura. El número que figura en el pasaporte o documento de identidad puede también ser comparado con el número de serie del certificado. Por último, la fecha de emisión del documento de identidad fija su fecha de vencimiento ya que los documentos oficiales también están sujetos a un período de validez.

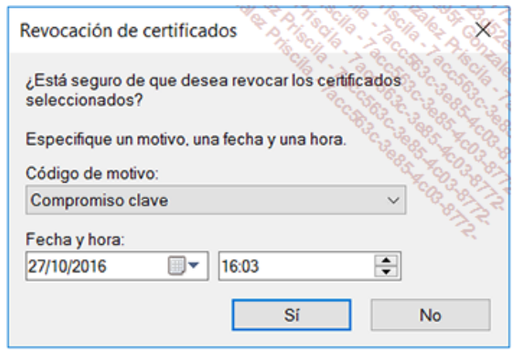
Administración de identidades, criptografía, biometría y logon único SSO

Hoy en día, nuestros pasaportes utilizan tecnología biométrica para demostrar de manera indiscutible la identidad de la persona. En efecto, aunque utilizable en el marco de un primer reconocimiento visual, la tradicional fotografía puede ser falsificada con demasiada facilidad. La huella digital o la retina del sujeto puede entonces verificarse en segunda instancia. Basta en este caso, con comparar los datos biométricos del sujeto en relación a los incluidos en el documento mismo o incluso fuera de éste, en cuanto a las operaciones de control realizadas en los aeropuertos de algunos países (toma de huellas dactilares y de retina en los Estados Unidos). Los datos personales de identificación se almacenan en un chip electrónico de tipo tarjeta inteligente con certificados y datos de identificación privados o una cadena de valores de tipo código de barras, mientras que los datos públicos son accesibles de forma libre para comprobar la exactitud de los datos biométricos presentados. Este principio también está disponible en los entornos Active Directory para autenticar a los usuarios empleando su tarjeta inteligente sustituyendo el tradicional código PIN (*Personal Identification Number*) por un control biométrico conde la parte privada estaría incluida en la tarjeta inteligente. De esta manera, las claves privadas y los datos biométricos privados del sujeto, a menudo llamados "template", solo están en posesión del mismo sujeto y nadie más. Solo son utilizables por el mismo y verificables en el último momento cuando se requiere un control. Las tecnologías biométricas participan, por tanto, en primera instancia en la reducción de la utilización de contraseñas y otros códigos secretos durante el proceso de logon inicial. En segunda instancia, los servicios de seguridad de tipo SSO, permiten el uso de logon inicial de tipo "único" para acceder a los datos y aplicaciones de la empresa.

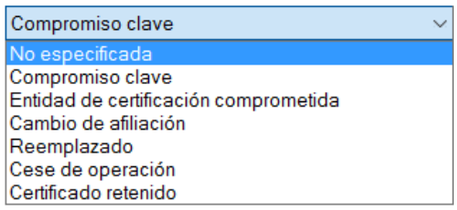
Cuando un documento de identidad, o un certificado se encuentra en peligro como consecuencia de robo o pérdida, se hace necesario hacer la declaración. De esta manera, el certificado robado o perdido deja de ser de confianza y se convierte en inservible. Esta operación llamada revocación permite romper la confianza declarada a través del certificado. Cada autoridad de certificación que emite certificados mantiene una lista de revocación de certificados, la cual se utiliza por el sistema operativo, programas o el usuario en el momento del control de validez de dicho certificado. Es importante señalar que el certificado revocado no pasará a ser realmente inservible hasta el momento en que la operación se publique en la lista de revocación de certificados.

Con respecto a la revocación de certificados: ¡Observe! Mientras que la lista de revocación no sea actualizada y luego publicada y comprobada en el marco del control de la validez del certificado, el mismo certificado revocado sigue siendo de confianza, por lo tanto, utilizable.

La figura siguiente ilustra esta operación realizada a nivel de la autoridad de certificación por un administrador de certificados:



Revocación de un certificado indicando la razón, la fecha y hora



Lista de códigos de causa de revocación

c. Certificados X.509 versión 1

La especificación X.509 Versión 1 aclara los diferentes campos contenidos por un certificado de tipo versión 1.

El nombre de los diferentes campos utilizados se especifica en español y también entre paréntesis en inglés por razones prácticas de uso corriente en mucha documentación, notas técnicas, sistemas de mensajes, etc.

- **Versión** (*version*): este campo contiene la versión del certificado.
- **Número de serie** (*Serial Number*): identificador único numérico asociado a cada certificado emitido por una entidad certificadora.
- **Algoritmo de firma de la autoridad** (*signature algorithm*): nombre del algoritmo de firma utilizado por la autoridad de certificación para firmar el contenido de un certificado digital. En general, se trata del algoritmo SHA1RSA.

Los campos Versión, número de serie, Algoritmo de firma, Emisor, Período de validez, Objeto y Clave pública serán firmados por la autoridad de certificación.

- **Emisor** (*Issuer Name*): este campo contiene el valor del DN X.500 (*Distinguished Name*) especificando el nombre de la autoridad de certificación que expide el certificado. Por ejemplo, CN=Corpnet Security Services, DC=Corpnet, DC=net. Como información, la utilización del formato X.500 para nombrar a la autoridad se define en la especificación X.509, así como en el RFC 3280 titulado**Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile**.
- **Válido a partir de/válido hasta el** (*Valid from/Valid to*): estos campos declaran el período durante el cual el certificado podrá ser utilizado. Algunas implementaciones sustituyen estos dos campos por un único campo llamado Período de validez (*Validity Period*).
- **Objeto** (*Subject Name*): este campo contiene el valor del nombre del equipo, dispositivo de red, usuario o servicio asociado al certificado. En general, el formato de este campo utiliza una sintaxis de tipo X.500, tal como se define en las especificaciones X.509, pero también puede utilizar formatos diferentes (dirección de correo electrónico, un nombre DNS, un sufijo UPN o incluso un SPN).

Particularidades de los diferentes formatos soportados por el campo objeto: los formatos siguientes pueden ser utilizados.

Nombre de correo electrónico: si el nombre de correo es introducido en el objeto usuario Active Directory, éste se utilizará. En este caso, se trata de un certificado de tipo Usuario.

Nombre DNS: el nombre de dominio completo (FQDN) del objeto que ha solicitado o que representa el certificado. En este caso, se trata de un certificado de tipo Equipo.

Nombre de usuario: el nombre de usuario es un atributo de los objetos Usuario Active Directory y podrá ser utilizado como este

concepto. En este caso, se trata de un certificado de tipo Usuario.

Nombre del servicio principal (SPN): el nombre del servicio principal es un atributo que forma parte de los objetos equipo Active Directory y podrá ser utilizado como este concepto.

Con respecto a los SPN: los SPN son los nombres utilizados como identificadores únicos utilizados para representar a los servicios que funcionan en un servidor dado. Los servicios que utilizan la autenticación Kerberos de los dominios Active Directory o reinos Kerberos requieren un SPN para cada uno de ellos. Así, los clientes pueden identificar a dicho servicio en la red.

Tenga en cuenta que en un entorno Active Directory, un SPN es un atributo de los objetos de las clases usuario y equipo. En general, cada servicio debe contar con un único SPN de tal forma que no sea posible seleccionar otro equipo o utilizar una clave errónea en un ticket Kerberos.

- **Clave pública** (*Public Key*): este campo contiene la clave pública asociada al poseedor del certificado. La clave pública es un dato criptográfico que será transmitido por el solicitante del certificado a la autoridad de certificación empleando una consulta de solicitud de certificado. Este campo contiene también la declaración del tipo de algoritmo de clave pública utilizado en la generación del par de claves asociadas al certificado.

d. Certificados X.509 versión 2

Acabamos de ver que los certificados X.509 Versión 1 disponen de información básica necesaria para describir el propio certificado. Sin embargo, la autoridad emisora sólo dispone de unos pocos parámetros. En efecto, la especificación X.509 Versión 1 pone a disposición el nombre del emisor y la firma de la autoridad.

Esta falta de información no permite gestionar bien determinados eventos como la renovación del certificado de la autoridad de certificación misma. En efecto, en este caso habrá dos certificados con el mismo valor de campo **Emisor**. Por consiguiente, es fácil aplicar una autoridad de certificación "falsa" con el mismo nombre que la primera.

Para resolver esta limitación inherente a los certificados X.509 Versión 1, la especificación X.509 Versión 2 publicada en 1993 introduce nuevos campos, los cuales se presentan a continuación:

- Identificador único del emisor (*Issuer Unique ID*): este campo contiene un identificador único definido por y para la autoridad de certificación emisora. Este identificador se regenera cuando el certificado de la autoridad se renueva.
- Identificador único del sujeto (*Subject Unique ID*): este campo contiene un identificador único definido para el certificado del sujeto por la autoridad emisora. En el caso de que el sujeto sea a su vez la autoridad de certificación emisora, el identificador único es situado en el campo **Identificador único del emisor** (*Issuer Unique ID*).

La implementación de estos dos campos permite mejorar de forma significativa la verificación de la cadena de enlace entre el certificado de un sujeto y la autoridad que lo expidió. En efecto, es posible buscar el certificado de la autoridad comprobando la relación existente entre el nombre de la autoridad emisora declarado en el certificado expedido y el nombre del sujeto declarado en el certificado de la autoridad de certificación. Una vez logrado este primer control, se podrá realizar una segunda verificación. Ésta tendrá como objetivo comprobar el identificador único del emisor (*Issuer Unique ID*) del certificado emitido con el identificador único del sujeto (*Subject Unique ID*) del certificado de la autoridad.

Atención: Aunque los certificados X.509 Versión 2, representan un avance significativo en comparación con la versión 1, no son utilizados en la práctiva por falta de soporte. De hecho, el RFC 3280 recomienda no utilizar los campos específicos de la versión 2 y de preferir la especificación X.509 Versión 3.

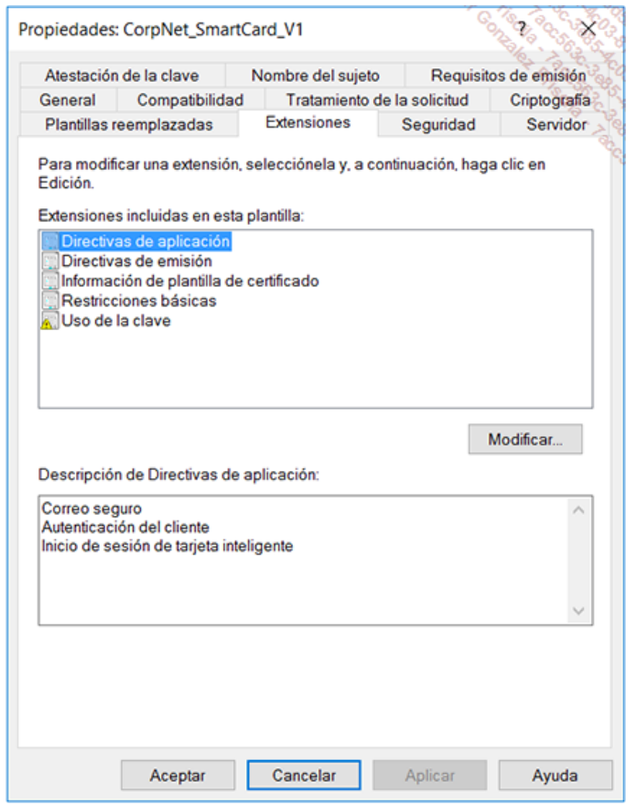
e. Certificados X.509 versión 3

La especificación X.509 versión 3 fue publicada en 1996. Ésta especifica el concepto de las extensiones. Estas extensiones añaden a la vez características para los certificados mismos y grandes posibilidades de cara a las aplicaciones que puedan utilizarlos. Además, las extensiones soportadas por los certificados X.509 Versión 3 permiten soportar la problemática de validación de la cadena de certificación presentada más arriba.

En primer lugar, conviene precisar que una extensión dentro de un certificado X.509 Versión 3 está compuesta por los siguientes elementos:

- El valor de la extensión que depende de cada extensión.
- El indicador de tipo Extensión crítica: este indicador especifica que el control de la extensión es de carácter crítico. En el caso de que la aplicación que use el certificado no pueda interpretar o reaccionar correctamente en función del valor de la extensión, el certificado no será utilizado.

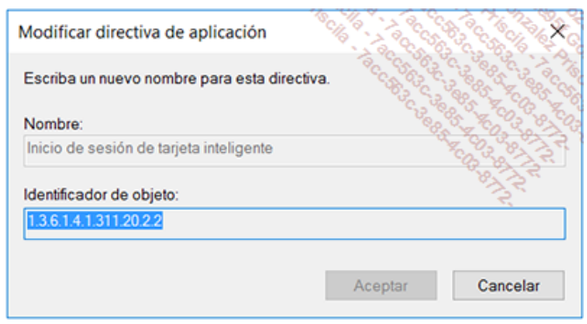
¡Importante! Cuando una aplicación no reconoce una extensión determinada y el indicador **Extensión crítica** no se declara, entonces la aplicación ignora la extensión y podrá seguir utilizando el certificado.



Directivas de aplicación y estrategia crítica (Uso de la clave)

La figura anterior muestra una plantilla de certificado soportada por una autoridad de certificación de Windows Server 2016. Este modelo podrá puede utilizarse por los miembros del grupo de usuarios del departamento de Marketing y será objeto de una extensión crítica. Las aplicaciones podrán utilizar los certificados basados en este modelo y controlar las funciones declaradas (derechos digitales, correo electrónico seguro, etc.) en base a los OID (*Object IDentifier*) relativos a cada uno de los roles.

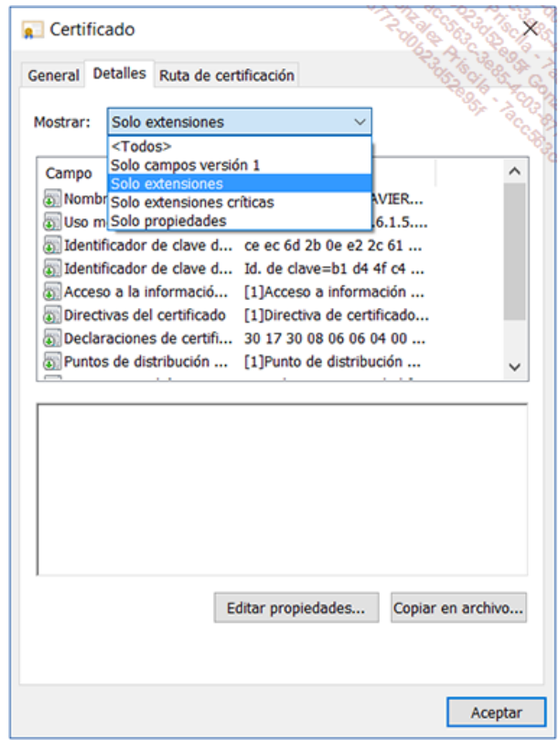
- El identificador de extensión: la imagen siguiente ilustra este importante campo. Este permite introducir el valor de la OID que será asignada a la extensión.



Identificador de Objeto (OID) de la extensión utilizado por la plantilla de aplicación "Inicio de sesión de tarjeta inteligente".

Ahora que sabemos que una de las características principales que ofrecen los certificados X.509 Versión 3 es la posible utilización de los "identificadores de extensiones", podemos describir el conjunto de los campos soportados por los certificados que utilizan esta especificación. La imagen siguiente pone de manifiesto el hecho de que un certificado utilizado hoy respeta siempre las especificaciones X.509 Versión 3, al igual que soporta los campos de tipo versión 1.

Los servicios de gestión de los certificados integrados en Windows permiten simplificar la visualización de la información contenida en el certificado filtrando los campos en base o no a las extensiones obligatorias.



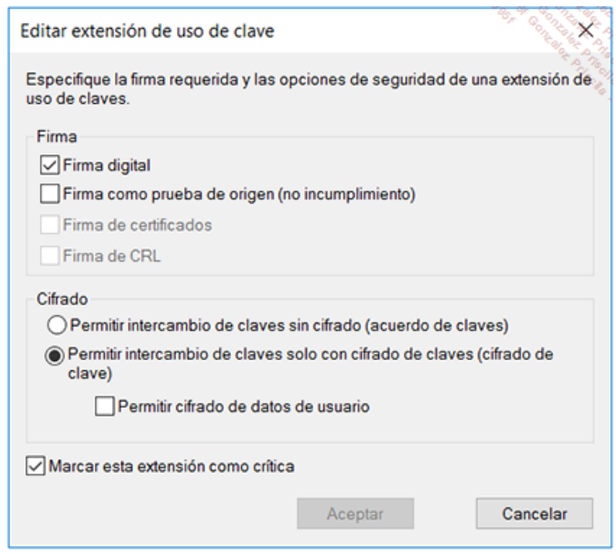
Visualización simple de los campos y filtrado de extensiones

Las extensiones propias de los certificados X.509 Versión 3 se presentan en detalle a continuación:

- **Identificador de clave de autoridad** (*Authority Key Identifier - AKI*): este campo puede contener dos tipos de valores. Por un lado, el nombre de la autoridad de certificación, así como el número de serie del certificado de la autoridad de certificación emisora. Por otra parte, una huella digital (hash) de la clave pública del certificado de la autoridad emisora del certificado.
- **Identificador de la clave del sujeto** (*Subject Key Identifier - SKI*): este campo representa una extensión que contiene una huella de la clave pública de dicho certificado.

Con respecto a las extensiones AKI y SKI: estos dos tipos de información son fundamentales para que la verificación de la cadena de certificación y validación de certificados X.509 Versión 3 pueda ocurrir.

- **Utilización de la clave** (*Key Usage*): cualquier entidad podrá disponer de un único certificado o de varios. Esta extensión permite precisar las funciones de seguridad que pueden ser utilizadas. Por ejemplo, un certificado puede ser utilizado solo para garantizar un inicio de sesión por tarjeta inteligente, mientras que otro permitirá que el mismo usuario firme y/o cifre los mensajes electrónicos. Para lograrlo, el uso de la clave debe precisarse empleando la ventana que aparece a continuación usando las opciones disponibles a nivel de extensión:



Utilización de la clave y el modo de "Marcar esta extensión como crítica".

El uso de claves se controla empleando los parámetros de uso de claves, así como las directivas de aplicación contenidas en el certificado. La utilización de la clave es también llamada "restricción básica" sabiendo que esta limitación se aplicará sobre el conjunto de las operaciones que se llevarán a cabo con el certificado. La figura anterior muestra que son posibles múltiples opciones y combinaciones en función del contexto de uso previsto.

En todos los casos, se trata de combinar el uso de las claves para las operaciones de firmas y para las operaciones de cifrado. Para cada certificado, la extensión **Uso de la clave** puede usar las siguientes opciones:

Funciones de firma

- **Firma digital** (*Digital Signature*): los datos pueden ser firmados de forma digital por el certificado. La clave pública puede ser utilizada para verificar las firmas, así como para las autenticaciones de los clientes y el origen de datos firmados.
- **No repudio** (*nonrepudiation*): los datos firmados por el certificado podrán hacer referencia al sujeto que suministra la firma digital. Esta relación permite el no repudio de la firma de tal manera que es posible aplicar las transacciones seguras basadas en esas firmas.
- **Firma de certificado** (*Certificate Signing*): un certificado puede ser utilizado para firmar otro certificado. Se trata de una función específica asignada a los Administradores de certificados. Las autoridades de certificación también utilizan este tipo de servicios.
- **Firma de la lista de revocación de certificados** (*Certificate Revocation list signing*): un certificado puede ser utilizado para firmar las

listas de revocación de certificados.

Funciones de cifrado

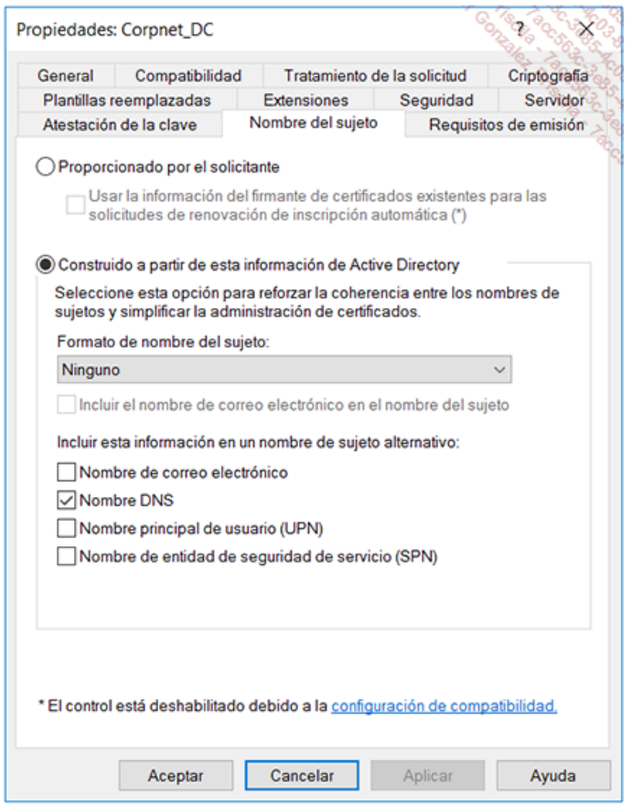
- **Intercambio de clave sin cifrado** (*Key Agreement*): esta opción configura el sujeto para que pueda utilizar un protocolo de gestión de claves que le permite generar una clave simétrica. Esta clave simétrica puede ser utilizada para cifrar y descifrar los datos entre el sujeto y el destinatario deseado. Esta técnica se utiliza con el protocolo de gestión de claves simétricas Diffie-Hellman. En este caso, la clave pública puede ser utilizada para transportar una clave simétrica entre dos socios empleando un protocolo de intercambio de clave.
- **Intercambio de clave cifrada** (*Key Encipherment*): esta opción configura el sujeto para que pueda utilizar un protocolo de gestión de claves que le permite generar una clave simétrica. Esta clave simétrica puede ser utilizada para cifrar y descifrar los datos entre el sujeto y el destinatario deseado. En este caso, la clave simétrica se genera y luego encripta para por último enviarse al destino que se hará cargo del descifrado. Este método debe ser seleccionado cuando se utilizan claves RSA.
- **Cifrado de datos de usuario** (*Data Encipherment*): esta opción permite al sujeto utilizar una clave simétrica para cifrar y descifrar los datos teniendo en cuenta que la misma clave simétrica se usa también para el cifrado de la clave durante su transporte.
- **Utilización de la clave privada** (*Private Key Usage Period*): esta extensión permite especificar un período de validez especial para la clave privada del sujeto. El valor de vida puede fijarse en un valor inferior a la vida del certificado en cuestión. De esta forma, podemos limitar el tiempo de uso de la clave privada para la firma de documentos, permitiendo a la clave pública asociada al certificado utilizarse por más tiempo para comprobar dichas firmas. Por ejemplo, la vida útil de la clave privada puede estar limitada a seis meses, mientras que la de la clave pública podría ser mucho más larga (dos años o más).

Observe: la RFC 3280 publicada en abril de 2003 recomienda no utilizar esta extensión.

- **Directivas de certificado** (*Certificate Policies*): esta extensión describe las directivas y procedimientos aplicados para validar la solicitud de certificado antes de que éste sea emitido. El valor de este campo está constituido por una serie de términos para definir la directiva aplicada al certificado, ya que éste se construye en base a un OID y cualificadores opcionales. Estos cualificadores opcionales se utilizan con frecuencia para declarar una URL que describe con precisión las directivas de gestión, políticas de seguridad, así como los procedimientos de emisión y revocación de certificados.

Los cualificadores, opcionales, no tienen influencia en la definición de la directiva declarada. Cuando se trata del certificado de un usuario, de un equipo o de un servicio, estos términos explican el contexto de uso del certificado y por lo tanto, para lo que se ha emitido. Cuando se trata del certificado de una autoridad de certificación, esta información limita el conjunto de directivas para las rutas de certificación, incluyendo el certificado de autoridad. En el caso de que no sea necesario restringir el conjunto de directivas, es posible declarar una directiva específica (anyPolicy) y asociarle un valor de la OID igual a 2 5 29 32 0.

- **Otros nombres de objeto** (*Subject Alternative Name*): esta extensión permite introducir los nombres adicionales asociados al sujeto. Mientras que el nombre del sujeto se incluye en forma de un DN X.500, esta extensión permite añadir información de identificación dentro del certificado. Esta información puede incluir la dirección de correo electrónico Internet, el nombre DNS del equipo o del dispositivo, e incluso una dirección IP. En general, el uso correcto de esta extensión permite disponer de la misma información en diferentes formas.



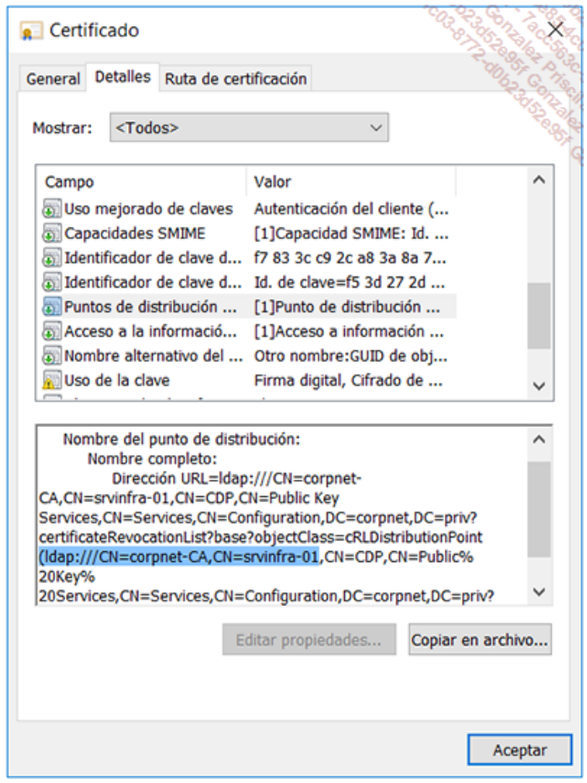
Nombre del sujeto basado en el nombre DNS para los equipos

¡Observe! Es imprescindible utilizar esta extensión respetando las instrucciones relativas al buen funcionamiento de las aplicaciones. Por ejemplo, una aplicación de correo electrónico podrá exigir que esta extensión introduzca la dirección de correo electrónico del usuario. Como los datos están incluidos en el certificado mismo, la autoridad de certificación debe ser capaz de verificar dicha información. Si el control del sujeto se realiza mediante otro método, es necesario declarar el campo Objeto del certificado vacío y declarar la extensión como crítica. Los detalles de los formatos soportados por esta extensión se describen en la RFC 3280 (sección 4.2.1.7).

- **Punto de distribución de la lista de revocación** (*Certificate Revocation List Distribution Point*): cuando una aplicación o el sistema operativo están configurados para comprobar la lista de revocación, la información contenida en el certificado se utiliza para localizar dónde se almacena la lista de revocación actual. La extensión **Punto de distribución de la lista de revocación** contiene una o varias URL que permiten localizar la lista de revocación actual. Podemos declarar URL que hacen referencia a los protocolos HTTP, FTP y por supuesto LDAP.

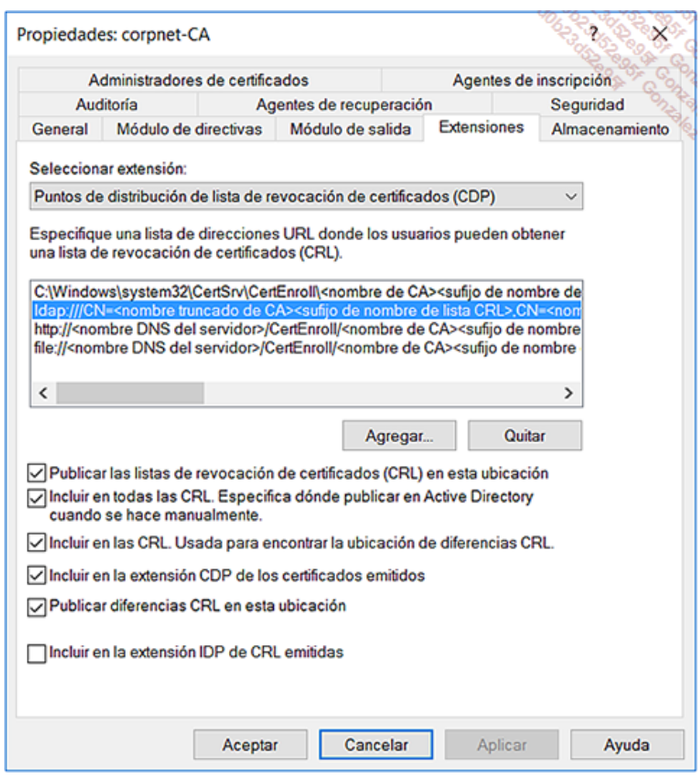
La extensión punto de distribución de la lista de revocación de certificados (DP CRL - *Certificate Revocation Lists*) indica cómo dicha lista puede ser obtenida, pero no significa que sea posible. Es importante prever la disponibilidad de las CRL en varios puntos de la red. Las RFC especifican que el nombre del punto de distribución debería utilizar un nombre de tipo X.500. En el ejemplo siguiente, el certificado de

usuario muestra que los CRL se publican en Active Directory a través de LDAP en la URL http://srvinfra-01.corpnet.priv.



El certificado contiene la lista que contiene los puntos de distribución de las listas de revocación (CRL - Certificate Revocation List)

La gestión de los puntos de distribución se lleva a cabo a nivel de la administración de la autoridad de certificación. La figura siguiente muestra las diferentes URL declaradas por defecto en una autoridad de certificación Windows Server 2016.



Configuración de los puntos de distribución en la autoridad de certificación Corpnet-CA

La consola de Administración de la autoridad de certificación integra todas las funciones de gestión de los puntos de distribución. El conjunto de opciones debe seleccionarse de manera individual para cada URL declarada.

¡Observe! Cada aplicación es libre de utilizar la lista de revocación de la autoridad de certificación. Por lo tanto, la declaración y las modificaciones de los emplazamientos de los puntos de distribución de listas de revocación pueden incidir en el proceso de validación del certificado por las mismas aplicaciones.

Configuración de los puntos de distribución: para más información sobre la configuración de los CDP, busque en el sitio de Microsoft Technet https://technet.microsoft.com " Guía de la autoridad de certificación" y "publish the CDP extension " o siga el enlace siguiente:https://technet.microsoft.com/es-es/library/hh831574(v=ws.11).aspx

3. Los certificados y la empresa

a. Relación entre los certificados y las autenticaciones

A partir del momento en que el certificado contiene elementos que permiten garantizar la identidad del sujeto, es simple autenticar a los usuarios o equipos específicos si el servidor debe efectuar el control de su acceso al igual que la confianza en la autoridad emisora de las piezas de identidad que son los certificados.

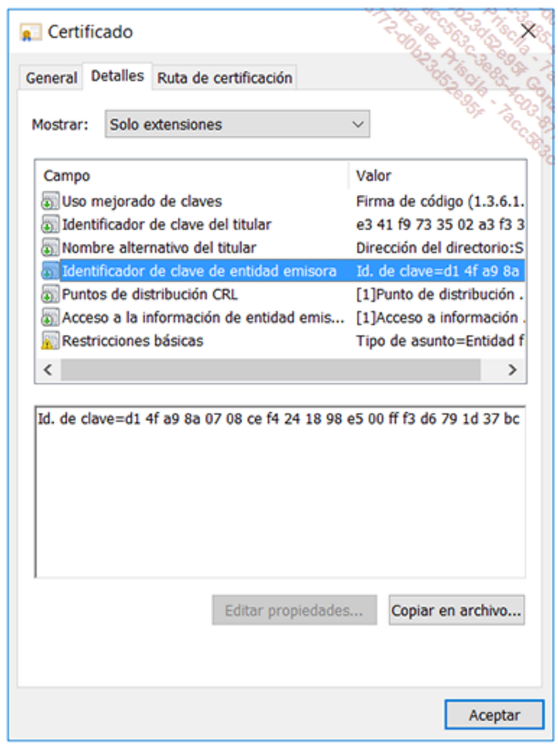
En otras palabras, el cliente posee un certificado emitido por una autoridad de certificación aprobado por sí mismo y el servidor está de acuerdo con la autoridad de certificación aprobada por el cliente. Por lo tanto, los dos asociados implicados en la operación de confianza, confían en un tercero, que en este caso es la autoridad aprobada.

Por ejemplo, cuando un servidor usa el protocolo seguro HTTPS, el servidor debe tener confianza en la autoridad de certificación raíz que haya expedido el certificado que utilizará el mismo. A partir de ese momento, el servidor acepta de forma implícita las directivas que la autoridad implementa a través del certificado. El término "directivas" significa qué los roles están soportados en realidad.

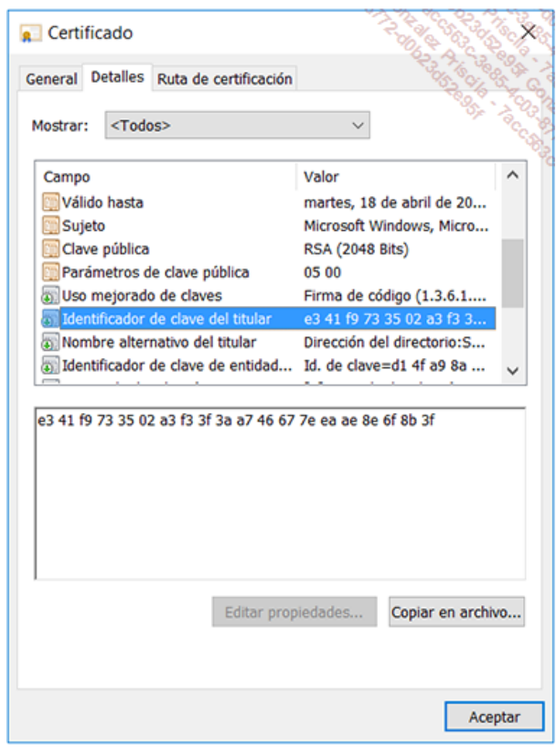
La figura siguiente muestra las directivas de un certificado utilizado para la aplicación del protocolo HTTPS en un servidor especial llamado srvinfra-01.corpnet.priv. El campo Utilización avanzada de la clave muestra que el rol del certificado permite al servidor demostrar su identidad ante el cliente. Esto puede ser el caso de una transacción bancaria: ¿estoy realmente en el servidor del banco? Sí, si el certificado lo demuestra mediante una autoridad que actúa como tercero de confianza. Puede que sí o puede que no, ¡si no existe un certificado o si el certificado es el resultado de una autoridad que no apruebo! La verdadera prueba de la relación entre el certificado instalado en el servidor Web y la autoridad que emitirá será realizado comprobando el campo identificador de clave de la autoridad situado en el certificado del servidor Web mismo. Este campo debe corresponder al campo Identificador de la clave del sujeto del certificado autofirmado de la autoridad de certificación.

En nuestro ejemplo, el ID de la clave correspondiente al campo Identificador de la clave del sujeto "e3 41 f9 73 35 02 a3 f3 3f 3a a7 46 67 7e ea ae 8e 6f 8b 3f" corresponde al identificador de la clave del sujeto del certificado de la autoridad de certificación. La confianza se verifica porque el certificado ha sido emitido por una autoridad aprobada y verificada en realidad.

La imagen siguiente muestra el rol **Autenticación del servidor**.



Rol - utilización avanzada de la clave, identificador de clave de la autoridad y modelo de certificado WebServer utilizado por el protocolo SSL



Certificado de la autoridad y valor del Identificador de la clave del sujeto

El servidor web delega entonces la verificación de la identidad del sujeto del certificado en la autoridad emisora. Esta operación se realiza con facilidad al declarar la autoridad raíz emisora como autoridad raíz de confianza. Basta para ello colocar el certificado autofirmado de la autoridad en el almacén de certificados del equipo. Por último, como podemos crear jerarquías de autoridades de certificación, las

autoridades secundarias no serán de confianza salvo que tengan una ruta de certificación válida hasta su autoridad de certificación raíz de confianza.

b. Marco de la utilización de los certificados

En la medida en que los certificados son utilizados para establecer una identidad y crear la confianza que permite una seguridad en los intercambios de datos, las autoridades de certificación podrán expedir certificados a los usuarios, a los equipos y, por supuesto, a los servicios de red tales como los protocolos IPSec o Radius (*Remote Authentication Dial-In User Service*) y también para aplicaciones tales como servidores de correo u otros servidores web. En el caso de que sea necesario un alto nivel de seguridad, los equipos deben ser capaces de controlar la identidad del otro equipo implicado en la transacción. Esta situación es idéntica de cara a las aplicaciones y usuarios. Una vez efectuada la verificación del certificado, el cliente puede "almacenar" el certificado de socio en su propio almacén de certificados, y luego usarlo para cifrar la continuación de la conversación. En este caso, el cliente usa la clave pública contenida en el certificado para cifrar una clave de sesión, la cual se utiliza para cifrar los paquetes de esta sesión. Por último, los mecanismos criptográficos ofrecidos por los certificados pueden ser utilizados para una gran variedad de funciones y aplicaciones, las cuales se presentan a continuación:

- **Utilización de firmas digitales**: las firmas digitales permiten asegurar las transacciones de Internet, y por fortuna, intranet cifrando y descifrando los mensajes, así como verificando al emisor. Además de estos mecanismos, las firmas garantizan que los datos no han sido alterados durante el tránsito.
- **Autenticación de Internet**: los certificados permiten autentificar al cliente frente al servidor y el servidor frente al cliente. Por ejemplo, una conexión segura SSL permite al cliente comprobar la identidad del servidor, controlando el certificado presentado al cliente por el servidor web.
- **Correo electrónico seguro**: los certificados permiten garantizar un alto nivel de confidencialidad y seguridad de los mensajes enviados y recibidos dentro de la mensajería corporativa y en Internet. Además el hecho de que la identidad del remitente de un mensaje pueda verificarse controlando el certificado del emisor, la integridad de los datos transmitidos, así como el no repudio de los mensajes están garantizados.
- **Autenticación por tarjetas inteligentes**: la autenticación Windows Active Directory por tarjeta inteligente, en inglés *SmartLogon*, permite al usuario abrir su sesión de dominio utilizando el certificado del representante empleando su tarjeta inteligente y el código PIN asociado. Se trata de una autenticación multifactor (dos factores), ya que el usuario debe disponer de su tarjeta inteligente, así como el código PIN para usarla. La tarjeta inteligente también sirve como almacén de certificados privilegiado, ya que en este caso, las claves privadas de los certificados no son almacenados de forma local en el disco duro del equipo, sino en la misma tarjeta inteligente.
- **Cifrado EFS**: los certificados podrán utilizarse por las operaciones de cifrado de archivos usando EFS (*Encrypted File System*). Tenga en cuenta que las autoridades de certificación de Windows Server 2003, hasta Windows Server 2016, implementan una nueva funcionalidad que permite la recuperación de las claves privadas de los usuarios. De esta forma, podemos recuperar la clave privada de un usuario a partir de la base de datos de una autoridad de certificación. Esta operación es por razones obvias de préstamo de identidad, compleja de realizar de forma tal que solo se lleve a cabo en casos de extrema necesidad. La última etapa del procedimiento consiste en importar esta clave privada archivada en un certificado de usuario para poder descifrar todos los archivos que habían sido codificados con esta clave privada. Observe que esta operación no es necesaria si los archivos están codificados bajo el control de un agente de recuperación EFS.
- **Seguridad IP** : cuando los equipos de la empresa forman parte de un dominio Active Directory, la autenticación IPSec del modo principal puede utilizar el protocolo de Autenticación por defecto Kerberos v5. En este caso, no es necesario desplegar certificados. Sin embargo, cuando los equipos no soportan Kerberos v5 o cuando los equipos están conectados a Internet y es necesario proteger las operaciones, se recomienda la autenticación por certificado.

Autenticación y protocolo IPSec: el protocolo IPSec soporta tres protocolos de autenticación. El protocolo Kerberos versión 5, los certificados X.509v3 y las claves compartidas. Esta última opción está disponible solo en el marco de la Interoperabilidad con sistemas no-Windows y el soporte de estándares y normas IPSec. La utilización de claves compartidas no se recomienda y no debe ser usada con fines de pruebas.

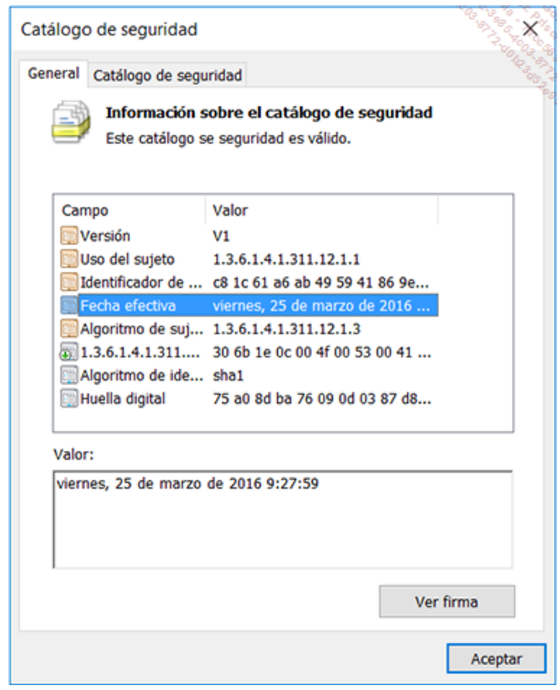
- **Authentifications IEEE 802.1X**: la utilización del protocolo 802.1x permite autenticar a los equipos y los usuarios que utilizan conexiones Wifi 802.11 así como las redes de cable de tipo Ethernet. Esta autenticación proporciona un soporte de los tipos de seguridad EAP (*Extensible Authentication Protocol*) y PEAP (*Protected EAP*) de tal manera que es posible utilizar los métodos de autenticación como los certificados.
- **Firma de los componentes de software**: la firma de los componentes de tipo controles ActiveX y applets Java y otros ejecutables y DLL protege los equipos de la instalación de componentes no autorizados. Este método utiliza la tecnología Authenticode, la cual permite a los fabricantes de software firmar sus componentes.

También es posible utilizar certificados para verificar la autenticidad del software (controles ActiveX y applets de Java, scripts, etc.) descargados a través de Internet. Esto es lo mismo durante la instalación de software y la adición de nuevos controladores de dispositivos en el sistema. Los certificados asociados a la tecnología Authenticode garantizan que el software proviene realmente de su fabricante, protegen el software contra cualquier alteración tras su publicación y aseguran la verificación y la conformidad de los controladores de dispositivos de hardware del sistema Windows.

Con respecto a la utilización de certificados con la tecnología Microsoft Authenticode: todas las DLL y Archivos centrales del sistema operativo Windows están firmados. De esta manera el componente Windows File Protection puede intervenir y restaurar la versión declarada de forma oficial en el catálogo correspondiente. En la medida que los componentes de sistema que se añaden son actualizados, nuevos catálogos (archivos con extensión .cat) se añadirán a la ubicación %SystemRoot%\ system32\catroot. Por ejemplo, la imagen siguiente muestra los detalles de un archivo de tipo Catálogo de seguridad para un componente de Windows Server 2016. Podemos comprobar más adelante en este capítulo que Microsoft firma sus propios certificados o utiliza a veces una autoridad oficial como VeriSign.

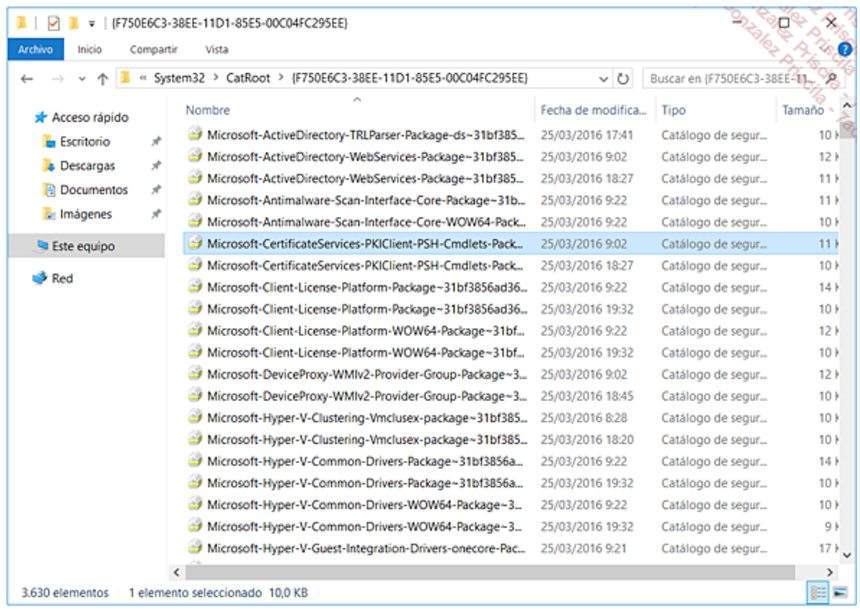
Catálogo de seguridad en Windows Server 2016

En este ejemplo, el archivo .cat de un componente del sistema indica que se utiliza a partir de su fecha efectiva.

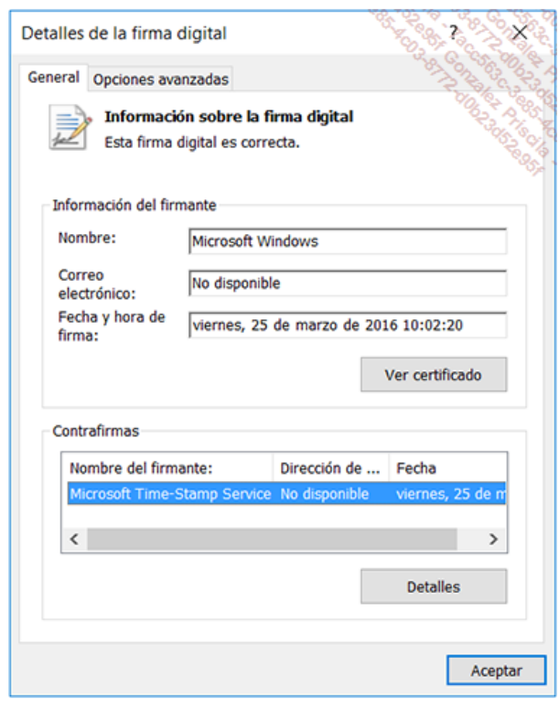


Ejemplo de archivo catálogo de Windows Server y certificado X509 de tipo V1 para la firma de los componentes de sistemas

El conjunto de los catálogos de seguridad de Windows Server se almacenan en la carpeta C:\Windows\system32\CatRoot.



Componentes de Windows y firmas de los catálogos

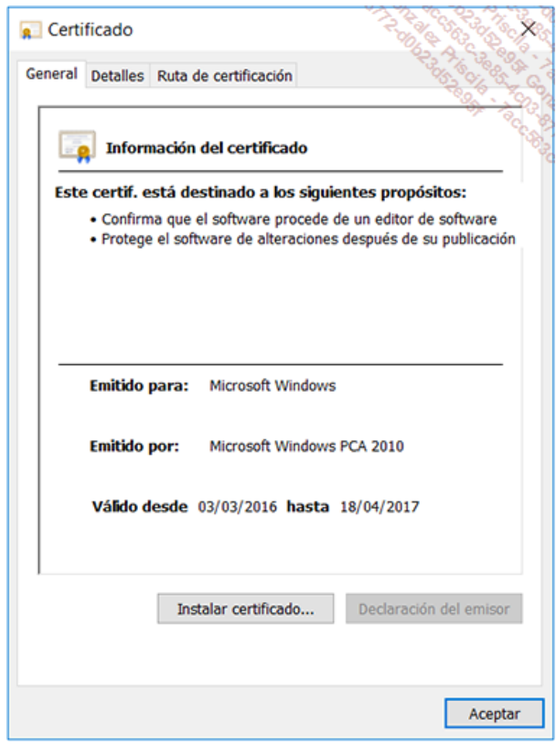


Información sobre la firma digital de un catálogo

El botón **Ver certificado** permite mostrar el certificado. Así, es posible verificar la identidad del emisor del software, es decir, Microsoft, así como el hecho de que estará protegido contra toda modificación tras su publicación. Estas funciones se declaran con el campo Utilización

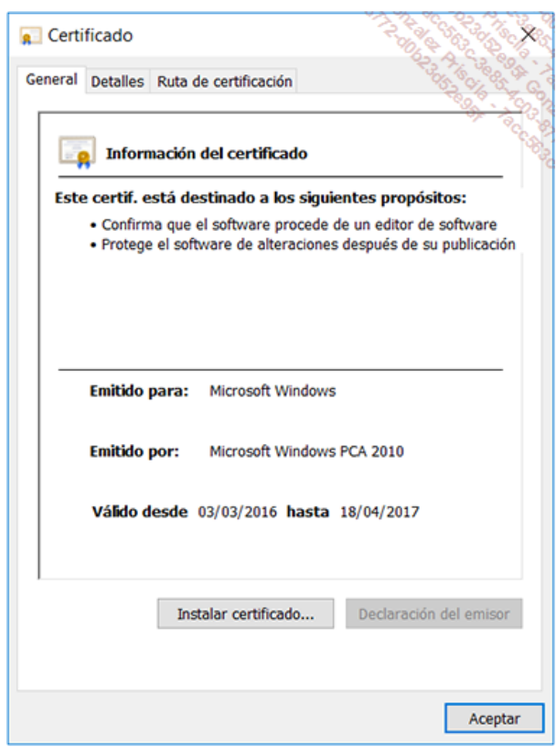
avanzada de la clave, el cual declara las funciones de firma de código y verificación de componentes del sistema Windows y firma del código a través de los OID (1.3.6.1.5.5.7.3.3) y (1.3.6.1.4.1.311.10.3.6).

Del lado de las firmas, el botón **Detalles** permite ver las características del certificado, lo que permite ver la firma de los datos con la hora en curso.



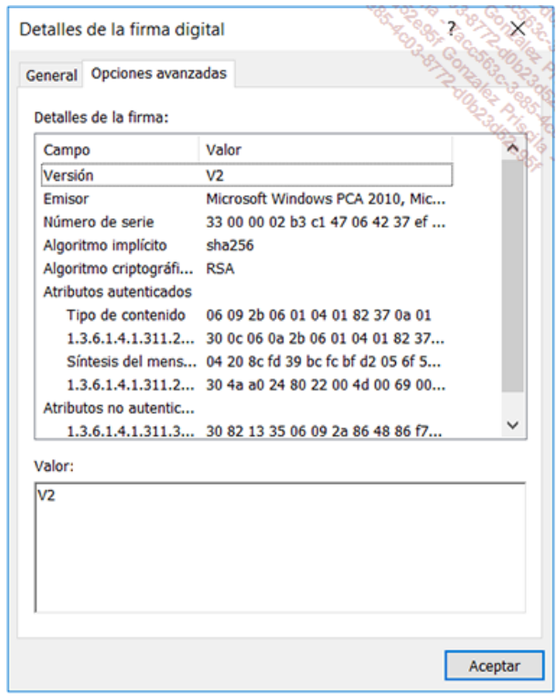
Certificado de la Autoridad Microsoft Windows PCA (Primary CA)

La figura presentada más adelante indica que las firmas utilizan como método de control el algoritmo MD5 (*Message Digest 5*) y como método de cifrado RSA. Fíjese también que las autoridades de certificación VeriSign y Microsoft implementan un enlace a la CPS (*Certificate Practice Statement*) relativa a cada uno de ellos. Así, podemos obtener todos los detalles de la política de gestión de dichos certificados. Para conseguir esto, basta con pulsar el botón **Declaración del emisor**.



Certificado de autoridad y acceso a la declaración del emisor

Por último, es importante precisar que sólo el propietario de un catálogo, por ejemplo, Microsoft o cualquier otro editor creador de catálogos registrados dentro del sistema, puede cambiar éste. De esta manera, es imposible que un tercero no autorizado pueda modificar los componentes declarados dentro de dicho catálogo.



Detalles de la firma de la Autoridad Microsoft PCA 2010

c. Utilización de certificados digitales en la empresa

En general, las empresas instalan sus propias autoridades de certificación. De esta manera, es fácil expedir certificados a los usuarios de la empresa, a los equipos y otros dispositivos específicos que deban disponer de estos para que las comunicaciones de red sean más seguras.

Cuando el tamaño de la empresa donde las exigencias y limitaciones inherentes a la expedición de certificados se imponen, es frecuente que sea necesario proceder a la implementación de varias autoridades de certificación integradas dentro de una jerarquía. El hecho de que varias autoridades se pongan en marcha implica que las entidades que utilizan los certificados podrán ser obligadas a tener varios certificados emitidos por diversas autoridades de certificación internas y también externas.

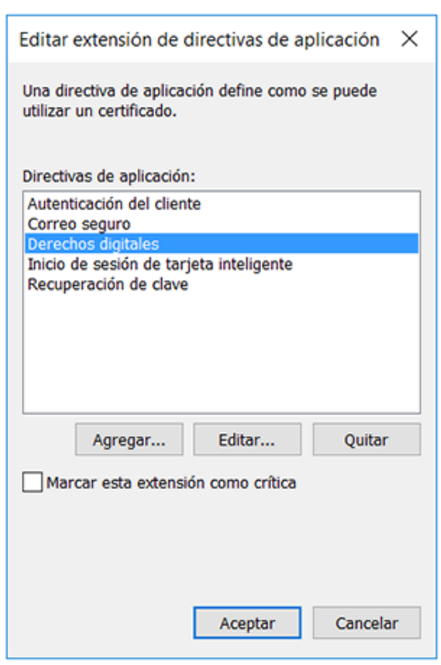
Por ejemplo, cuando un usuario de la empresa accede a la red empresarial desde el exterior a través de una conexión de tipo VPN (*Virtual Private Network*), el servidor VPN presenta un certificado de tipo servidor para probar su identidad. Como el equipo del cliente aprueba la autoridad raíz de la empresa la cual expide el certificado del servidor VPN, el equipo cliente confía en el servidor VPN.

Por último, para que el servidor VPN tenga confianza en el cliente, es necesario que éste pueda reconocer el cliente VPN antes que cualquier intercambio de datos pueda llevarse a cabo a través de la conexión virtual. Para lograrlo, deberá tener lugar un intercambio de certificados de equipo entre los dos equipos, o una autenticación de tipo usuario a través de un método de autenticación soportado por PPP (*Point-to-Point Protocol*).

A diferencia de las conexiones VPN de tipo PPTP (*Point to Point Tunneling Protocol*) las conexiones VPN que usen el protocolo L2TP (*Layer 2 Tunneling Protocol*) y el cifrado IPSec requieren certificados de tipo equipo en el cliente y en el servidor.

En este ejemplo, los certificados se utilizan para crear la confianza y establecer una comunicación segura de tipo VPN. Sin embargo, un certificado puede ser utilizado para otros usos, como por ejemplo, una autenticación para acceder a un portal seguro o el acceso al correo electrónico. Del mismo modo, un servidor puede también utilizar un certificado para varias funciones. Así, un mismo certificado puede ser utilizado para verificar la identidad de un servidor web, de un servidor de correo electrónico o de cualquier otro servicio específico.

Muchas aplicaciones utilizan el protocolo SSL 3.0 - *Secure Sockets Layer*. Este protocolo fue creado originalmente para autenticar y encriptar las comunicaciones de los servidores web, son muchas las aplicaciones que no utilizan este rol específico para utilizar solo los certificados de tipo servidor web para su propio uso. Para que sea posible asociar un rol definido utilizable por una aplicación tan específico, es indispensable que el rol se declare en las extensiones de la plantilla del certificado utilizado en el momento de la solicitud del certificado.



Ejemplo de declaración de un rol específico para una aplicación

Es por lo tanto a nivel de la autoridad de certificación que expide el certificado donde se declaran los roles. La figura muestra las funciones declaradas en una plantilla de certificado soportadas por una autoridad de certificación de tipo Raíz de empresa Windows Server 2016.

d. Certificados de usuarios

Los certificados de tipo usuario permiten la representación digital de una persona al igual que un documento de identidad como un pasaporte. Podemos adquirir certificados de una autoridad de certificación comercial como VeriSign, de tal manera que el titular del certificado tenga la posibilidad de enviar mensajes electrónicos personales cifrados a fines de seguridad, o incluso firmados digitalmente para acreditar la autenticidad. El hecho de utilizar un emitido por una autoridad oficial permite una utilización de dicho certificado por cualquier cliente que apruebe dicha autoridad oficial. Para uso interno, contamos con la posibilidad de utilizar nuestra propia autoridad de certificación dentro de la red corporativa. Muchos otros ejemplos de utilización de certificados de usuario existen tales como las autenticaciones de dominio Active Directory con tarjeta inteligente, la autenticación EAP-TLS para las conexiones VPN L2TP-IPSec, la autenticación en los sitios web de manera segura a través de SSL por certificados de tipo usuario. También se puede citar el caso de la utilización de certificados de usuario para el cifrado de archivos EFS.

En el caso del correo electrónico, el usuario tiene un certificado que podrá utilizar para firmar de forma digital un mensaje de correo electrónico. El destinatario podrá entonces comprobar que el mensaje no ha sido alterado durante su transporte y verificar la identidad del emisor. Esta última operación no será posible salvo si el destinatario aprueba la autoridad de certificación que emitió el certificado del remitente.

Queda entendido que cuando un mensaje de correo electrónico o un dato es cifrado, nadie puede leer el contenido durante el tránsito por la red. Solo el destinatario puede descifrar y leer el contenido.

La gestión de los certificados usuarios así como su uso con tarjetas inteligentes, correo electrónico y el sistema de archivos codificados EFS son tratados en detalle más adelante en este libro.

e. Certificados para los equipos

Bajo el mismo principio que los certificados de tipo de usuario, los certificados de tipo equipo constituyen una representación digital utilizable por todos los tipos de dispositivos de hardware (equipos cliente y servidores, routers, impresoras, dispositivos de red, etc.).

Los certificados utilizados por los ordenadores pueden ofrecer sus servicios al mismo dispositivo. Las plantillas de certificados ofrecidos por las autoridades de certificación de Windows Server 2003 y Windows Server 2008 proponen muchos modelos diseñados de forma específica para responder a determinados usos. Estas plantillas orientadas a equipos son presentados de forma rápida a continuación:

- **Servidor Web**: los servidores web, puede implementar la confidencialidad de los datos transmitidos cifrando las comunicaciones HTTP empleando el certificado "servidor" situado en el servidor web.
- **Servidor RAS e IAS**: dos métodos de autenticación pueden utilizar los certificados: por un lado el método EAP-TLS (*Extensible Authentication Protocol - Transport Layer Security*) y por otra parte el método PEAP (*Protected-EAP*). Ambos métodos utilizan siempre los certificados de autenticación del servidor. En función de la metodología utilizada, los certificados serán utilizados para autenticar el equipo cliente o el usuario.
- **Router** (petición sin conexión): esta plantilla de certificado podrá ser utilizada por un router en caso de solicitud SCEP (*Simple Certificate Enrollment Protocol*), emitida por una autoridad de certificación que posea un certificado de cifrado CEP.
- **Replicación de la mensajería del directorio**: esta plantilla permite la replicación del directorio Active Directory empleando mensajes electrónicos a través de SMTP.
- **Equipo**: esta plantilla de certificado permite a un equipo autenticarse en la red.
- **IPSec (petición sin conexión) e IPsec**: el protocolo IPSec utiliza certificados de equipo entre el cliente y el servidor para la autenticación. A contrario el método EAP-TLS usa un certificado de usuario proveniente de una tarjeta inteligente o del almacén de certificados local para la autenticación del usuario.
- **Cifrado CEP**: esta plantilla permite al equipo titular actuar como autoridad de registro para las solicitudes SCEP.
- **Controlador de Dominio**: esta plantilla de certificado tiene múltiples funciones utilizadas por los controladores de dominio.
- **Autenticación del controlador de dominio**: esta plantilla de certificado soporta la autenticación de los equipos y usuarios de Active Directory.
- **Autenticación del puesto de trabajo**: esta plantilla de certificado permite a los equipos cliente autenticarse en los servidores.
- **Agente de inscripción (equipo)**: esta plantilla modelo de certificado permite al equipo solicitar certificados para la cuenta de otro sujeto equipo.

Recuerde: en algunos casos, los equipos computadoras deben ser capaces de intercambiar información con un alto nivel de confianza que necesita controlar la identidad de uno o ambos participantes. Las roles soportados por los certificados dedicados a los equipos, así como el uso de extensiones soportadas por la especificación X.509 Versión 3 permiten aplicar soluciones adaptadas a estas limitaciones de seguridad.

f. Certificados para las aplicaciones

El principio de las firmas digitales y los mecanismos criptográficos está relacionado de forma estrecha con los requisitos de seguridad impuestos por las aplicaciones donde los datos son fundamentales. De hecho, en un principio, las aplicaciones soportaban estas operaciones. Hoy en día, la implementación de estos mecanismos se realiza a nivel del sistema operativo. Por ejemplo, con las plataformas Windows Server, el servicio Servicios de cifrado ofrece operaciones de cifrado y firma mejorados a las aplicaciones que necesitan proteger sus datos.

La mayoría de los clientes de mensajería permiten firmar y/o cifrar los mensajes electrónicos. Es por supuesto el caso de las aplicaciones como Microsoft Outlook. Los servicios de cifrado básicos integrados en la familia de los sistemas operativos Windows Cliente desde Windows XP hasta Windows 10, están directamente expuestos a nivel de la shell de Windows Explorer. Los archivos relacionados con los certificados, así como las operaciones de manipulación de los certificados están disponibles de forma directa a partir de la línea de comandos, de la consola de gestión de MMC, así como del escritorio de Windows, para todas las aplicaciones que utilicen los servicios de cifrado

El comando Certreq.exe es una herramienta de línea de comandos que viene con los sistemas operativos Microsoft cliente y servidor -sin incluir a Windows XP. Observe que este comando es compatible tanto con Windows XP como con Windows Server 2003 y que puede ser todavía utilizado en las operaciones de gestión de certificados tanto de usuario como de equipo. Empleando este comando, tendremos la posibilidad de someter, recuperar, crear y aceptar las solicitudes de certificados enviadas a una autoridad de certificación Windows Server 2003 hasta Windows Server 2016. También es posible utilizar el comando Certreq dentro de scripts para automatizar las solicitudes de certificados o realizar ciertas operaciones engorrosas.

Para más información sobre el comando Certreq, busque "Command-Line Reference" en el sitio Microsoft Technet en la dirección https://technet.microsoft.com o use el vínculo https://technet.microsoft.com/en-us/library/cc754340(v=ws.11).aspx.

4. Almacenamiento de los certificados

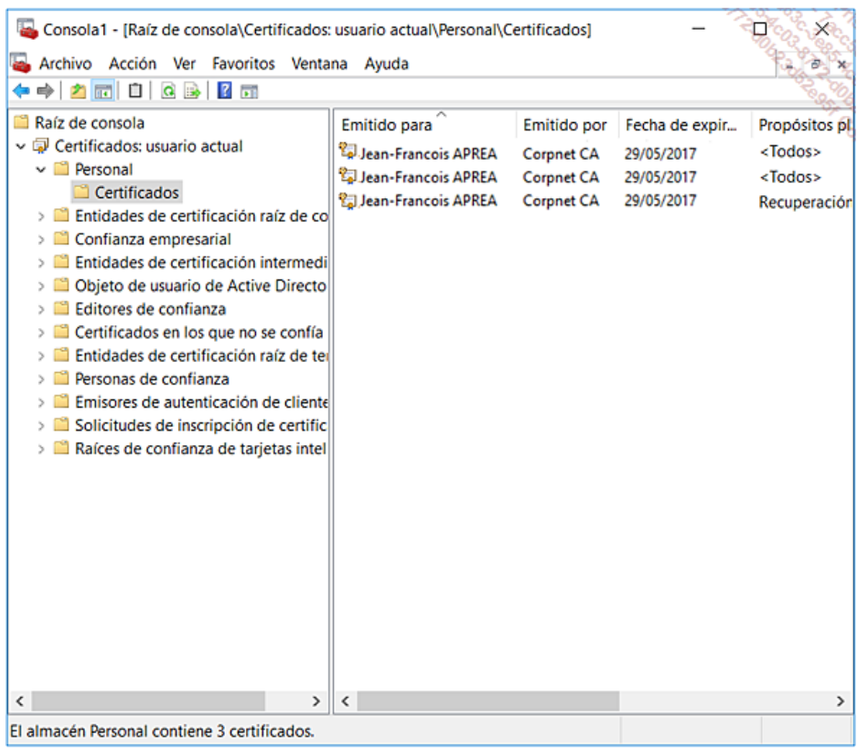
a. Introducción

El soporte de los certificados está integrado de forma muy estrecha dentro del sistema operativo Windows, es fundamental comprender donde se almacenan de forma real los datos numéricos relativos a los certificados X.509 v3. En sistemas Windows y en particular en los sistemas de la familia Windows Server los certificados se almacenan, gestionan y protegen por un componente llamado Almacén de certificados. Además de los certificados utilizados por el equipo y el usuario, el Almacén de certificados integrado en el sistema operativo soportará otros elementos indispensables, por ejemplo las listas de aprobación de certificados (*Certificate Trust Lists* - CTL), las listas de revocación de certificados (*Certificate Revocation Lists* - CRL), así como las listas de revocación de certificados de tipo Delta (Delta CRL).

El almacenamiento de los certificados se hará cargo del contexto de los certificados de los usuarios y en concreto del usuario en sesión. De esta manera las claves privadas de los certificados de un usuario no podrán ser utilizadas por otro usuario con una sesión en el mismo equipo. Por último, el equipo mismo y cada servicio de Windows que utilice uno o varios certificados tendrá su propio almacén de certificados. Este sistema de almacenamiento seguro permite garantizar una "estanqueidad" total de las claves privadas relacionadas con cada certificado entre las distintas entidades que puedan utilizarlos.

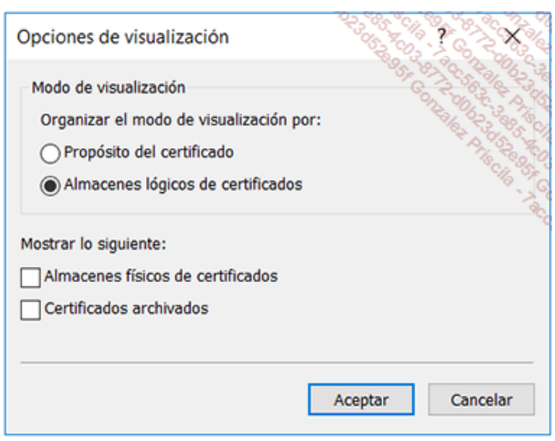
b. Almacenamiento de certificados e interfaz CryptoAPI

La interfaz de programación CryptoAPI incorpora todas las funciones de gestión de los certificados. Cualquier equipo o usuario puede solicitar de forma sencilla, almacenar, buscar y verificar los certificados.



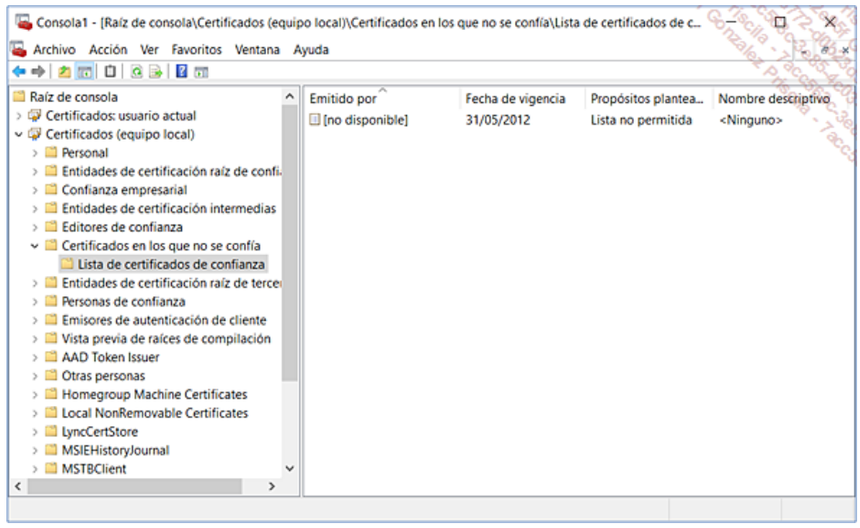
Almacén de certificados

La figura ilustra los almacenes de certificados del equipo local y del usuario en sesión en el equipo, los cuales ofrecen una visión lógica y una clasificación en función de la naturaleza y de la fuente de la información presentada. También es posible cambiar la interfaz de la consola de gestión de certificados para que ésta nos presente una visión física de los almacenes de certificados. Las distintas opciones de visualización permiten también ordenar los certificados que se muestran según su tipo de uso (por ejemplo, autenticación del cliente y usuario de seguridad IP).



Opciones de visualización de los almacenes de certificados

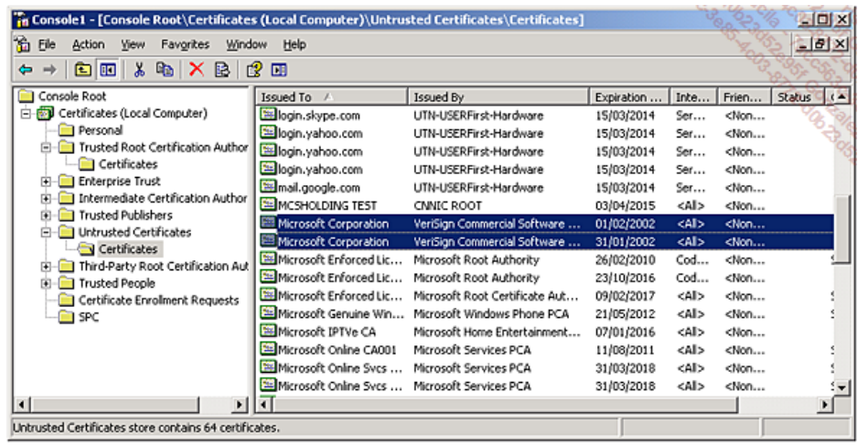
La figura siguiente destaca el almacenamiento y el control de los parámetros presentados. Así, cuando la opción **Almacenes físicos de certificados** se activa para el componente de administración de la Consola MMC **Certificados - Usuario actual**, la interfaz gráfica muestra las categorías **registro**, la **directiva de grupo** y el **equipo local**.



Lista de certificados no autorizados y almacenes

En este ejemplo, dos certificados no autorizados y obtenidos de forma fraudulenta son mostrados en el epígrafe **Certificados no autorizados**, poniendo de relieve el hecho de que están almacenados en el equipo local, y no en otro lugar.

En marzo de 2001, la empresa VeriSign, anunció que había sido atacada y que, en efecto, había emitido dos certificados digitales de VeriSign de tipo "Class 3 code-signing" a un individuo que había pretendido de forma fraudulenta ser un empleado de Microsoft. Este problema de seguridad ha sido objeto de un boletín de seguridad (MS01-017) cuyo impacto ha sido importante, ya que un hacker tenía la posibilidad de firmar digitalmente el código utilizando el nombre "Microsoft Corporation". Este boletín está disponible en la dirección https://technet.microsoft.com/library/security/ms01-017.



Visualización de los almacenes de certificados físicos

VeriSign por supuesto, revocó sus dos certificados y procedió a la actualización de la lista de revocación de certificado VeriSign (CRL) en Internet. Sin embargo, ya que los certificados de firma de código VeriSign no indican ningún punto de distribución de la lista de revocación, solo se puede utilizar el mecanismo de verificación basado en el uso de la CRL. Para remediarlo, Microsoft publicó una actualización de seguridad que corrige este defecto. El parche incorpora una lista de revocación declarando los dos certificados como fraudulentos, así como un módulo para consultar de forma directa el CRL a partir del equipo local y no en Internet.

La interfaz gráfica de Microsoft Internet Explorer también permite consultar el almacén de certificados usando el botón **Certificados** situado en **Opciones de Internet - Contenido**.

c. Visualización de los certificados: almacén lógico y almacén físico

Cuando examinamos el contenido de un almacén de certificados en el modo de almacén lógico, podemos encontrar dos copias del mismo certificado. Esta situación se produce porque el mismo certificado se almacena en los almacenes físicos diferentes agrupados en un mismo almacén lógico. Cuando el contenido de los distintos almacenes de certificados físicos se combina en un único almacén lógico, se muestran todas las instancias de un mismo certificado.

¿Cómo realizar una verificación? Para lograrlo, definimos la opción de visualización que permite ver los almacenes de certificados físicos. El certificado figura en los almacenes físicos diferentes que dependen del mismo almacén lógico. Compare los números de serie de los dos elementos. Si se trata del mismo certificado mostrado dos veces, el número de serie será el mismo. El componente de software Certificados nos permite mostrar los certificados en función de su almacén lógico o de su función. Del mismo modo, si está visualizando los certificados según su función, un certificado que cumple varias aparecerá en cada carpeta que define uno de estos roles.

d. Almacenamiento local de certificados expirados

Los equipos Windows Server en todas las versiones de Windows disponen de un mecanismo interno de archivo y de renovación automática de certificados y las claves privadas asociadas. Estas características permiten garantizar la correcta utilización de los certificados en el tiempo. En efecto, la función de archivo es en especial importante ya que permite al usuario ser capaz de descifrar los documentos que hacen referencia a los certificados expirados o que hayan sido objeto de una renovación de la clave privada.

Por defecto, los certificados archivados no aparecen. Para mostrar los certificados archivados en la consola MMC, active la opción **Certificados archivados** situada en las **Opciones de visualización - Mostrar los elementos siguientes**.

e. Estructura de almacenamiento del almacén lógico de certificados

La utilización de almacenes lógicos de certificados elimina la necesidad de almacenar varias veces algunos elementos manipulados por más de una única entidad. De hecho, algunos datos tienen un carácter común y deben ser compartidos. Por ejemplo, los certificados de las autoridades de certificación raíz de confianza y las listas de revocaciones son elementos útiles para los usuarios, equipos y también los servicios asociados al equipo.

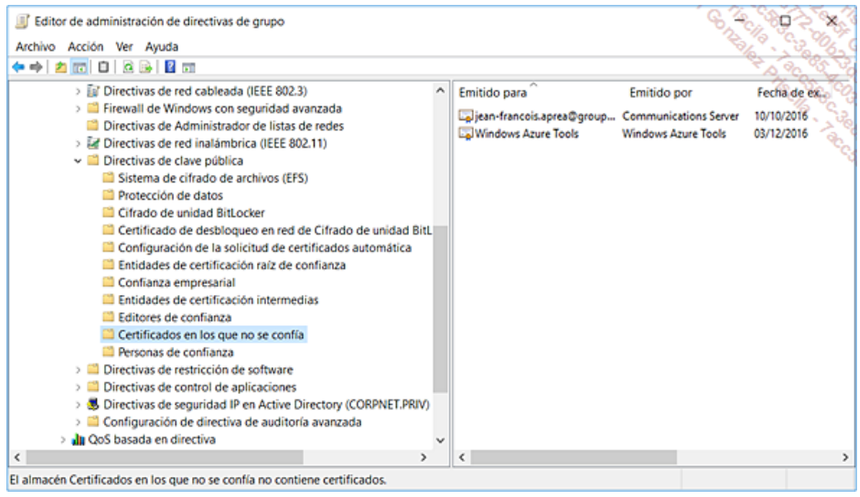
Sin embargo, algunos certificados o listas de certificados de confianza (CTL) o listas de revocación de certificados (CRL) solo deben estar disponibles para algunos usuarios. Cuando un certificado o bien una lista de revocación se almacena en el almacén del usuario, estos elementos no son accesibles al equipo mismo o a cualquier servicio del equipo.

Desde un punto de vista visual, cuando los parámetros tales como los CTL se distribuyen a través de directivas de grupo de Active Directory, entonces los datos aparecen en la consola dentro de una carpeta llamada **Directiva de grupo**.

Con respecto a la aplicación de los parámetros empleando objetos GPO: cuando los parámetros son colocados en la parte**Configuración del equipo** de la directiva de grupo, estarán disponibles para el equipo pero también todos los usuarios del equipo mientras que si se trata de la parte de **Configuración del usuario**, los parámetros solo serán accesibles a los usuarios afectados por la aplicación de la directiva de grupo.

Los almacenes lógicos de certificados incluyen las siguientes categorías para las entidades de tipo usuarios, equipos, y servicios:

- **Personal (Personal)**: el contenedor contiene los certificados de usuario, el equipo o el servicio actual. Cuando una autoridad de certificación de empresa emite un certificado a un usuario, entonces el certificado se colocará en el almacenamiento personal de este usuario. Técnicamente, el certificado se almacena en el perfil de usuario (sin la clave privada). Las claves privadas se almacenan en una zona segura del registro.
- **Autoridades de certificación raíz de confianza** (*Trusted Root Certification Authorities*): el contenedor contiene los certificados autofirmados de las autoridades raíz. Los certificados que disponen de una ruta de certificación hasta un certificado de la autoridad raíz son aprobados por el equipo para todos los roles válidos del certificado. Observe que los certificados de las autoridades no raíz también pueden ser colocados en esta ubicación, que se denomina a menudo "Almacén de raíces". Dichas autoridades podrán ser las autoridades de certificación Windows internas o también las autoridades de certificación externas a la empresa.
- **Confianza de empresa** (*Enterprise Trust*): el contenedor contiene los CTL (*Certificate Trust Lists*). Una CTL es una lista firmada que contiene los certificados de las autoridades de certificación aprobados. Todos los certificados que disponen de una ruta de certificación a una CTL serán aprobados por el equipo en función de los roles especificados en el CTL.
- **Autoridades intermedias** (*Intermediate Certification Authorities*): el contenedor contiene los certificados de las autoridades de certificación que no son las autoridades de certificación raíz de confianza. Por ejemplo, los certificados de las autoridades de certificación subordinadas serán colocados en este contenedor. Esta ubicación también contiene las listas de revocación que serán utilizadas por los usuarios, el equipo local, al igual que los servicios.
- **Objeto usuario Active Directory** (*Active Directory User Object*): este contenedor incluye los certificados de usuario que se publican en los servicios de directorio Active Directory. Tenga en cuenta que este almacén solo aparece para los usuarios y no para los equipos o servicios.
- **Editores aprobados** (*Trusted Publishers*): el contenedor incluye los certificados emitidos para las personas o entidades expresamente autorizadas. En general, se trata de certificados autofirmados o certificados aprobados por una aplicación como Microsoft Outlook. También puede tratarse de los certificados que representan a los fabricantes de software. Estos certificados son utilizables para la verificación del código firmado empleando la tecnología Authenticode.
- **Certificados no autorizados** (*Disallowed Certificates*) : el contenedor contiene los certificados a los que el usuario y/o el equipo no otorgará su confianza. También es posible restringir el uso de determinados certificados declarando la información en una directiva de restricción de software.



Objeto directiva de grupo, Directiva de clave pública y certificados no autorizados

- Otro método consiste en denegar de forma explicita su confianza en el certificado durante su validación cuando la aplicación lo propone.

La presencia de este contenedor es consecuencia del robo de dos certificados de Microsoft en el proveedor de certificados VeriSign.

- **Personas autorizadas** (*Trusted People*): este contenedor incluye los certificados emitidos por los usuarios o las entidades aprobadas de forma explícita.
- **Otras personas** (*Another People*): este contenedor incluye los certificados emitidos por los usuarios o las entidades aprobadas de forma implícita. Estos certificados deben formar parte de una jerarquía de autoridades de certificación aprobados. En general, se trata de certificados utilizados por las funciones de seguridad como el cifrado y descifrado de datos empleando EFS (*Encrypting File System*) o la mensajería electrónica segura S/MIME.
- **Solicitud de inscripción de certificado** (*Certificate Enrollment Requests*): el contenedor permite ver las solicitudes de certificados esperando ser procesados o rechazados. Puede contener archivos de solicitud de certificados, los cuales se crean cuando las solicitudes están sujetas a una autoridad de certificación autónoma o cuando una autoridad de certificación de tipo empresarial no está operativa.

Con respecto a la gestión del contenido de los almacenes de certificados: la ubicación física de un certificado se determinará de forma automática en función de sus características. Será pues siempre almacenado de forma local y a menudo en el directorio Active Directory, aparte de la clave privada que como su nombre indica, debe seguir siendo privada y sólo a disposición del sujeto. Por defecto, la consola de administración de los certificados muestra una vista lógica de los certificados muy práctica que no requiere la visualización de los lugares físicos. Observe sin embargo que para resolver posibles problemas, puede ser muy útil activar la visualización de los almacenes físicos.

f. Origen de los certificados guardados en los almacenes

Los certificados que se encuentran en los almacenes de certificados pueden provenir de cuatro fuentes principales, las cuales se presentan a continuación:

- El certificado se emite durante el proceso de instalación del sistema operativo Windows cliente o Windows Server. Los certificados utilizados reflejan la identidad de la empresa Microsoft, así como las de sus asociados.
- Una aplicación web inicia una sesión SSL. En virtud de esta sesión segura y una vez establecida la relación de aprobación, un certificado se almacena en el equipo.
- El usuario acepta de forma implícita un certificado. Esto puede ser el caso de la instalación de un software, durante la recepción de un mensaje de correo electrónico cifrado o firmado digitalmente.
- Un usuario solicita de forma expresa un certificado a una autoridad de certificación para acceder a recursos específicos de una organización.

A medida que los usuarios y los equipos utilizan aplicaciones que requieren certificados (conexiones de Internet, autenticaciones fuertes, etc.), nuevas entradas aparecen en el almacén de certificados de los equipos y usuarios.

g. Protección y almacenamiento de claves privadas

El almacenamiento de claves privadas es un tema fundamental que afecta a todos los sistemas implementan de cerca o lejos, los certificados X.509 Versión 3 y los servicios ofrecidos por la infraestructura de claves públicas. El no tomar en cuenta esta problemática hace ineficaces los altos niveles de protección y seguridad que ofrecen. En efecto, es como si las llaves de una cámara acorazada no fueran mantenidas en un lugar seguro, lo que, por supuesto, ¡es en parte paradójico!

También hay que poner de relieve el hecho de que cualquier persona (o proceso) que pueda obtener y utilizar de manera ilegal una clave privada usurpa de hecho la identidad del propietario real de la clave. La persona puede utilizarse para descifrar los datos cifrados en base a la clave pública del propietario y también para firmar todos los tipos de datos soportados. Una vez más, hay usurpación de identidad del verdadero poseedor de la clave privada. Por todas estas razones, es fundamental que las claves privadas estén "almacenadas" en lugares protegidos de tal modo que sólo las personas autorizadas puedan acceder a ellos.

Por lo general, la protección de las claves privadas es por supuesto soportada por el sistema operativo a través de mecanismos de protección de las zonas de memoria que contienen las claves y el código durante el funcionamiento. Sin embargo, un hacker puede atacar al sistema operativo, provocar un incidente importante para luego explotar la información contenida en un volcado de memoria.

Por supuesto, también es posible atacar de forma física a un equipo situado en una zona con accesos poco o nada controlados. En este caso, resulta fácil para un hacker reiniciar el equipo desde un CD-ROM, una llave USB o cualquier otro medio y utilizar herramientas de bajo nivel para localizar y tratar de descifrar las claves privadas. El almacenamiento de copias de seguridad, que contienen las claves privadas que se almacenan en el disco duro, es, desde este punto de vista, un tema al que también hay que prestar atención.

Almacenamiento de claves y externalización del almacenamiento de copias de seguridad: en la mayoría de los casos, los sistemas más sensibles son objeto de procedimientos de acceso físico regulados muy restrictivos. Las salas de informática están equipadas con sistemas de control de acceso, los racks que contienen los servidores pueden estar provistos de cerraduras reforzadas, etc. La virtualización de servidores los protege y de esta manera, es poco probable que un ataque físico pueda llevarse a cabo. Sin embargo, ¿que podemos decir de los respaldos? Este punto es importante porque quizás es más fácil para el hacker acceder al sistema de copias de seguridad y exportar una o varias VM en un medio extraíble. Bastará luego restaurarlos fuera de la red de producción para, con toda tranquilidad, romper la seguridad del sistema y recuperar las claves que allí se almacenan. Una vez obtenidos estos datos, las claves pueden ser utilizadas ilegalmente.

Para proteger el lugar donde residen las claves privadas, hay que almacenar éstas fuera del entorno del equipo y del sistema operativo. La instalación de un dispositivo de tipo tarjeta inteligente lo permite. Las claves privadas son protegidas, ya que ninguna de ellas reside en el equipo, y ni siquiera en la memoria RAM, que está bajo el control del sistema operativo subyacente.

Las recomendaciones presentadas a continuación nos permitirán poner en marcha un entorno adecuado para garantizar una buena protección de las claves privadas.

- Hay que asegurarse de que los equipos que contiene las claves privadas en particular sensibles residen en un entorno seguro tanto desde un punto de vista físico, de forma local en un equipo determinado, como en la red. Por ejemplo, el alojamiento de un sitio de comercio electrónico, cuya seguridad depende en gran parte de la clave privada asociada al certificado del servidor, debe tratarse de manera especial.
- Se recomienda implementar dispositivos de almacenamiento de claves privadas. Una clave privada puede ser almacenada en una cabina externa codificada. En caso de fallo del sistema, de volcado de memoria o de ataque en red del servidor, no habrá ningún acceso posible a las claves privadas, ya que éstas estarán situadas fuera del servidor, y nunca en la memoria del sistema.

Es necesario ofrecer el mejor nivel de seguridad a los sistemas que hacen uso de claves privadas sensibles en particular. Por ejemplo, el caso de una autoridad de certificación raíz es un caso donde es frecuente que el equipo de este servicio esté internado en un lugar muy seguro, pero también desconectado de la red de producción. En este caso, se hablará de una autoridad de certificación raíz en modo desconectado -en inglés, Offline Root CA.

Recuerde que la pérdida o amenaza de una clave privada puede tener un impacto que variará en función de la importancia de ésta. Así, una persona que disponga de la clave privada de otra persona tendrá la oportunidad de descifrar todos los mensajes codificados en base a la clave pública asociada -en este caso concreto, la del destinatario. Además, la clave privada en cuestión podrá también ser utilizada para firmar los mensajes o datos "en nombre" del verdadero sujeto. Este último caso pone de relieve la usurpación real de la identidad del sujeto.

5. Consola de gestión MMC de certificados

El componente de Certificados permite gestionar los certificados para los usuarios, equipos o servicios. Nos permite solicitar nuevos certificados a las autoridades de certificación empresariales que funcionen en todas las versiones de Windows Server. Además, los usuarios pueden buscar, visualizar, importar y exportar certificados a partir de los almacenes de certificados. Sin embargo, en la mayoría de los casos, los usuarios no tienen que gestionar de forma personal sus certificados ni sus almacenes de certificados. Esta operación puede ser efectuada por los administradores, por los parámetros de la directiva de grupo y a través de programas que utilizan los certificados.

Los administradores son los principales usuarios del componente Certificados, y como tales son capaces de realizar una variedad de tareas de gestión de certificados en su almacén de certificados personal así como en los almacenes de certificados de cualquier equipo o servicio para el que tengan permisos de administración.

6. Evolución de las interfaces criptográficas de Windows

Los sistemas Windows incorporan varias interfaces de programación criptográficas. Estas interfaces están dentro de los mecanismos de seguridad del sistema y las aplicaciones que utilizan estos servicios. A continuación se presentan en forma condensada:

a. Interfaz CNG (Cryptographic API Next Generation)

La interfaz CNG es la interfaz de programación que sustituye a la interfaz CryptoAPI a largo plazo a partir de los sistemas operativos Windows 7 hasta las versiones posteriores, tales como Windows 10 y Windows Server 2016. Los mecanismos criptográficos han avanzado mucho en los últimos años, siendo necesario definir una nueva interfaz más extensible y más duradera.

Las características principales de la interfaz CNG son las siguientes:

- CNG permite a los desarrolladores implementar sus propios algoritmos criptográficos.
- CNG soporta la ejecución en modo kernel. De hecho, la misma interfaz de programación está disponible en modo usuario y en modo kernel. De esta manera, los protocolos SSL e IPSec pueden funcionar en modo kernel para el arranque de los procesos basados en la interfaz CNG.
- CNG está en curso de evaluación para obtener la certificación FIPS 140-2 - (*Federal Information Processing Standards*), así como la evaluación Common Criteria sobre las plataformas seleccionadas (mecanismos de aislamiento fuerte y funciones de auditoría).
- CNG es compatible con todos los algoritmos incluidos en la interfaz CryptoAP 1.0. Microsoft ha definido que todos los algoritmos soportados via CryptoAPI 1.0 serán soportados con la nueva interfaz CNG.
- CNG proporciona el soporte de los algoritmos ECC (*Elliptic Curve Cryptography*) Suite B, necesarios para las limitaciones de seguridad del gobierno estadounidense (Algoritmos ECC (ECDH, ECDSA), curvas P-256, P-384 y P-521 y condensados SHA-2 (256, 384, 512).
- Otro punto importante se refiere a la gestión de las tarjetas TPM soportadas por Windows tanto en los sistemas operativos cliente como en los sistemas de la familia Windows Server. CNG soporta el almacenamiento y aislamiento de las claves, funcionalidad necesaria para soportar las tarjetas TPM (*Trusted Platform Module*).

¡Observe! La interfaz CNG utilizada por las entidades de certificación Windows Server 2008 y las versiones posteriores permite a los protocolos como IPsec y SSL utilizar algoritmos criptográficos personalizados. Aunque no sea hoy frecuente utilizar estos Algoritmos criptográficos, tenga en cuenta que para su uso es indispensable que la autoridad de certificación y las aplicaciones soporten ECC, o cualquier otro algoritmo implementado a través de la interfaz CNG. Por su parte, la autoridad de certificación Windows Server debe ser capaz de emitir y gestionar los nuevos tipos de certificados, y por otra, las aplicaciones deben ser capaces de utilizar las claves generadas empleando estos nuevos algoritmos.

Los algoritmos de tipo ECC de la Suite B solo son soportados por los sistemas Windows 7 y versiones posteriores. Los antiguos sistemas Windows XP y Windows Server 2003, deberán seguir utilizando los algoritmos RSA. Es importante señalar que los sistemas Windows 7,Windows Server 2008 R2 y versiones posteriores podrán utilizar simultáneamente la antigua interfaz criptográfica CryptoAPI y la nueva interfaz CNG.

Servicios de certificados de Windows Server 2016

1. Introducción

Las tecnologías criptográficas y los servicios de certificados fueron considerados temas muy importantes en las primeras versiones de Windows NT.

La primera aplicación de los servicios de certificados estuvo disponible para Windows NT Server en su versión 4.0 SP2 con el paquete Windows NT Opción Pack. Esta primera versión, aunque básica, permitía a los administradores NT generar certificados X.509v3 para aplicar el cifrado HTTPS a través de SSL, mensajería electrónica segura a través del protocolo S/MIME y la creación de aplicaciones seguras específicas.

Luego, los servicios de certificados incluidos en la familia Windows Server son un avance significativo. En efecto, las autoridades de empresa que funciona en todas las versiones de Windows Server pueden ser integradas en los servicios de directorio Active Directory. Esta relación con los servicios de directorio LDAP y los servicios de seguridad Kerberos permite a los equipos Windows autenticados mediante el protocolo Kerberos utilizar servicios sofisticados como la inscripción automática de los certificados para los equipos y también los usuarios. Por último, las autoridades de certificación Windows soportan los principios de arquitectura propios de las autoridades de certificación de claves públicas, posibilitando así la creación de jerarquías de autoridades con o sin integración en Active Directory.

A partir de Windows Server 2008 R2 y hasta Windows Server 2016, la administración Windows Server permite a los administradores de empresas de cualquier tamaño disponer de toda la granularidad de administración que pueden desear. Más allá de la capacidad de delegación propias de las autoridades de certificación de Windows Server, una de las operaciones más interesantes permite a los administradores delegar en un tercero la autorización de validar las solicitudes de certificados solo para determinados usuarios o grupos de usuarios. Esta posibilidad permite delegar la validación de ciertos tipos de certificados a los responsables de esta delicada tarea. Esto podrá, por ejemplo, ser el caso de un jefe de departamento de cara al permiso para conceder a las identidades aprobadas en la base de certificados emitidos específicamente para tal o cual aplicación de negocio.

Por último, entre las funciones ofrecidas por las autoridades Windows Server, es importante señalar los puntos siguientes:

- La gestión de certificados empleando plantillas totalmente personalizables.
- La gestión del archivo y recuperación de claves privadas de forma centralizada.
- La inscripción automática de certificados para los usuarios que utilizan equipos de trabajo Windows XP Professional y Windows Vista miembros de un dominio Active Directory.
- La puesta a disposición de las listas de revocación de certificados de tipo delta para todas las aplicaciones que utilizan la interfaz CryptoAPI disponible en todas las plataformas Windows. Esta nueva funcionalidad permite publicar las listas de revocación de certificados en base a deltas. Este método minimiza el tráfico de red, reduciendo el número de descargas de listas de revocación de certificados demasiado largas. El puesto cliente descarga la lista delta más reciente y la asocia a la última lista de base para disponer de una lista completa.
- El soporte de las certificados cruzados, las cuales permiten establecer relaciones de confianza entre las autoridades de certificación que pertenecen a jerarquías de aprobación separadas para permitir a un certificado ser utilizado en las jerarquías de certificación diferentes a la de origen.
- El soporte de la subordinación cualificada. Esta posibilidad permite imponer limitaciones de emisión de certificado a las autoridades de certificación subordinadas. Es posible imponer restricciones para el uso de los certificados expedidos por las autoridades limitando así el poder de las autoridades de certificación subordinadas en función de las necesidades.
- La separación de roles. Esta nueva funcionalidad prohíbe que un usuario realice una operación de administración de una autoridad de certificación si tiene más de un rol en dicha autoridad. De esta manera, la posible implicación de la cuenta en cuestión no podrá poner en peligro el conjunto de la Autoridad.
- La auditoría de los eventos. Esta opción, que apareció de forma inicial con las autoridades de certificación Windows Server 2003 Enterprise y Datacenter Edition, hoy está disponible en todas las versiones de Windows Server. Permite registrar todos los eventos relativos a la actividad de la autoridad de certificación y en particular el seguimiento de las operaciones críticas como la emisión de certificados o el cambio de roles.

El conjunto de estas funcionalidades se presenta y comenta más adelante, así como las nuevas funcionalidades de los servicios de certificados de Windows Server 2016.

2. ¿Por qué utilizar una AC Microsoft Windows Server en lugar de otra?

Los servicios de certificados incluidos en Windows Server ofrecen muchas ventajas que interesarán en más de un aspecto a los administradores de infraestructuras seguras Windows.

- Las entidades de certificación Microsoft son flexibles. En efecto, una entidad de certificación Windows Server puede instalarse de dos maneras: en modo "autónomo" o en modo "empresa". Estos dos tipos de configuraciones permiten cubrir todos los escenarios empresariales, teniendo en cuenta que la principal característica de las entidades de tipo empresa es aprovechar la integración de Active Directory, del detalle de personalización de las plantillas de certificados y los mecanismos de inscripción automático y renovación de certificados. Por último, el despliegue de una arquitectura de servicios de certificados Microsoft aprovechará las inversiones técnicas y hardware relacionados con la infraestructura de Active Directory, así como el inmenso ecosistema propio de los entornos Microsoft.

Entidades de certificación de Microsoft y ecosistema: la adopción generalizada de los servicios de dominio de Active Directory en las empresas, y principalmente las Fortune 500, llevó a la adopción de muchas tecnologías relacionadas. Con respecto a los servicios de certificados, encontramos a los principales jugadores, como Citrix y Gemalto. Para el primero, la solución de gestión de dispositivos BYOD Citrix XenMobile permite la inscripción automática de certificados para dispositivos móviles Andoid, iOS y Windows Phone, mientras que el segundo permite la creación de una solución de autenticación multifactor basada en la inscripción de los certificados de usuario en tarjetas inteligentes GEMALTO e incluso la utilización de una autenticación biométrica.

- Las AC de Microsoft son interoperables. Microsoft es un miembro activo de los diferentes grupos de trabajo dedicados a las PKI existiendo muchos acuerdos entre Microsoft y otros fabricantes de soluciones criptográficas. De hecho, los servicios de certificados Microsoft soportan la mayoría de los algoritmos criptográficos (RSA (*Rivest Shamir Adleman*), DSA (*Digital Signature Algorithm*), RC4 (*Rivest Cipher 4*), AES (*Advanced Encryption Standard*), así como los estándares relativos a la infraestructura de claves públicas tales como las publicaciones IETF PKIX (*Public Key Infrastructure X.509 Working Group*), y los formatos ITU-T X.509 y PKCS (*Public Key Cryptography Standards*). El soporte de estas normas es fundamental para exportar o importar certificados hacia o desde archivos PKCS #12 y PKCS #7, así como los archivos de certificados binarios codificados a través del formato X.509.
- Las AC de Microsoft ofrecen un rendimiento muy alto. Los laboratorios de Microsoft han demostrado que una sola autoridad de certificación Windows Server, podría emitir más de treinta millones de certificados a un ritmo superior a cincuenta certificados por segundo. Esta gran rendimiento se explica por el hecho de que los servicios de certificados interactúan con una base de datos utilizando el motor ESE (*Extensible Storage Engine*), ya utilizado con los servicios de dominio Active Directory, y también los bancos de información Exchange Server.

Importancia del criterio de resultados: la primera función de una autoridad de certificación es la de tramitar las solicitudes de certificados emitidos por los usuarios, los equipos, dispositivos o aplicaciones. Este tratamiento consiste en aceptar o rechazar las solicitudes de certificados, así como garantizar las funciones de gestión de certificados, como la renovación o la revocación. Las autoridades de certificación son también responsables de la publicación de las listas de revocaciones básicas y las listas de revocación delta, que también requieren un nivel de disponibilidad y rendimiento adecuado.

- Las AC de Microsoft son extensibles. Las autoridades de certificación de Windows Server soportan muchos módulos de directiva y de salida. Los módulos de directiva indican a la autoridad las condiciones en las que las solicitudes de certificados serán soportadas. Los módulos de salida indican a la autoridad cómo y dónde se publicarán los certificados emitidos. Por último, para aumentar la seguridad de las claves, entre ellas la de la clave privada de la autoridad, también podemos relacionar la autoridad de certificación con los módulos de seguridad hardware HSM (*Hardware Security Modules*) que desempeñarán el papel de caja fuerte, en el exterior del sistema operativo.

Con respecto a las otras alternativas a los servicios de certificados de Windows Server. Las soluciones alternativas proporcionadas por los editores especializados como Entrust o Baltimore son muy eficientes pero tienen unos costes muy importantes sin ofrecer una integración tan avanzada como la de Microsoft dentro de las redes Windows. Los estudios demuestran que el coste total de propiedad de la infraestructura PKI está relacionado en gran medida con el despliegue y la renovación de los certificados. Este punto es en especial importante puesto que sólo los servicios de certificados de Windows Server soportan la inscripción y la renovación automática de certificados para los equipos y los usuarios.

- Las AC de Microsoft pueden elevar el nivel de seguridad con facilidad. La integración de los servicios de certificado dentro de los servicios de directorio Active Directory permite desplegar un sistema de autenticación multifactor basado en la utilización de tarjetas inteligentes. También es posible utilizar el protocolo IPSec para garantizar la confidencialidad e integridad de los datos transmitidos en la red, así como el cifrado de archivos EFS (*Encrypting File System*) para garantizar la confidencialidad de los datos almacenados en discos NTFS.
- Las AC Microsoft se benefician de una administración simplificada. La empresa podrá expedir certificados y, junto con otras tecnologías, eliminar el uso de contraseñas. Las funciones de revocación y la publicación de las listas de revocación de certificados se ven facilitadas en gran medida. Una vez más, los administradores se beneficiarán de la integración de los servicios de certificados con el directorio Active Directory, directivas de grupo, aplicaciones integradas en Active Directory, objetos usuarios y equipos así como los servicios de autenticación y protección de red (servicios Radius - NPS y funcionalidad NAP (*Network Access Protection*) de Windows Server 2012 R2).

Tenga en cuenta que la funcionalidad NAP, disponible con los servicios NPS (*Network Policy Server*), Windows Server 2008 R2 y Windows Server 2012 R2 no se renueva con Windows Server 2016, ni del lado del cliente con Windows 10. Los clientes que disponen de una solución de protección de red NAP deben orientarse por ejemplo, a los proveedores como Cisco, Avaya o Symantec.

3. Importancia de la arquitectura de una infraestructura de claves públicas

Es muy importante considerar el carácter "crítico y central" de una infraestructura PKI dentro de un sistema de información empresarial. En efecto, los servicios ofrecidos por una PKI sirven como componentes de seguridad para muchas aplicaciones y son por lo tanto, tan importantes como las aplicaciones mismas. Los puntos siguientes, siendo bien comprendidos, podrán servir de puntos de referencia para evitar los errores más frecuentes.

- Estudie y valide todos los temas relacionados con la arquitectura y el despliegue "de la última tecnología" de su infraestructura PKI. Cada empresa tiene sus propias limitaciones de aplicaciones y sus propios requisitos en términos de niveles y prácticas de seguridad, también hay varias soluciones, cada una adaptada a cada caso.
- Busque la simplicidad. Las tecnologías, procesos y metodologías relativas a las infraestructuras PKI son muy complejas. El primer objetivo es reforzar la seguridad de los usuarios, los equipos y las aplicaciones disponibles en la red, siendo indispensable enmascarar los detalles y la complejidad de las tecnologías PKI promocionando el lado funcional de las mismas.

4. Temas específicos de las entidades Windows Server

Con respecto a Windows Server 2003, Windows Server 2008 es una versión mayor en muchos aspectos, en especial en materia de seguridad, fiabilidad y de interoperabilidad. De hecho, los servicios de certificados se llaman AD CS, en inglés de *Active Directory Certificate Services*, a partir de esta versión y aportan muchas mejoras que permiten un mejor uso global de la infraestructura de claves públicas.

Tenga en cuenta el hecho de que los servicios de certificados de Windows Server se llaman desde ahora Active Directory Certificate Services lo que no implica que sean un requisito previo. Este será, por ejemplo el caso de las autoridades de certificación de tipo raíz no conectada -en inglés, *Standalone Root CA*.

Con respecto a las autoridades de certificación raíz autónomas o integradas en Active Directory: por lo general, la aplicación de una infraestructura de clave pública (PKI) está compuesta por una o varias AC de tipo "raíz de la empresa" es decir, integradas en los servicios de dominio de Active Directory. Observe que existen las mejores prácticas de arquitectura que recomiendan la aplicación de una AC raíz de confianza autónoma y "totalmente desconectada" de la red. Este tipo de modelo, más complejo en términos de puesta en marcha, puede incrementar significativamente la seguridad de una arquitectura compuesta por varias AC. Para más información sobre las arquitecturas de claves públicas, busque "Stand-Alone Certification Authorities" en el sitio Microsoft Technet en la dirección https://technet.microsoft.com o consiga el excelente libro "Windows Server 2008 PKI and Certificate Security" de Brian Komar, disponible en versiones de Microsoft Press.

Microsoft pone de relieve la importancia de los servicios de Active Directory cuando es conveniente para desplegar una infraestructura de claves públicas a través de los servicios de certificados de Windows Server. En efecto, las funcionalidades avanzadas que afectan a las empresas requieren de Active Directory a través del soporte de autenticación Kerberos y objetos de directivas de grupo.

Partiendo del principio de que los protocolos relativos a la infraestructura de claves públicas no son hoy objeto de modificaciones importantes, el objetivo principal de las mejoras introducidas en los servicios de certificados de Windows Server se centra en una gestión más flexible y más fina de los certificados expedidos a todos los tipos de clientes. En efecto, aunque en primera instancia Microsoft centró sus esfuerzos en el soporte de los equipos Windows y Windows Server, hoy Microsoft pone el acento sobre la integración de dispositivos no-Windows.

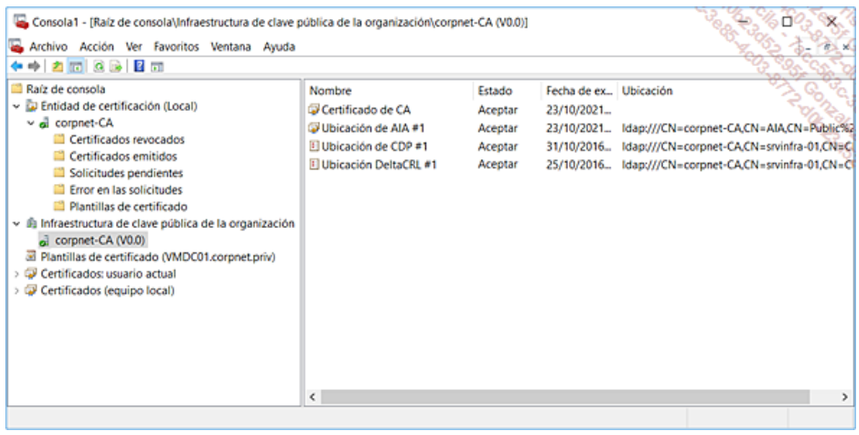
Las funciones de los servicios de certificados AD CS más significativas y siempre de actualidad con Windows Server 2012 R2 y Windows Server 2016 se presentan a continuación:

- El control de parámetros globales empleando PKI View.
- El soporte del protocolo SCEP (*Simple Certificate Enrollment Protocol*). La infraestructura PKI que funciona con versiones anteriores como Windows Server 2003 participaron en la actualización de métodos inteligentes para que la inscripción de los certificados de los equipos y los usuarios sea lo más transparente posible. Hoy, el servicio NDES (*Network Device Enrollment Service*) permite la expedición de certificados a los dispositivos de red, como por ejemplo los enrutadores, los servidores VPN o cualquier otro elemento activo que deba disponer de un certificado.
- Para soportar mejor los escenarios que favorecen a los métodos basados en la web (formularios de solicitud de inscripción, etc.), los servicios AD CS aportan importantes modificaciones en la interfaz de inscripción en la Web para aumentar de forma significativa la seguridad de la plataforma a través de mecanismos de inscripción por completo modernizados.
- El soporte del protocolo OCSP (*Online Certificate Status Protocol*) tiene por objeto facilitar el soporte de infraestructuras PKI complejas, en especial cuando es necesario hacerse cargo de sitios remotos.
- Una mayor precisión y facilidad de gestión mediante los nuevos parámetros de directivas de grupo disponibles con Windows 7, Windows 8.1 y Windows 10, para desarrollar diferentes tipos de certificados. Esto también es válido para la renovación de certificados, tarea quizá aún más pesada que la inscripción inicial.

a. Componente MMC PKI de empresa

Este nuevo componente de administración facilita las tareas de administración básicas de la infraestructura de claves públicas integradas en un entorno Active Directory. Permite la supervisión, el rescate y proporciona un rápido estado del funcionamiento de los jerarquías de autoridades integradas en Active Directory.

Al principio, esta herramienta formaba parte del kit de recursos técnicos de Windows Server 2003 y su necesidad era tal que forma parte hoy de todas las versiones posteriores de Windows Server, hasta Windows Server 2016.



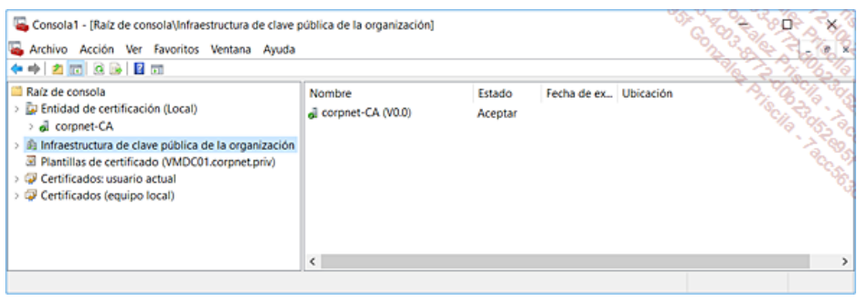
Componente PKI de empresa y control de la infraestructura PKI registrada en Active Directory

La funcionalidad principal de esta herramienta es obtener una visibilidad eficaz del estado del entorno vital de las autoridades de certificación. También podemos ver la accesibilidad y la validez de la información de acceso de autoridad, AIA (*Authority Information Access*), así como el estado de los puntos de distribución (*Certificates Distribution Points*) que contienen las listas de revocación de certificados (CRL). Se soportan los estados siguientes:

- Estado En línea y fuera de línea de las autoridades.
- Estado de tipo problema crítico.
- Estado de tipo problema no crítico.
- Estado de tipo operativo.

El componente MMC PKI Empresarial permite también un acceso simplificado a las funciones de administración de servicios de certificados AD CS. Es también sencillo, a partir de esta herramienta corregir o modificar los parámetros de una autoridad de certificación o incluso publicar o actualizar las listas de revocación.

La figura siguiente muestra el estado de funcionamiento de la autoridad de certificación Corpnet CA.



Visualización del Estado de las autoridades de certificación inscritas en la partición de configuración Active Directory

b. Inscripción para los dispositivos de red empleando el protocolo MSCEP

Las autoridades de certificación Windows Server 2016 y las versiones anteriores como Windows Server 2008 soportan el protocolo SCEP (*Simple Certificate Enrollment Protocol*), que es hoy la referencia estándar de Internet. Esta RFC describe el protocolo de comunicación capaz de permitir a los distintos tipos de elementos de red comunicarse con una autoridad de registro - RA (*Registration Authority*), para la inscripción de los certificados.

Las versiones desde Windows Server 2008 R2 a Windows Server 2016 implementan las funcionalidades más avanzadas publicadas por la versión estándar del IETF. Esta versión se denomina MSCEP Para Microsoft SCEP. De partida, el protocolo SCEP fue desa-rrollado por Cisco como una extensión de los métodos de inscripción que existían antes. El mismo se basa en el protocolo desarrollado por VeriSign para equipos Cisco.

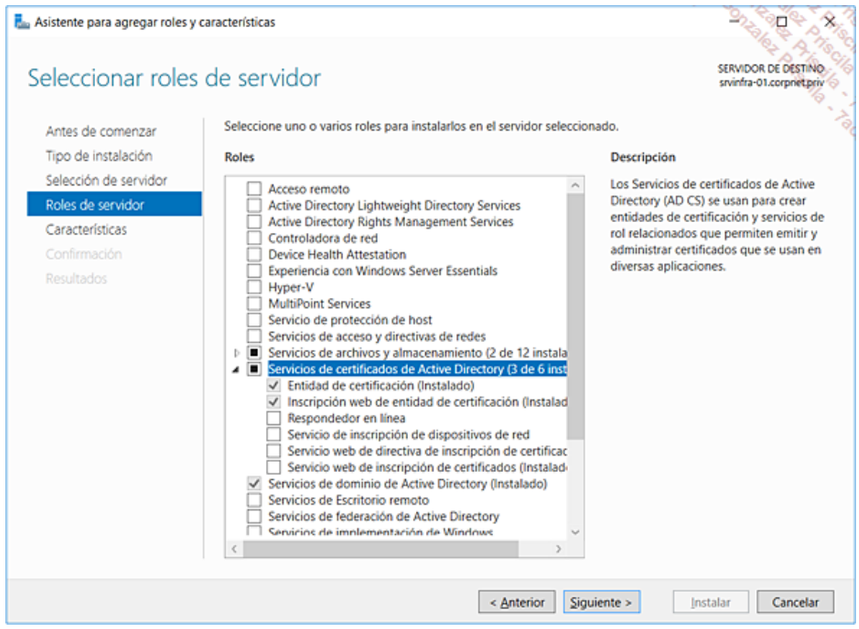
Tenga en cuenta que el protocolo SCEP no está disponible en versiones estándar de Windows Server 2008 y Windows Server 2008 R2, pero sólo en las versiones Enterprise y Datacenter. Estas diferencias se eliminaron con Windows Server 2012, 2012 R2 y Windows Server 2016.

La implementación de la DLL ISAPI responsable del Protocolo MSCEP soporta las siguientes características:

- La generación de contraseñas de uso único (*one-time passwords*) para los administradores.
- El soporte de las solicitudes de inscripción transportadas por el protocolo SCEP emitidas por dispositivos de red tales como los switches, routers y otros elementos activos que soporta el protocolo SCEP.
- La recuperación de las solicitudes en espera almacenadas en la autoridad de certificación.

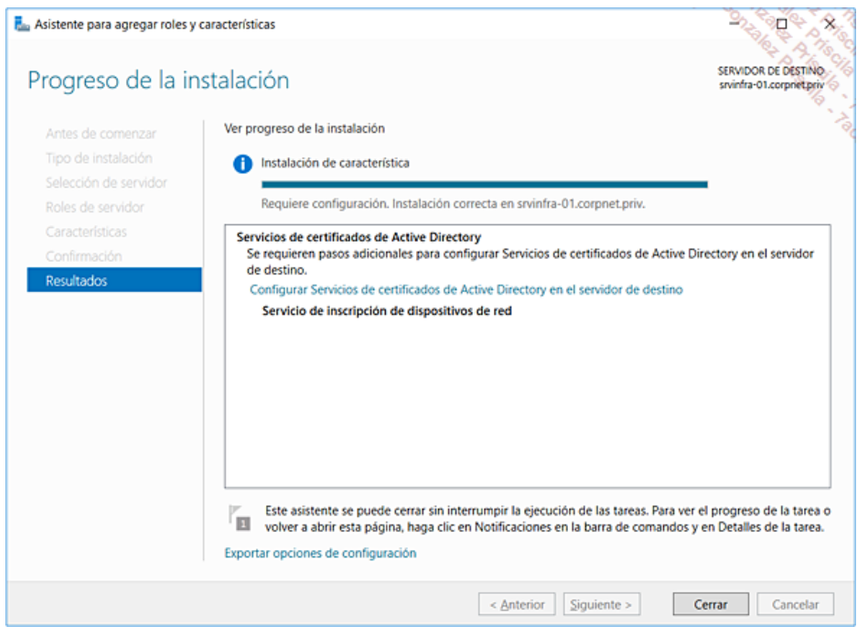
Instalación y método de despliegue

El despliegue de los servicios de inscripción de dispositivos de red requiere un planificación rigurosa. Presentamos estos puntos a continuación: El primer concepto consiste en instalar el servicio adecuado, el cual no puede ser instalado al mismo tiempo que la autoridad de certificación.



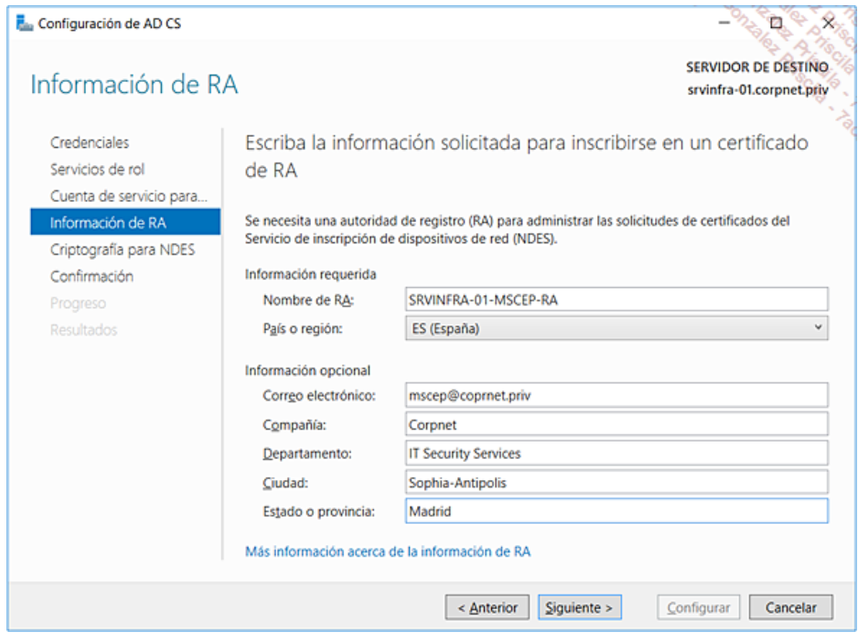
Esta primera etapa se realiza con sencillez utilizando la opción **Administrar / Agregar Roles y características** del administrador de servidor de Windows Server 2016. Luego, el asistente de instalación solicitará rellenar los siguientes parámetros:

- Declarar la identidad utilizada para el servicio de registro de dispositivos de red. Tendremos la posibilidad de utilizar una cuenta de servicio, es decir, la autoridad integrada Network Service, sabiendo que la primera alternativa es la recomendada. Tenga en cuenta que en este caso, la cuenta abierta deberá ser miembro del grupo IIS_IUSRS.
- Declarar el nombre de la autoridad de registro (*Registration Authority*), sin omitir la información de la región y país, las cuales se incluyen en todos los certificados MSCEP que serán expedidos.
- Declare el CSP (*Cryptographic Service Provider*) a utilizar para generar las claves de cifrado que serán utilizadas para cifrar el tráfico entre la autoridad de certificación y la autoridad de registro. También será necesario efectuar el mismo tipo de opciones de seguridad de los flujos entre la autoridad de registro y los dispositivos de red. En ambos casos, también habrá que definir el tamaño de las claves de cifrado, por defecto de 2048 bits.



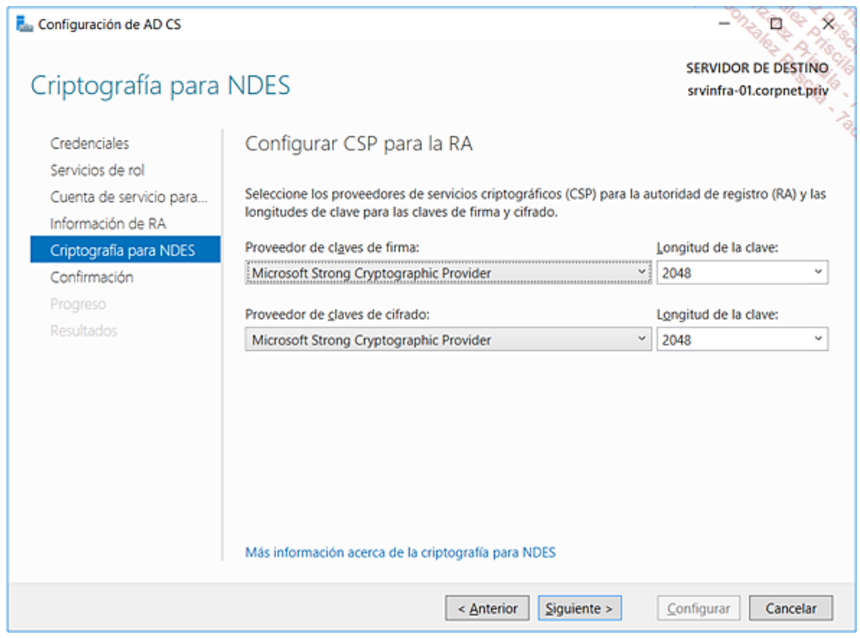
Agregar el servicio de Rol "Servicio de inscripción de dispositivos de red "

¡Observe! El proceso de instalación de los Servicios de inscripción de dispositivos de red incluye una nueva autoridad de registro y elimina los certificados de las anteriores autoridades de registro que podrían haberse instalado de forma previa. Microsoft recomienda que en el caso de que sea necesario instalar una RA - *Registration Authority*, en un equipo donde ya se haya instalado, las operaciones en curso se concluyan bajo el riesgo de perderse.



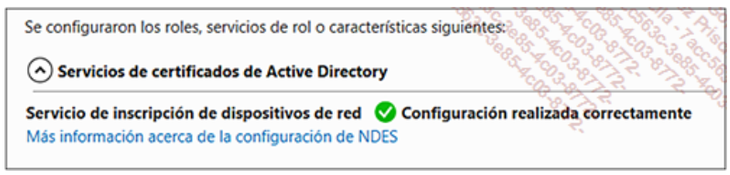
Configuración de la autoridad de registro MSCEP para dispositivos

Instalación de los servicios de inscripción de dispositivos NDES (*Network Devices Enrollment Services*): tenga en cuenta que el asistente de configuración configura una nueva plantilla de certificado adaptada a la utilización de certificados en los dispositivos y que define a su vez los permisos de lectura y de inscripción en dicha plantilla. El Servicio Asociado dispondrá también de un SPN (*Servicio Principal Name*), registrado en Active Directory.



Proveedores de firma y cifrado recomendados

Atención: el servicio NDES utiliza dos certificados, y las claves asociadas. Microsoft requiere que sólo los CSP basados en la interfaz CryptoAPI, tales como el CSP Microsoft Strong Cryptographic Provider, se soporten.

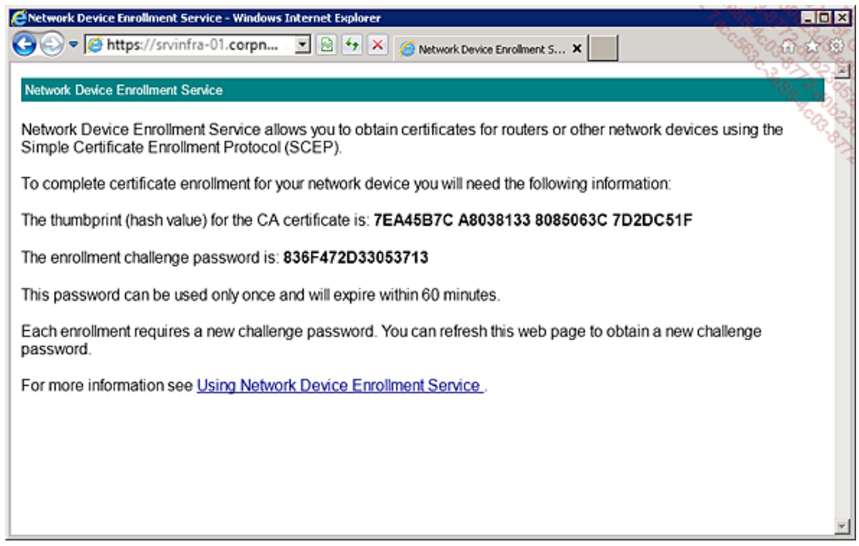


Final de la configuración de servicios NDES

El proceso de inscripción se compone de los siguientes pasos:

1. El dispositivo de red genera un par de claves RSA en el dispositivo.

2. El Administrador obtiene una contraseña a partir del Servicio de Registro de dispositivo de red de Windows Server utilizando la página de administración de los servicios de inscripción de dispositivos de red. El Servicio verifica que el administrador tiene los permisos necesarios sobre el o las plantillas de certificados requeridas.



Solicitud de inscripción a través de la URL https://srvinfra-01.corpnet.priv/certsrv/mscep_admin/

3. El Administrador configura el dispositivo con la contraseña y declara el certificado de la autoridad de certificación empresarial utilizada. Esta operación es específica para cada dispositivo, pero se utiliza en general la función GetCACert implementada por el Servicio SCEP.

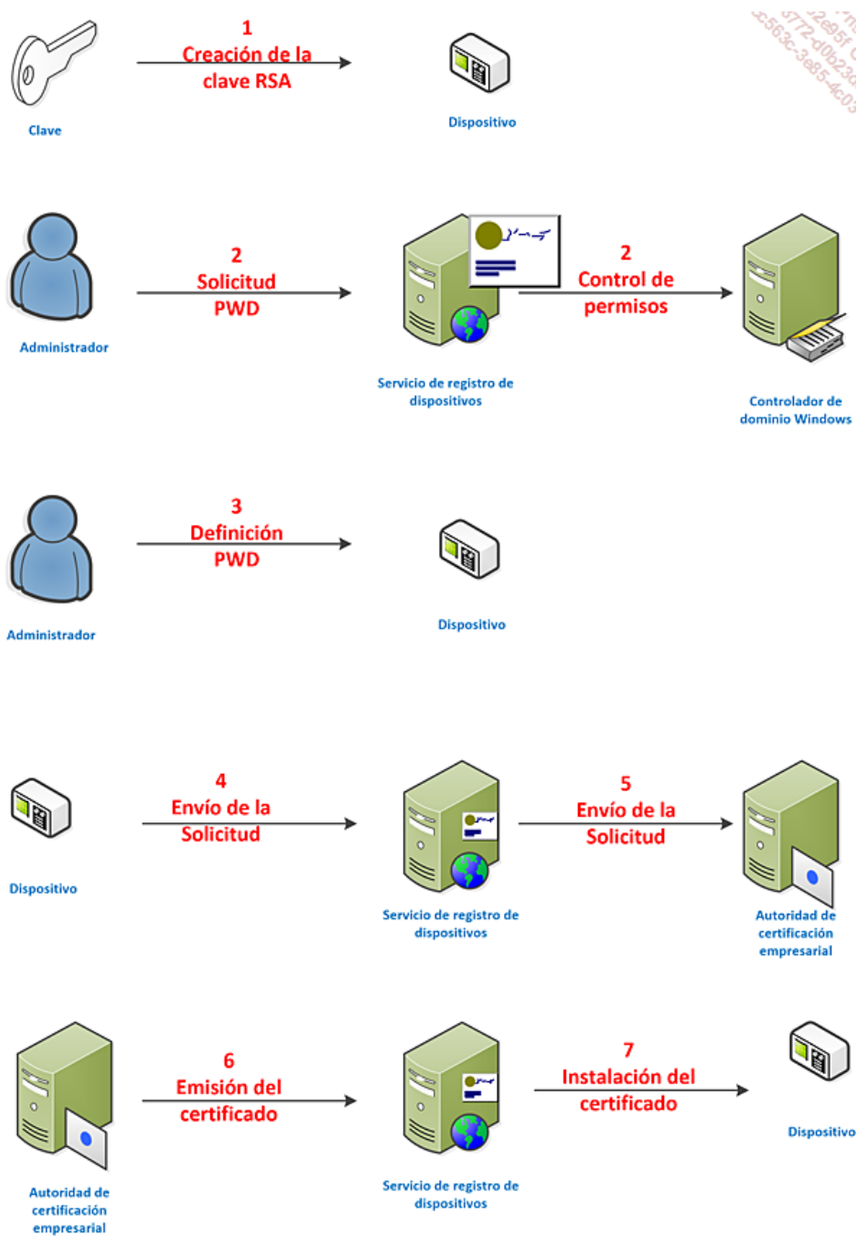
4. El Administrador configura el dispositivo para enviar la solicitud de inscripción al servicio de registro de dispositivo de red que funciona en el servidor Windows Server.

5. El servicio de inscripción del dispositivo de red firma una solicitud de inscripción empleando el certificado de tipo Agente de inscripción y luego lo envía a la autoridad de certificación.

6. La autoridad de certificación emite el certificado y transmite la información al servicio de inscripción del dispositivo de red.

7. El dispositivo obtiene el certificado emitido a partir del servicio de inscripción del dispositivo de red.

Al final de este proceso, el dispositivo es capaz de implementar los mecanismos criptográficos que le son necesarios en base al par de claves pública/privada de las que dispone por último.



Proceso de inscripción completo empleando una RA (Registration Authority) y el Protocolo SCEP con Windows Server 2008 y Windows Server 2008 R2

Securización del Protocolo SCEP y configuración del IIS

Durante el proceso de instalación, el asistente de configuración de los servicios de inscripción del dispositivo de red ofrece la instalación y configuración de Microsoft IIS y los componentes IIE necesarios.

Durante esta fase, se crean dos directorios virtuales:

- El primer directorio virtual se utiliza para las solicitudes de contraseñas.
- El segundo directorio virtual se utiliza durante el envío de las demandas de certificados.

Las solicitudes de contraseñas solo son posibles después de que el solicitante haya sido autenticado y que las autorizaciones necesarias hayan sido verificadas. Si el solicitante es validado, entonces el servicio generará una nueva contraseña, la que será devuelta en texto claro.

Tenga en cuenta que por esta razón, **es indispensable implementar SSL** en este directorio virtual.

Parámetros por defecto del servicio SCEP

El Servicio de inscripción de dispositivos de red se configura por defecto para satisfacer la mayoría de las configuraciones. El conjunto de los parámetros de configuración del servicio están situados en la clave siguiente: HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

En el caso de que la clave siguiente no se encuentre, el servicio de inscripción de dispositivos de red utilizará los parámetros por defecto codificados de forma permanente en el software (hard coded).

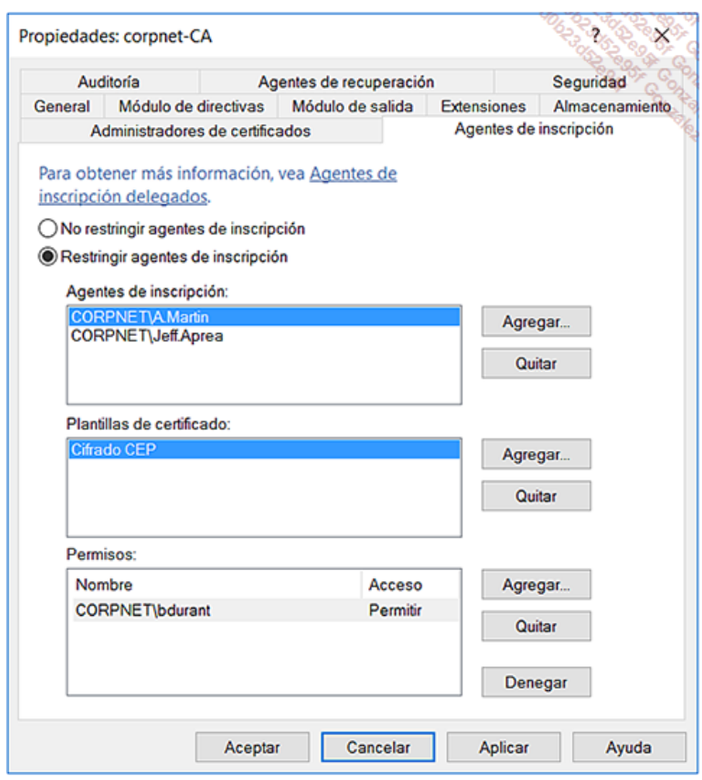
Para más detalles sobre la aplicación y las configuraciones avanzadas del servicio de inscripción de dispositivos de red, busque "Network Device Enrollment Servicie Guidance" en el sitio Microsoft Technet en la dirección https://technet.microsoft.com o siga el vínculohttps://technet.microsoft.com/en-us/library/hh831498(v=ws.11).aspx

Implementación de restricciones para los agentes de inscripción delegados en el certificado de la autoridad de registro (RA Certificate)

Microsoft recomienda restringir los agentes de inscripción declarando sobre cada autoridad de certificación Windows Server los agentes de inscripción delegados configurados de forma específica. De esta forma, cada certificado de agente de inscripción solo podrá ser utilizado por algunos dispositivos.

El hecho de no crear una delegación implica que el servicio de inscripción de dispositivos de red tiene todos los permisos para emitir certificados de cualquier solicitante.

La siguiente ventana muestra que Alice Martin tiene una restricción que le permite, sobre la plantilla llamada **Cifrado CEP** de autorizar al usuario Bob Durand para reclutar un certificado basado en esta plantilla, mientras que otros usuarios pueden disponer de restricciones diferentes (en este ejemplo, el grupo Todo el mundo y el usuario JFAprea tienen otras restricciones).



Restricciones sobre los agentes de inscripción y las plantillas de certificados

En efecto, las autoridades de certificación Windows Server 2008 y las versiones posteriores hasta Windows Server 2016 permiten a una empresa controlar de manera muy estricta que plantillas de certificado son utilizables por que agente y por quién. El hecho de limitar el alcance de los agentes de inscripción permite controlar mejor la delegación de la confianza a terceros aprobados y así los riesgos asociados a ella.

Definición de un período de validez correcto para los certificados de dispositivos

Es necesario encontrar un equilibrio entre facilidad de administración y nivel de seguridad exigido. Cuanto mayor sea el período de validez del certificado menor será necesario desarrollar el proceso de inscripción y renovación. El inconveniente de esta estrategia es que un hacker dispondrá de más tiempo para calcular la clave privada.

Por defecto, el período de validez será de un año. Se recomienda que para un número limitado de dispositivos y si el riesgo en materia de seguridad es aceptable, el período de validez pueda ampliarse a dos años. Esta política permitirá minimizar las operaciones de renovación de certificados y, por lo tanto, reducir las tareas de administración.

Seguridad de las solicitudes y la disponibilidad del servicio SCEP

No es necesario que el servicio de registro de dispositivos esté disponible de forma permanente. En efecto, una vez inscritos uno o varios dispositivos, se recomienda interrumpir los servicios IIS. Luego será necesario reiniciar el servicio IIS para poder renovar los certificados expirados.

En el caso de que el servicio IIS sea utilizado por otras aplicaciones, también es posible no detener el conjunto de aplicaciones utilizadas por el sitio Web responsable de los servicios de registro de dispositivos. El hecho de detener el conjunto IIS -o de forma directa el servicio IIS, borra todos los datos temporales utilizados por el Servicio SCEP, como por ejemplo las contraseñas ocultas en espera de utilización.

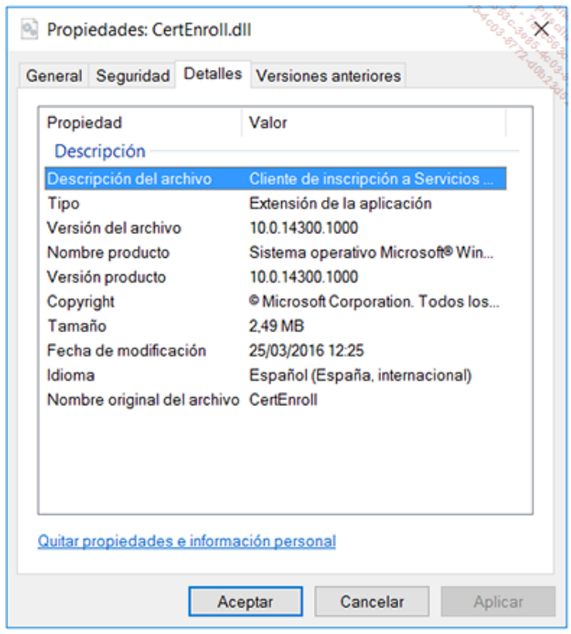
c. Evolución de los métodos de inscripción web con AD CS

Con Windows Server 2008, 2008 R2 y versiones posteriores, los servicios de certificados AD CS introducen un cambio importante en relación con el soporte para la inscripción de los certificados empleando una interfaz Web. Este método, disponible con Windows 2000 Server y Windows Server 2003, ofrece un servicio de expedición completamente configurable para emitir y gestionar los certificados utilizados por muchas aplicaciones que utilizan las tecnologías criptográficas basadas en la utilización de claves públicas y privadas. El uso de esta interfaz web es en especial interesante y necesaria cuando el puesto de trabajo solicitante no forma parte de un dominio Active Directory o bien cuando la autoridad de certificación está situada en otro bosque de Active Directory.

Con Windows Server 2008 R2 y versiones posteriores, el control ActiveX Xenroll será sustituido por CertEnroll.dll

Windows Server 2008 R2, Windows 7 y versiones posteriores, tales como Windows Server 2016 y Windows 10 introducen un nuevo componente COM -incluido de forma directa en el sistema operativo, para hacerse cargo de todas las operaciones relativas a la inscripción de los certificados.

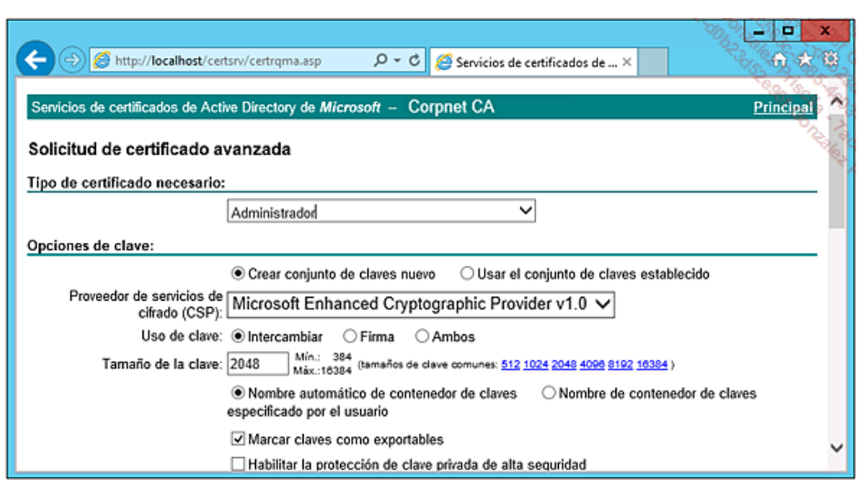
El nuevo componente, CertEnroll.dll, se desarrolló de forma específica para evitar la instalación y utilización del antiguo control ActiveX Xenroll aparecido con Windows 2000 y considerado hoy en día demasiado inseguro.



Cliente de inscripción de los servicios de certificados AD CS Certenroll.dll

Como ocurría con Windows Server 2003, las autoridades de certificación Windows Server 2008 R2 incluyen una interfaz web que soporta las operaciones de reclutamiento a través de un navegador como Microsoft Internet Explorer o Firefox.

La imagen siguiente ilustra el uso del antiguo control ActiveX Xenroll - Microsoft Certificate Enrollment Control, publicado por Microsoft y disponible a partir del servidor Windows Server 2008 con los servicios de certificados de Active Directory AD CS.



Portal AD CS y solicitud de certificado

Las autoridades de certificación AD CS permiten a los equipos Windows XP y Windows Server 2003 utilizar el control XEnroll. Por razones de seguridad, los sistemas Windows 7, Windows Server 2008 R2 y versiones posteriores hasta Windows 10 y Windows Server 2016, utilizan de forma nativa el nuevo componente CertEnroll.dll y no pueden utilizar el antiguo control ActiveX.

Interoperabilidad de las interfaces de inscripción en la web de Windows Server 2003 y Windows Server 2008 R2

Hemos visto antes que las autoridades de certificación Windows Server 2008 R2 soportaban tanto los equipos Windows XP y Windows Server 2003, pero también los equipos Windows 7, Windows Server 2008 R2 y versiones posteriores, tales como Windows 10 y Windows Server 2016.

Aunque sabemos que en el momento en que escribimos estas líneas que Windows Server 2003 ya no está soportado, no es menos cierto que esta versión del sistema operativo se encuentra todavía en algunos sitios en producción. Por ello es importante recordar que, lamentablemente, no es lo mismo con las autoridades de certificación Windows Server 2003, que no soportan los sistemas operativos Windows 7 y versiones posteriores. Los niveles de interoperabilidad se listan a continuación:

- En el caso de los puestos cuyo sistema operativo es anterior a Windows 7: estos equipos son soportados por las autoridades de certificación de Windows Server 2003. Las autoridades de certificación de Windows Server 2008 R2 soportan también estos equipos, pero de manera limitada.
- En el caso de los puestos cuyo sistema operativo es igual o posterior a Windows 7: estos equipos son soportados por las autoridades de certificación de Windows Server 2003. Durante el uso de la interfaz web de inscripción se mostrará el siguiente mensaje:*Unsuccessful together with a "Downloading ActiveX control" message*. Lo mismo modo ocurre para las autoridades de certificación Windows Server 2003 SP2. Sin embargo, el mensaje especificará que se requiere una actualización. Las autoridades de certificación de Windows Server 2008 R2 soportan por completo a los equipos Windows 7 y versiones posteriores.

Para más información sobre el soporte de la interfaz web de inscripción de certificados y el procedimiento de instalación de la interfaz de los servicios de certificados AD CS de Windows Server 2008 en un servidor Windows Server 2003, podemos consultar el artículo técnico Microsoft KB 922706 .

En cuanto a los servicios de infraestructura tales como los servicios de certificados AD CS, se recomienda aplicar, o actualizar, los servicios de certificados de Windows Server 2008 R2 a Windows Server 2012 R2 o Windows Server 2016. Así contará con la plataforma más moderna que ofrece la mayor interoperabilidad con los sistemas que funcionan con Windows 7 o versiones posteriores, como Windows 10.

Cambios incluidos en la inscripción web con los servicios AD CS

Es importante señalar que la interfaz Web integrada en los servicios de certificados AD CS de Windows Server 2008 R2 y versiones posteriores, tales como Windows Server 2012 R2 y Windows Server 2016, introdujo una serie de cambios con respecto a la anterior versión Windows Server 2003.

- Para poder enviar de forma directa una solicitud de certificado a través de las páginas de inscripción web, es necesario disponer de una versión de navegador igual o superior a Microsoft Internet Explorer 6.x o Netscape 8.1. Los usuarios que no dispongan de estos niveles mínimos de navegador deberán realizar su solicitud de certificado generando una solicitud PKCS#10, siempre empleando las páginas de inscripción web.
- No es posible utilizar las páginas de inscripción web para realizar solicitudes de certificados basados en los modelos de certificados versión 3.0, disponibles sólo a través de las autoridades Windows Server 2008 R2 y posteriores. Los certificados creados en base a plantillas de certificados Versión 3.0 soportan la emisión de certificados utilizando los protocolos criptográficos del tipo B.
- Un usuario ya no puede solicitar certificados de tipo equipo a través de la interfaz Web con Windows 7 o versiones posteriores. Esta limitación se explica porque, en los equipos Windows Vista, Internet Explorer no puede ejecutar en el contexto del equipo local.
- No es posible utilizar las posibilidades aportadas por los agentes de inscripción ya que estas funcionalidades se han eliminado de las páginas de inscripción web incluidas con los servicios de certificados AD CS de Windows Server 2008 R2 y versiones posteriores. Esta característica era en especial interesante para inscribir tarjetas inteligentes para los usuarios. Si todavía requerimos esta funcionalidad con una autoridad de certificación Windows Server 2008 R2 o una versión superior, es recomendable utilizar un puesto de trabajo Windows 7 o posterior que desempeñará el rol de la estación de registro de tarjetas inteligentes.

d. OCSP y parámetros de validación de la ruta de acceso

A medida que el uso de certificados y la necesidad de protección de los datos aumenta, los administradores utilizan una estrategia para la aprobación de certificados para mejorar su control sobre la utilización de éstos. Además, una gestión no centralizada de los certificados puede convertirse de forma muy rápida en una tarea de administración imposible. Es por estas razones que Windows Server 2008 R2, Windows 7 y las versiones posteriores ofrecen hoy un avance significativo para controlar mejor todo el proceso de inscripción así como la verificación de las rutas de acceso a la información de autoridades en particular respecto de las listas de revocación. Es en este último punto donde el protocolo OCSP (*Online Certificate Status Protocol*) permite gestionar mejor la información de revocación.

Con el fin de garantizar una gestión coherente de los parámetros de seguridad importantes, es muy recomendable gestionar los certificados usando los parámetros de directivas de grupo que se aplican a los clientes en un dominio Active Directory, un grupo o una unidad organizativa. Los detalles de los parámetros importantes se presentan más adelante.

El proceso de revocación es un aspecto importante de la gestión de los certificados. En efecto, cuando un certificado es presentado a una aplicación, la aplicación determina el estado de revocación del certificado, comprobando si se incluye o no en la lista de revocación CRL (*Certificate Revocation List*) publicado por la autoridad de certificación.

Un equipo toma la iniciativa de descargar una lista de revocaciones a partir de un punto de distribución CDP (*CRL Distribution Point*) sólo cuando la CRL de la caché del equipo ha expirado. Varias limitaciones son impuestas por las listas de revocación. Las cuestiones relativas a estas limitaciones se conjugan con las problemáticas presentadas a continuación:

- ¿Con qué frecuencia se actualizan las CRL al nivel de las autoridades de certificación?
- ¿Con qué frecuencia se publican las CRL en los CDP?
- ¿Qué impacto tiene en la red la publicación de las CRL?

Los inconvenientes relacionados con las listas de revocación suelen ser su tamaño, que introduce el número de limitaciones y efectos secundarios. En función del número de puestos de trabajo, el número de certificados revocados, el ancho de banda consumido aumenta y es necesario compensar limitando la frecuencia de las actualizaciones y descargas de los CRL.

Para responder a estos puntos, los servidores Windows Server 2008 R2 y versiones posteriores, tales como Windows Server 2016 soportan el protocolo OCSP (*Online Certificate Status Protocol*) definido por la RFC 2560. Este protocolo se implementa a través de un servicio cliente / servidor de réplica en línea que proporciona la información de revocación de certificados, evitando así la verificación y descarga de las listas de revocación de certificados.

El respondedor en línea implementado en Windows Server 2008 y Windows Server 2008 R2 permite a un destinatario de un certificado presentar una solicitud de estado de certificado a un respondedor automático OCSP a través del protocolo HTTP (*HyperText Transfer Protocol*). El respondedor automático OCSP devuelve una respuesta firmada digitalmente que indica el estado del certificado. A diferencia de los CRL que aumentan de manera incremental, la cantidad de datos para comprobar por demanda es constante. No hay ninguna relación entre el número de certificados revocados en la autoridad de certificación y el número de verificación de validez de los certificados en la empresa.

Para más información sobre el Protocolo OCSP, podemos consultar las RFC siguientes, así como el enlace Microsofthttp://go.microsoft.com/fwlink/?LinkID=71068. **RFC 5019**: The Lightweight Online Certificate Status Protocol (OCSP) Profile for

High-Volume Environments. **RFC 4806**: Online Certificate Status Protocol (OCSP) Extensions to IKEv2. **RFC 4557**: Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). **RFC 2560**: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol.

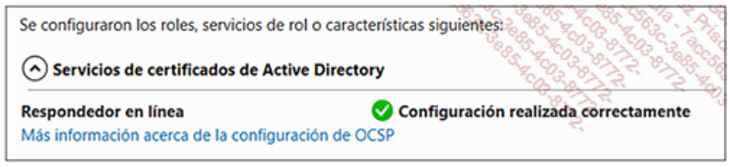
Todas estas RFC se encuentran disponibles para descargar desde el sitio http://www.rfc-editor.org/.

Componentes de un respondedor en línea

El Servicio respondedor en línea incluído con las autoridades de certificación Windows Server 2008 R2 y hasta Windows Server 2016, comprende los siguientes elementos:

- **Servicio de respondedor en línea**: el servicio de respondedor en línea decodifica una solicitud de estado de revocación de un certificado, evalúa el estado y luego envía una respuesta firmada. Esta respuesta contiene la información de estado del certificado.

Tenga en cuenta que el servicio de respondedor en línea es un componente distinto de una autoridad de certificación (CA). Por razones de seguridad, puede ser instalado con independencia de ésta en un servidor diferente de la autoridad de certificación.



Instalación y configuración de un respondedor en línea

- **Respondedor en línea**: un servidor en el cual el servicio de respondedor en línea así como el proxy web del respondedor en línea se ejecutan. Un equipo que hospede una autoridad de certificación puede ser configurado como respondedor en línea, pero se recomienda mantener las autoridades de certificación y los respondedores en línea en equipos separados.

Tenga en cuenta que un respondedor en línea único puede proporcionar información de estado de revocación de los certificados expedidos para una o varias autoridades. La información de revocación puede ser soportadas por varios respondedores en línea. El Servicio respondedor en línea puede ser instalado en cualquier servidor que ejecute Windows Server 2008 R2 o una versión posterior.

Los datos de revocación de certificados se derivan de una lista de revocación de certificados (CRL) publicada que puede provenir de una autoridad que funciona en cualquier versión de Windows Server o incluso de una autoridad no Microsoft.

- **Proxy web del respondedor en línea**: la interfaz del respondedor en línea existe en forma de una extensión ISAPI incluida en los servicios de IIS. El proxy web recibe y decodifica las consultas y gestiona la caché de las respuestas.
- **Configuración de revocación**: una configuración de revocación incluye los parámetros necesarios para atender las solicitudes de estado de los certificados que hayan sido emitidos empleando una clave de la autoridad de certificación específica. Estos parámetros incluyen el certificado de la autoridad, el certificado de firma del respondedor en línea y el tipo de proveedor de revocación a utilizar.
- **Proveedor de revocación**: un proveedor de revocación es el módulo de software que, junto con otros parámetros de configuración de revocación, permite a un respondedor en línea verificar el estado de un certificado. El proveedor de revocación de Windows Server 2008 R2 o una versión posterior, tal como Windows Server 2012 R2 o Windows Server 2016, utiliza los datos de las listas de revocación de certificados (CRL) para proporcionar la información de estado a los clientes que utilizan el protocolo OCSP.
- **Matriz de respondedores en línea**: un grupo de respondedores en línea comprende uno o varios respondedores en línea miembros. Podemos añadir respondedores en línea a un grupo de respondedores en línea.

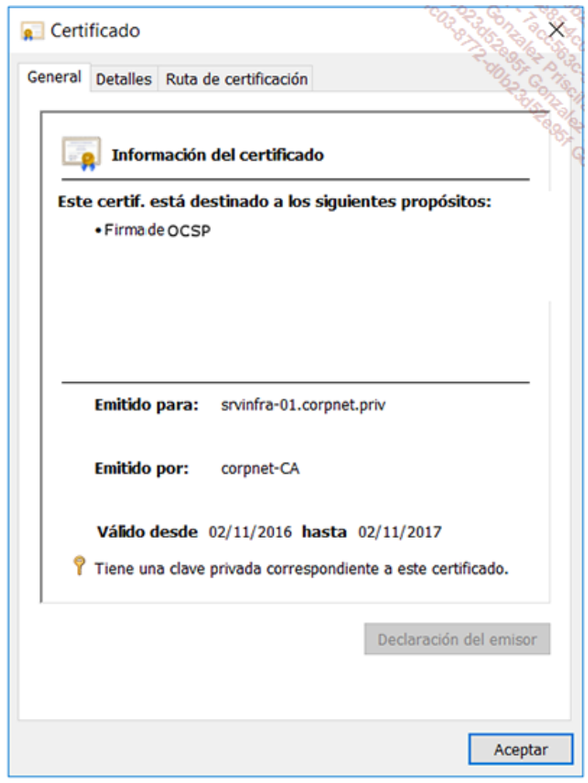
Puede ser muy interesante añadir los respondedores en línea a una matriz existente para la gestión de ubicaciones geográficas diferentes, para mejorar la tolerancia a fallos o gestionar de forma correcta los posibles problemas de rendimiento en los sitios importantes.

- **Controlador de matriz de respondedores en línea**: cuando varios respondedores en línea son miembros del mismo grupo, uno de los miembros del grupo será designado como controlador del grupo.

Cada respondedor en línea dentro de un grupo puede ser configurado de manera independiente. Sin embargo, en caso de conflicto, la información de configuración del controlador del grupo tendrá prioridad sobre los de los demás miembros del grupo.

Configuración de servicios de respondedor en línea en la red

La configuración de los servicios de respondedor en línea requiere varias etapas que deben realizarse en el nivel de la autoridad de certificación que se usará para expedir los certificados de firma OCSP (*Online Certificate Status Protocol*). Estos certificados son necesarios para el funcionamiento de cada equipo que actúa como respondedor en línea.

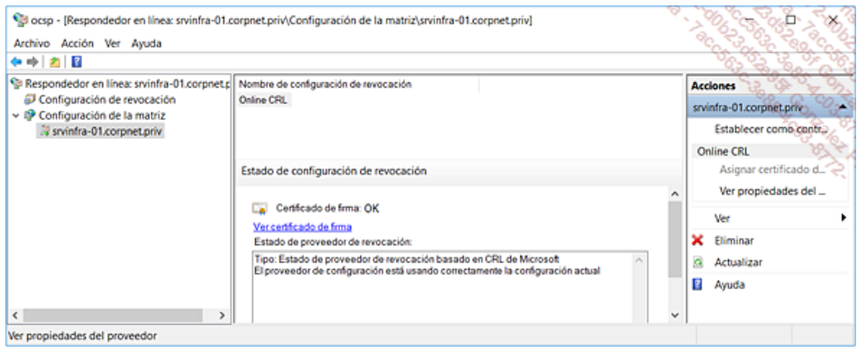


Certificado de firma OCSP para un servicio Respondedor en línea

Es necesario declarar la plantilla de certificado correspondiente, activar la plantilla de certificado de la autoridad emisora y por último activar la inscripción automática en el servidor que incluirá el servicio de respondedor en línea. Esta última etapa permite al equipo autorizado obtener el certificado necesario para el funcionamiento del respondedor en línea.

El proceso completo de instalación y configuración de un respondedor en línea requiere el uso del administrador de servidor para instalar el servicio de respondedor en línea, el componente de software MMC **Plantillas de certificados** para configurar y publicar las plantillas de certificados de tipo Firma de respuesta OCSP, y del componente de software MMC **Autoridad de Certificación** para incluir las extensiones OCSP. El último paso consiste en utilizar el componente **Respondedor en línea** para crear una configuración de revocación y luego comprobar el funcionamiento del respondedor empleando un puesto cliente.

La imagen siguiente muestra el certificado utilizado y obtenido a través de la inscripción automática.



Consola MMC Respondedor en línea y configuración de la revocación

Declaración de la ubicación del respondedor en línea OCSP a la extensión de acceso a los datos de la autoridad en la autoridad de certificación

La etapa final de configuración consiste en introducir las URL de cada respondedor en línea. A continuación listamos las etapas de configuración:

En la autoridad de certificación, empleando la consola de administración MMC **Entidad de certificación**, seleccionamos la autoridad de certificación y luego en el menú **Acción**, hacemos clic en **Propiedades**.

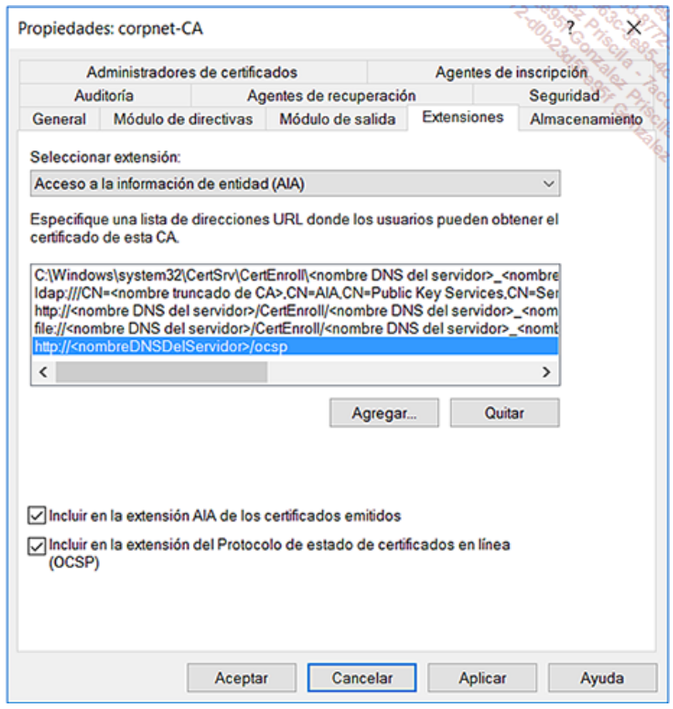
Hacemos clic en la pestaña **Extensiones**.

En la lista **Seleccionar extensión**, hacemos clic en **Acceso a la información de Entidad (AIA)**, luego **Agregar**.

Especifique los lugares a partir de los cuales los usuarios pueden obtener los datos de revocación de certificados. Por defecto, se tratará de una URL con forma http://ServerOCSP/ocsp.

¡Observe! Asegúrese de activar la opción **Incluir en la extensión del Protocolo de estado de certificados en línea (OCSP)**.

En este punto, asegúrese de que la plantilla de certificado **Firma de la respuesta OCSP** está listado en la sección **Plantillas de certificados** a nivel de la autoridad de certificación.



Configuración de las extensiones AIA para declarar la ubicación de los servicios OCSP

Verificación del correcto funcionamiento del respondedor en línea OCSP

Al término de la instalación de un nuevo respondedor en línea, es indispensable comprobar su buen funcionamiento. El procedimiento consiste en revocar uno o varios certificados emitidos y luego verificar que los datos de revocación están disponibles a partir del respondedor en línea. Esta operación requiere que dispongamos de los permisos de administrador en el nivel de la autoridad de certificación. A continuación listamos las diferentes operaciones a realizar:

Declare una o varias plantillas de certificado en la autoridad de certificación. Podemos utilizar cualquier método de inscripción soportado por la autoridad y el puesto de trabajo con el fin de obtener uno o varios certificados a revocar. La inscripción automática de los certificados es el método más moderno y más seguro para los puestos de trabajo Windows 7, Windows 8.1 y Windows 10.

Una vez los datos relativos a los nuevos certificados están publicados en la configuración Active Directory, puede ocurrir que debamos esperar a la replicación de Active Directory o bien forzar la replicación del controlador de dominio solicitado empleando el comando`repadmin`, o la Consola MMC **Sitios y Servicios de Active Directory**.

En un puesto de trabajo, abra un intérprete de comandos y arranque un ciclo de inscripción automático para obtener un certificado a través del comando `certutilpulse`.

En el puesto cliente, utilice la consola MMC **Certificados** para asegurarse de que los certificados se han expedido para el usuario y el equipo de manera adecuada.

En el caso de que la inscripción automática no se haya realizado todavía, podemos escribir el comando `Gpupdate /force`. También es posible reiniciar el equipo cliente con el fin de forzar la inscripción automática y obtener el certificado a través de la inscripción automática.

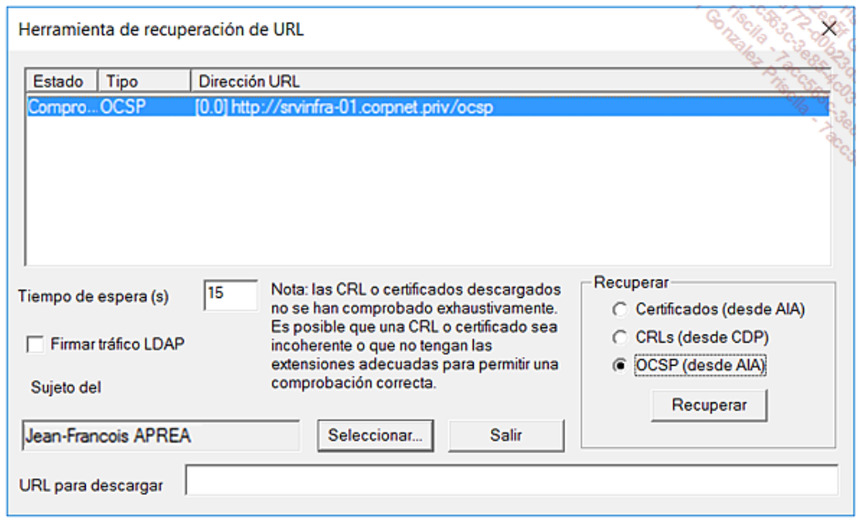
En la autoridad de certificación, empleando la Consola MMC **Autoridad de certificación**, revoque uno o varios de los certificados expedidos a través del menú **Acciones - Todas las tareas - Revocar un certificado - Selecciona el motivo de revocación del certificado**, y luego confirme la operación.

En la autoridad de certificación, empleando la Consola MMC **Entidad de certificación**, publique una nueva CRL a través del menú **Acción - Todas las tareas - Publicar**.

Podemos decidir no publicar listas de revocación y utilizar sólo los respondedores en línea OCSP. Para eliminar los puntos de distribución de listas de revocación de la autoridad de certificación, utilice la consola MMC **Entidad de certificación**, seleccione la autoridad de certificación, en el menú **Acción** haga clic en **Propiedades**, en la pestaña **Extensiones**, seleccione **Puntos de distribución de listas de revocación**, seleccione los puntos de distribución de listas de revocación y haga clic en **Quitar**.

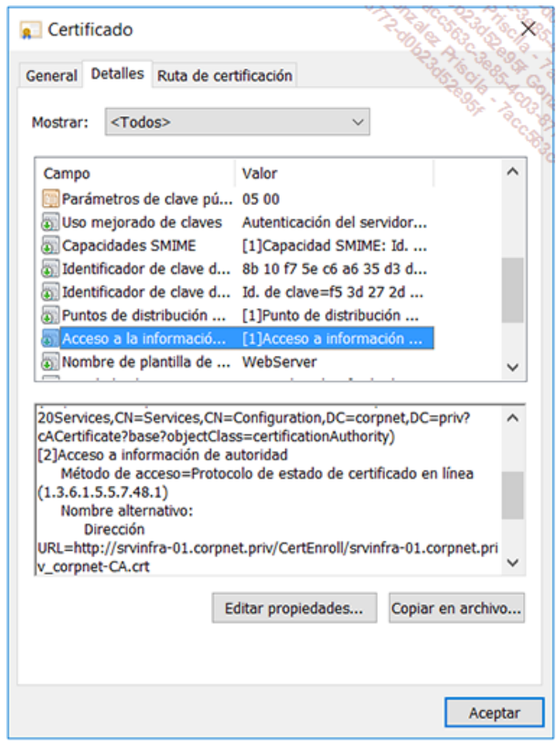
Reinicie los servicios de certificados AD CS y haga las pruebas de funcionamiento del respondedor en línea a partir de un puesto cliente mediante la consola MMC **Certificados** para exportar el certificado de prueba a un archivo con extensión .cer.

Una vez exportado el certificado de usuario (por ejemplo JFAprea-Export.cer para el usuario JFAprea), escriba en la línea de comandos:`certutil -url JFAprea-Export.cer`



Verificación del correcto funcionamiento del protocolo OCSP

El comando `Certutil -url c:\JFAprea-Export.cer` extrae información de revocaciones emitidas por el respondedor en línea en función de la información de la AIA (*Authority Information Access*) declaradas al nivel de la autoridad de certificación. La imagen siguiente muestra la URL http://srvinfra-01.corpnet.priv/ocsp declarada a nivel de AIA - Información de acceso de la Autoridad para el uso del protocolo OCSP.



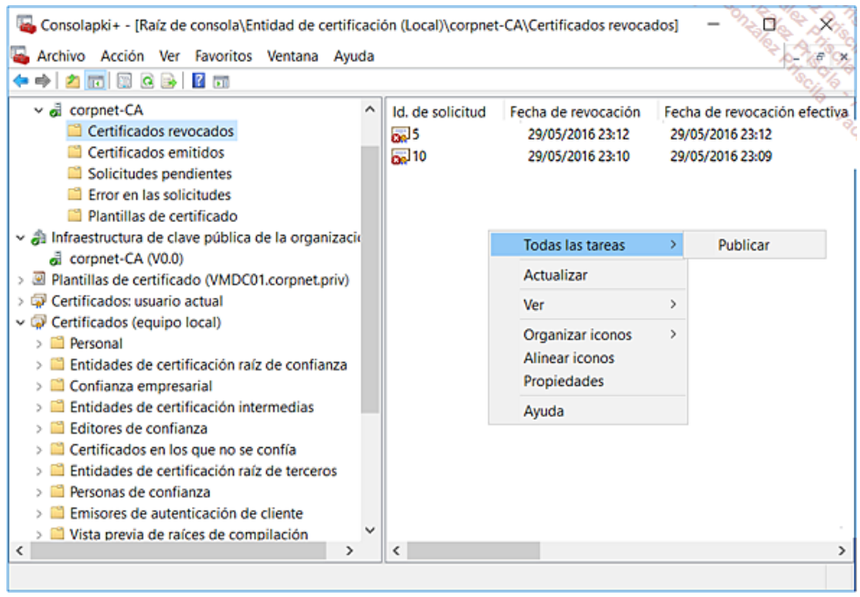
Información OCSP (1.3.6.1.5.5.7.48.1) publicada a través de las AIA en el certificado de un usuario

Publicación de datos

¡Observe! Los certificados deberán ser emitidos después de que el servicio de respuesta en línea sea instalado y luego declarado a nivel de información de AIA.

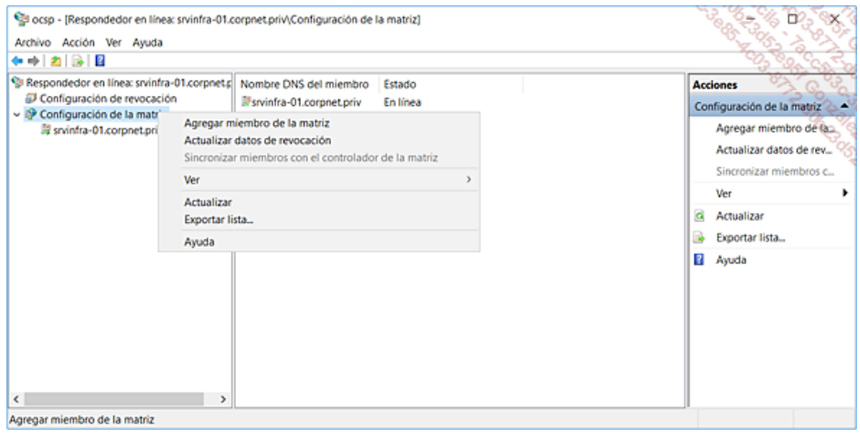
Una vez validado el funcionamiento empleando la herramienta de recuperación de URL vista antes, conviene comprobar la correcta interpretación de la información de revocación. Para este último y definitivo test, debemos proceder de la siguiente manera:

- A nivel de la autoridad de certificación, revoque el certificado antes validado a través del estado **Verificado**.
- A nivel de la autoridad de certificación, publique una nueva lista de revocaciones.



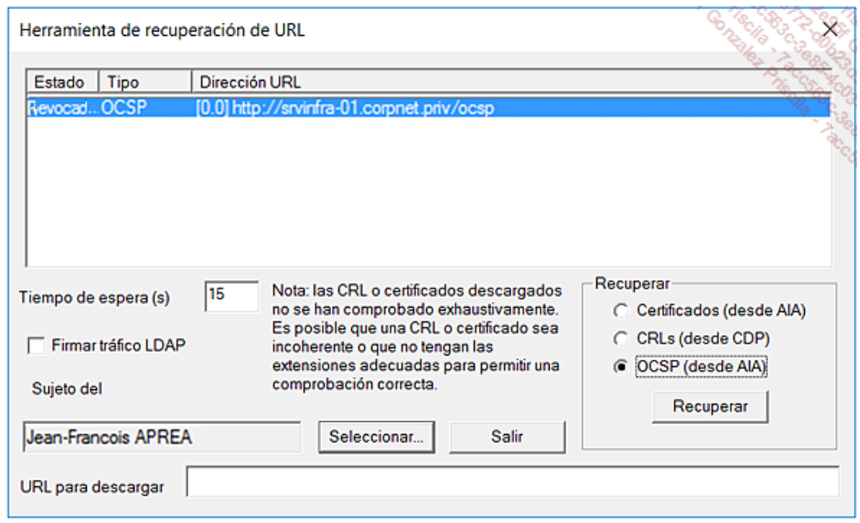
Publicación de una nueva lista de revocación

- En el servicio de respuesta en línea OCSP, actualizamos la información de revocación como se muestra en la imagen siguiente.



Actualización de datos de revocación en el respondedor en línea

En nuestro ejemplo, el último paso consiste en validar una vez más el certificado del usuario JFAprea utilizando el comando: `certutil -url JFAprea-Export.cer`.



Control a través del protocolo OCSP del certificado de usuario Jeff APREA con el estado Revocado

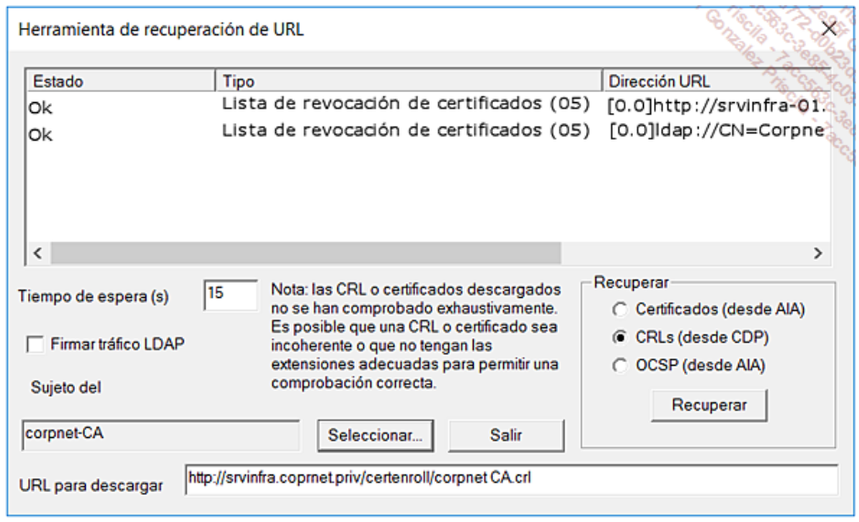
Esta vez, la verificación del certificado empleando el Protocolo OCSP para el usuario Jeff APREA, revela que éste dispone del estado **Revocado**. En este punto, el respondedor en línea puede considerarse operativo.

Comando Certutil y validación de CRL

El comando Certutil también puede utilizarse para ayudar a la resolución de problemas de verificación de la validez de los certificados. Podemos en efecto basarnos en el mismo principio que hemos utilizado para la verificación de la información de revocación de los respondedores en línea.

Basta con seleccionar la opción **Listas CRL (CDP)** luego de seleccionar la opción **Extraer**. La herramienta de recuperación de URL mostrará el estado de las distintas listas de revocación publicadas a través de Active Directory, el protocolo LDAP y a través del protocolo HTTP.

En nuestro ejemplo, el comando introducido es el siguiente: `certutil -url "http://srvinfra-01.corpnet.priv/certenroll/corpnet CA.crl"`



Acceso al conjunto de listas de revocación de certificados

5. Novedades aportadas por las autoridades de certificación de Windows Server 2008 R2

Acabamos de ver que Windows Server 2008 R2 aporta una evolución significativa de los servicios de certificados. En resumen, los principales avances se listan a continuación:

- el componente MMC PKI de empresa permite una mejor gestión de los datos técnicos y una mejor percepción del correcto funcionamiento de las autoridades de certificación Microsoft;
- el soporte del protocolo SCEP permite la entrega de certificados a los dispositivos hardware empleando el servicio NDES (*Network Device Enrollment Service*);
- el soporte del nuevo servicio de rol Respondedor en línea optimiza las respuestas a las consultas del estado de las revocaciones;
- La posibilidad de delegar la inscripción de los certificados a terceros en función de las plantillas de certificados y de usuarios o grupos de usuarios ofrece una granularidad aumentada en la gestión de los certificados.

Por supuesto, estas evoluciones son la respuesta a verdaderos problemas técnicos y funcionales, pero el sistema operativo mismo aporta también novedades interesantes. A continuación veremos con más detalle estas novedades que atañen en primer lugar a los entornos complejos.

a. Mejora de las bases de datos de las autoridades de certificación que gestionan grandes volúmenes

Esta mejora se refiere en principio al despliegue del protocolo NAP (*Network Access Protection*), con IPSec. La implementación de este método requiere la emisión de certificados de salud NAP cuya expiración se fija en horas y provoca la emisión de n certificados por hora y por equipo, lo que conlleva un aumento de los registros dentro de la base de datos de certificados.

Para solucionar este problema, el administrador puede decidir desactivar algunas operaciones para evitar la saturación de la base de datos de certificados.

El soporte del protocolo NAP se efectúa empleando los servicios NPS (*Network Policy Server*), de Windows Server 2008 R2, Windows Server 2012 y 2012 R2. Observe que esta funcionalidad no se encuentra, ni con Windows Server 2016 dentro del servicio NPS, ni con Windows 10 que ya no dispone del agente Microsoft NAP.

b. Servicio web de inscripción de certificados

Este nuevo servicio de Rol permite a los usuarios y a los equipos inscribirse y renovar los certificados mismos cuando el equipo no es miembro de un dominio, o bien si un equipo miembro de un dominio se encuentra de forma temporal en una zona de red securizada como por ejemplo, una DMZ.

Este nuevo servicio funciona con el servicio web Directiva de inclusión de certificados para proporcionar a los usuarios y los equipos una inscripción automática basada en una directiva definida por el administrador a través del protocolo HTTPS.

El servicio web Inscripción de certificados utiliza el protocolo HTTPS para aceptar las solicitudes de certificados procedentes de los ordenadores de la red, así como para el retorno de los certificados emitidos. El servicio web Inscripción de certificados se basa en la utilización del Protocolo DCOM para conectarse a la autoridad de certificación y realizar la inscripción para la cuenta del solicitante.

En Windows Server 2003 o Windows Server 2008, la inscripción de certificados a través del uso de los objetos directivas de grupo no podrá llevarse a cabo por equipos miembros del dominio Active Directory que utilizan DCOM. Esta limitación técnica acota los escenarios de emisión de certificados a los dominios y confianzas establecidas entre los dominios y bosques Active Directory. El nuevo servicio de rol Servicio Web de inscripción de certificados de servicios AD CS permite eliminar esta limitación.

El nuevo servicio web Inscripción de certificados asociado al nuevo servicio web Directiva de inclusión de certificados permite la implementación de la inscripción automática de certificados a través de directivas a través del protocolo HTTP. Estos servicios web desempeñan el papel de proxy entre un equipo cliente y una autoridad de certificación. Este nuevo enfoque hace innecesarias las comunicaciones directas entre los equipos cliente y las autoridades de certificación, permitiendo la distribución de certificados a través de Internet y entre los bosques de Active Directory.

Ventajas: estos nuevos servicios permiten soportar la inscripción automática para los equipos de un bosque en las autoridades de certificación situadas en otro bosque. Permite también a los usuarios de tipo extranet registrarse a través de Internet.

Limitaciones de aplicación: los bosques de Active Directory deben utilizar un esquema Windows Server 2008 R2 o posterior. Las autoridades de certificación deben ser de tipo Raíz de empresa. Los equipos cliente deben funcionar en Windows 7 o una versión posterior. El servicio web Inscripción de certificados se encuentra en todas las versiones de Windows Server.

c. Soporte de la inscripción de los certificados entre los bosques

Los entornos que utilizan los servicios de certificados de Windows Server 2008 -o una versión anterior, no permiten la emisión de certificados fuera de su propio bosque. Este tema significa que cada bosque deberá por fuerza disponer de su propia infraestructura de claves públicas. Las autoridades de certificación Windows Server 2008 R2 y posteriores soportan las referencias LDAP que permiten a estas autoridades de certificación emitir certificados entre los bosques con relaciones de aprobación bidireccionales.

Este escenario es en particular útil para las empresas que deciden crear un bosque cuyo objeto es "solo" concentrar los servicios globales ofrecidos a otros bosques.

Limitaciones de aplicación:

- Los bosques de Active Directory deben utilizar como mínimo el nivel funcional Windows Server 2003 y contar con relaciones de aprobación bidireccionales.
- Los clientes pueden operar en Windows XP o cualquier versión posterior, tales como Windows 8.1 o Windows 10, y no requieren ninguna actualización específica.
- Las autoridades de certificación deben funcionar bajo Windows Server 2008 R2 Enterprise Edition o cualquier versión superior..

Active Directory Federation Services (AD FS)

1. Conceptos y funcionalidades básicas

Los servicios de Federación de Active Directory AD FS (*Active Directory Federation Services*) incorporados en Windows Server constituyen una plataforma abierta que integra sistemas Windows y no-Windows, para poner en práctica una solución de control de acceso basada en identidades.

La característica principal de los servicios de federación AD FS permite a las aplicaciones y servicios web situados dentro y fuera de la red empresarial permitir un acceso seguro a las aplicaciones en base a identidades y aplicaciones que están ubicadas en distintas redes. De esta forma, los servicios de federación ofrecen a los usuarios una autenticación única SSO (*Single Sign On*), para acceder a aplicaciones compatibles AD FS, donde éstas estén situadas, es decir, dentro o fuera de la red privada de la empresa. AD FS juega entonces el papel de proveedor de identidad autenticando a los usuarios y proporcionándoles tokens de seguridad para acceder a las aplicaciones aprobadas. Otro escenario de utilización permitirá a AD FS utilizar otros proveedores de identidad para, en este caso, proporcionar tokens para las aplicaciones aprobadas en el entorno AD FS.

Tenga en cuenta que la función de proporcionar un acceso externo a aplicaciones seguras vía AD FS no está garantizada a través del servicio de Rol Proxy de federación AD FS. Con Windows Server 2012 R2 y Windows Server 2016, este servicio de publicación está soportado a través del servicio de Rol de acceso remoto Proxy de Aplicación Web. Este servicio está incluido con Windows Server 2012 R2 y Windows Server 2016 y permite publicar aplicaciones como Microsoft Exchange y SharePoint y puede ser utilizado con o sin AD FS.

Los servicios AD FS permiten por lo tanto no tener necesidad de usar identidades adicionales mediante la aplicación de las relaciones de confianza capaces de transmitir la información de identidad hacia uno o varios socios que las acepten.

La idea misma del principio de federación de identidades permite imaginar muchos escenarios donde el despliegue de servicios de federación AD FS sería apropiado.

Las relaciones de colaboración basadas en la federación de socios a través de servicios tales como los ofrecidos por AD FS convienen a las empresas que cumplen estos requisitos y limitaciones.

Entidades que agrupan recursos

Las empresas que poseen y administran sus propios recursos, por ejemplo, el despliegue de servidores de federación AD FS para permitir a los socios autorizados acceder a aplicaciones o servicios web integrados en AD FS. El concepto de federación no está limitado a entidades externas, sino que también puede ser utilizado para divisiones o filiales de la misma organización.

Entidades que agrupan identidades

Las empresas que poseen y administran sus propias identidades pueden desplegar servidores que certificarán a los usuarios locales y crearán tokens de acceso que los servidores de federación ubicados en las entidades que agrupan los recursos utilizarán para dar tal o cual autorización.

AD FS, el SSO para aplicaciones web

El proceso que permite al ser autenticado en un contexto determinado, acceder a los recursos ubicados en un contexto diferente sin tener que exigir una acción de re-autenticación por parte de los usuarios, se llama Inicio de sesión único o SSO (*Single Sign On*).

Los servicios de federación Active Directory proporcionan en este escenario una solución de autenticación única para las aplicaciones y servicios web dentro del inicio de sesión del navegador del cliente Internet o de la aplicación.

Servicios de roles AD FS en Windows Server 2016

El servidor que alberga los servicios de federación AD FS de Windows Server 2016 incluye los servicios federación, los servicios de proxy y los servicios de agente web. Estos servicios deben ser configurados para permitir el SSO de aplicaciones web, la federación de los recursos de tipo web, así como las autorizaciones otorgadas de forma efectiva a los usuarios.

Selección de servicios de rol AD FS

En función de las limitaciones de la empresa, podemos desplegar servidores en relación con estas limitaciones. Estos diferentes roles se resumen a continuación:

- **Servicio de Federación**: el servicio central está compuesto por uno o varios servidores de federación que comparten una directiva de aprobación común. Los servidores de federación se utilizan de forma principal para encaminar las solicitudes de autenticación de usuarios de otras organizaciones o de clientes ubicados en Internet.
- **Servicio proxy de federación**: este servicio asume el rol de proxy de autenticación dentro una red perimetral DMZ (*DeMilitarized Zone*). El servicio proxy de federación utiliza los protocolos WS-F PRP (*WS-Federation Passive Requestor Profile*) para transferir la información de identificación de los navegadores de Internet a los servicios de Federación de Active Directory.
- **Agente para notificaciones**, (***Claims-aware agent***): este agente puede ser implementado en un servidor web que alberge una aplicación compatible para que pueda solicitar tokens de acceso AD FS. Por lo general, una aplicación compatible es una aplicación de tipo ASP.NET que utiliza el concepto de función presente en los tokens de acceso AD FS. Estos datos permiten asignar los permisos correctos, así como la personalización de aplicaciones.
- **Agente basado en los tokens de acceso Windows**: este agente puede ser utilizado en un servidor Web que alberga una aplicación basada en la utilización de tokens de acceso Windows para asegurar la conversión de tokens de acceso AD FS en un token de acceso Windows. Las aplicaciones basadas en los tokens de acceso utilizan mecanismos de autorización implementados en los sistemas Windows y posteriores.

Con respecto a las notificaciones (Claims)

Los servicios de federación AD FS proporcionan una arquitectura de seguridad extensible que soporta los tokens de acceso basados en la norma SAML 2.0 (*Security Afirmación Markup Language*) y las autenticaciones Kerberos. Los servicios AD FS pueden también realizar equivalencias entre las identidades y los roles utilizados por los elementos de la lógica de las aplicaciones.

Las empresas pueden utilizar estos mecanismos para integrar su infraestructura de autenticación existente, así como sus estrategias de seguridad internas dentro de los servicios de federación de Active Directory.

Estos elementos técnicos y lógicos adoptarán la forma de objetos llamados notificaciones (en inglés, claims). Estos elementos, representando en general un cliente, están construidos por un servidor y pueden representar un nombre, una identidad, una clave, un grupo, un privilegio, un rol o cualquier otra estructura útil a la gestión de la confianza dentro de la federación.

Empleando estas herramientas, los servicios de federación de Active Directory transmitirán la confianza acordada entre entidades que pueden ser muy diferentes. Los servicios AD FS fueron diseñados para permitir el intercambio de estos elementos que contienen valores muy arbitrarios. En función de estos valores, el socio podrá por ejemplo prestar determinado nivel de autorización a tal o cual identidad aprobada.

Los intercambios y relaciones pueden tener lugar y combinarse de la siguiente manera:

- Del almacenamiento de las cuentas de usuario al servicio de federación y luego hacia el socio de recursos.
- Del socio con las cuentas de usuario al servicio de federación y luego al recurso de aplicación.
- Del almacenamiento de las cuentas de usuario al servicio de federación y luego al recurso de aplicación.

2. Funcionalidades aportadas por Windows Server 2012 R2

Con Windows Server 2012 R2, más allá de los servicios de federación propiamente dichos, Microsoft añade soporte de nuevos escenarios de uso interesantes:

- Acumulación de dispositivos en un espacio de trabajo (Workspace) para soportar una autenticación SSO multifactor transparente: con esta característica, podemos autorizar la utilización de dispositivos personales limitando al máximo los riesgos relacionados con este tipo de acceso.
- Gestión de riesgos a través de MFA (*Multi Factor Authentication*): con un control de acceso multifactor, AD FS soporta el acceso a las aplicaciones a través de controles de muchos elementos como el nombre de usuario, la dirección de e-mail, la UPN, el uso de los grupos de Active Directory y, cuando el dispositivo es miembro de un espacio de trabajo, los atributos propios de los dispositivos tales como, por ejemplo, la dirección IP o la dirección MAC.

3. Novedades aportadas por Windows Server 2016

Windows Server 2016 introduce una nueva versión de los servicios de federación AD FS basada con fuerza en los servicios ya presentes en Windows Server 2012 y Windows Server 2012 R2. En efecto, con Windows Server 2016, el rol de servidor AD FS soporta en gran parte las mismas características que las ofrecidas por sus predecesores.

Sin embargo, aunque esta versión no es una revolución, evoluciona en el sentido correcto, proponiendo nuevas capacidades de autenticación a través del soporte de usuarios procedentes de directorios no Active Directory. Así, ahora es posible conectar AD FS con directorios LDAP o de forma directa con bases de datos de tipo SQL. Estas nuevas posibilidades son interesantes porque permiten responder a nuevos escenarios de gestión de identidades "híbridos" compuestos por los servicios de dominio de Active Directory, pero no de forma exclusiva.

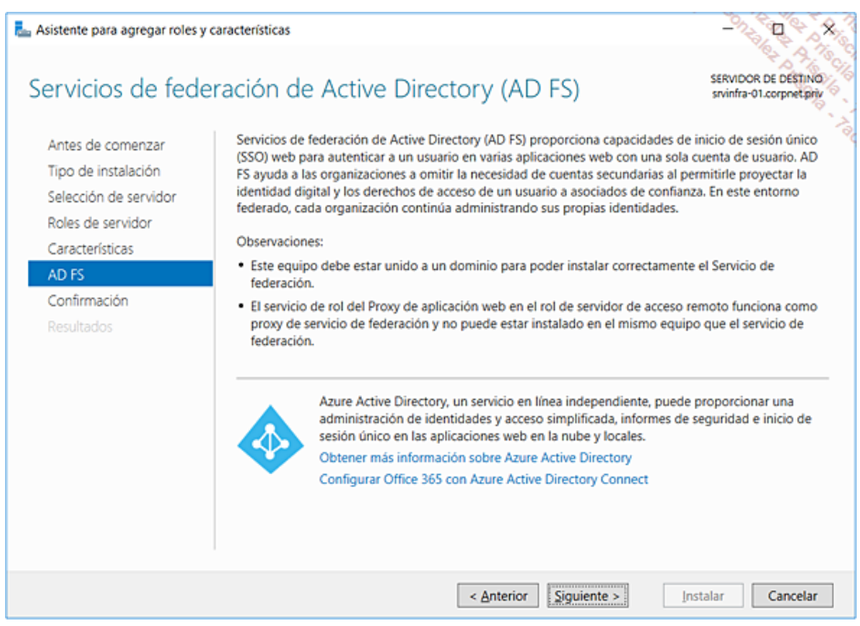
Además de estas nuevas funcionalidades, esta nueva versión nos permitirá una aplicación más fácil de los escenarios más comunes, en particular para el soporte nativo de las aplicaciones. A continuación presentamos estas evoluciones:

- Instalación simplificada e integrada en el Administrador del servidor. El asistente soporta todos los puntos a comprobar para garantizar una instalación y una implementación rápida y segura.
- Integración de las aplicaciones empresariales con AD FS: Microsoft SharePoint, Microsoft Exchange Server, servicios de gestión de derechos digitales AD RMS (*Active Directory Rights Management Services*), Carpetas de trabajo (*Work Folders*), de Windows 8.1 y Windows 10...
- Administración simplificada de las declaraciones necesarias para la aplicación de las aprobaciones de federación. La exportación e importación de los parámetros de aprobación se ha mejorado para permitir una disminución de la complejidad de configuración asociada por lo general a la implementación de las federaciones.
- Integración de la autenticación Microsoft Passport con Windows 10: Windows 10 aporta nuevas tecnologías integradas que mejoran la experiencia del usuario y también la seguridad. Así, con Windows Hello y Microsoft Passport to Work, es fácil eliminar las tradicionales contraseñas mediante dispositivos orientados a usuarios protegidos por una huella dactilar, reconocimiento facial y/o un código PIN. Este método aportado por Windows 10 permite al usuario autenticarse y tener acceso a sus aplicaciones dondequiera que se encuentre, sin tener que enviar de forma directa sus identificadores de empresa.
- Integrando en el sistema operativo Windows 10 y la autenticación Microsoft Passport, AD FS puede utilizar la funcionalidad de Microsoft Passport for Work para autenticar usuarios On-Premise o aprobados a través de una federación AD FS.

4. Instalación del Rol AD FS

La instalación del rol AD DS puede efectuarse a través del administrador de servidor de Windows Server 2016. Una vez instalados los servicios, el asistente de configuración será ejecutado y permitirá crear un clúster AD FS o integrar un nuevo servidor dentro de un clúster existente, después de introducir los diferentes parámetros de configuración. La consola MMC AD FS y el entorno de Windows PowerShell podrán luego utilizarse para la continuación de la configuración.

¡Observe! No es posible instalar en el mismo servidor Windows Server los roles de servicios de federación y de aplicación Web Proxy.



Añadir la función AD FS a través del Administrador del servidor de Windows Server 2016

Limitaciones técnicas para los servicios de federación AD FS

Los servicios de federación AD FS deben respetar las restricciones de instalación siguientes:

- Podemos optar por la implementación de un servidor AD FS Windows Server 2012 R2 o Windows Server 2016. La elección de una de

estas plataformas le permitirá mantener una gran interoperabilidad con las aplicaciones más modernas y los entornos Microsoft Azure. No es recomendable utilizar las versiones anteriores incluidas con Windows Server 2008 o versiones más antiguas.

- Los dominios Active Directory que contengan servidores AD FS deben utilizar como mínimo el nivel funcional Windows Server 2003. Es indispensable utilizar como mínimo el nivel funcional Windows Server 2008 para poder utilizar la autenticación de usuarios con un certificado cliente.
- AD FS no requiere modificaciones específicas de esquema.
- El uso de la funcionalidad (*Workplace Join*) con AD FS requiere que el esquema del dominio que contenga los servidores AD FS utilice el nivel funcional de Dominio Windows Server 2012 R2.
- El servidor AD FS requiere una cuenta de servicio o la utilización de una cuenta de servicio gestionada. En este último caso, el dominio debe tener al menos un Controlador de dominio funcionando con Windows Server 2012.
- Para soportar la autenticación Kerberos entre clientes miembros de un dominio Active Directory y los servicios AD FS, el nombre de HOST/Cuenta_de_servicio_ ADFS debe estar registrada como SPN por cuenta del servicio utilizado. Esta operación se realiza de forma automática en el momento de la instalación si los permisos necesarios son suficientes.
- Todos los servidores AD FS de una granja deben ser miembros del mismo dominio Active Directory.
- AD FS ya no depende de IIS. Esta modificación permite instalar los servicios AD FS sobre controladores de dominio sin tener que añadir los componentes IIS.
- AD FS requiere una base de datos de tipo WID (*Windows Internal Database*). Tenga en cuenta que las bases de datos WID soportan un máximo de 30 servidores AD FS y menos de 100 socios aprobados.
- Los servidores AD FS de una misma granja podrán estar repartidos en distintos Datacenter a fines de tolerancia a fallos con un límite de 30 servidores AD FS.
- AD FS puede utilizar bases de datos WID, SQL Server 2008, SQL Server 2012 y SQL Server 2014.
- La autenticación AD FS vía un navegador de Internet requiere la activación de JavaScript, la activación de las cookies y el soporte de nombres de tipo SNI (*Server Name Indication*).
- El soporte de la funcionalidad *Workplace Join* requiere certificados, una autenticación del dispositivo vía certificado, así como un navegador Internet que soporte la autenticación SSL por certificado.
- Los servicios AD FS de Windows Server 2012 R2 y Windows Server 2016 están soportados por los sistemas operativos Windows 7, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

Limitaciones técnicas para las autoridades de certificación

El soporte del protocolo SSL y de la firma de tokens requiere el uso de certificados digitales. Para ello es indispensable que los permisos utilizados estén aprobados por los sistemas implicados en la infraestructura AD FS. Podemos utilizar las autoridades de certificación de tipo raíz de empresa, es decir, integradas en Active Directory. Dichas autoridades de certificación de empresa pueden funcionar con Windows Server 2008 R2 o cualquier versión posterior, tal como Windows Server 2012 o Windows Server 2016. También podemos usar un certificado emitido por una autoridad pública como Verisign.

AD FS y los certificados: todos los clientes que acceden a un servidor o punto AD FS deben tener confianza en dicho certificado. Se recomienda en especial utilizar un certificado emitido por una autoridad pública. La utilización de un certificado autofirmado es posible, pero en el marco de un entorno de pruebas.

Durante la fase de configuración, un certificado de tipo Wild Card puede ser introducido sabiendo que es recomendable usar el mismo certificado en todos los nodos de la granja AD FS así como en los servidores que desempeñen el papel de WAP (*Web Aplication Proxy*).

Limitaciones técnicas para los navegadores de Internet

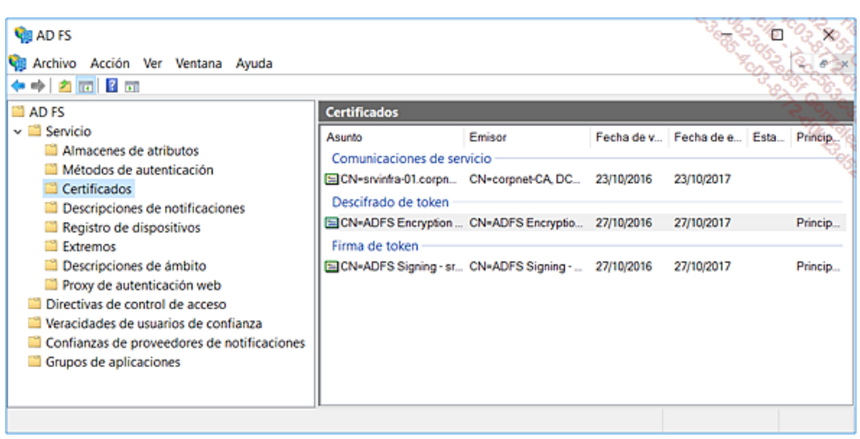
La mayoría de los navegadores de Internet están soportados por los servicios de federación AD FS de Windows Server 2012 R2 y Windows Server 2016. Sin embargo, tenga en cuenta que Microsoft ha validado las funciones AD FS con las versiones de Internet Explorer 10 y 11, Firefox v21, Safari v7, iOS 6, Mac OS X 10.7 y Chrome v27. Microsoft especifica que JavaScript y el soporte de cookies deben estar activados, tanto en los clientes como en los servidores de la federación AD FS y los servidores web accedidos.

Configuración de los servicios de federación AD FS

La configuración de los servicios de federación AD FS requiere un proceso de configuración, cuyo objetivo final es permitir una mayor apertura y autenticación única para el acceso a las aplicaciones web para los socios externos aprobados.

De esta forma, deberemos:

- Definir una arquitectura de servicios de federación adaptada a nuestras necesidades en función de los grandes escenarios de arquitecturas AD FS. La solución debe proporcionar los medios a los administradores para permitir a la empresa alcanzar sus objetivos de gestión federada con identidades, compartiendo estas identidades a través de las aprobaciones de federación, cuando ello sea necesario.
- Añadir las diferentes entidades asociadas a los servicios de federación. Puede tratarse de socios de recursos o de socios de cuentas de usuarios.
- Añadir y configurar uno o varios proveedores de almacenamiento de identidades dentro de los servicios de federación. Con Windows Server 2016, el entorno podrá soportar los servicios de dominio de AD DS, los servicios LDAP v3 Microsoft AD LDS, los servicios LDAP no-Microsoft compatibles LDAP v3, y las bases SQL de terceros.
- Añadir las diferentes entidades asociadas a los servicios de federación.



Para más información sobre la configuración de servicios de federación AD FS, busque el artículo de la base de conocimiento Microsoft KB 3061192, llamado "step-by-step Video: Set up ADFS for Office 365 for Single Sign-On » o siga el enlace siguiente: https://support.microsoft.com/en-us/kb/3061192

5. Referencias para AD LDS con Windows Server

Para más información sobre los detalles técnicos de los servicios de federación AD FS, consulte el sitio de Microsoft, a partir de las direcciones siguientes:

- Active Directory Federation Services Overview: http://go.microsoft.com/fwlink/?LinkId=78692
- Windows Communication Foundation: https://msdn.microsoft.com/es-es/vstudio/aa663324.aspx

Con respecto a la interfaz SAML 2.0 de AD FS: para más información sobre las novedades de la interfaz SAML 2.0, busque en el sitio de Microsoft Technet https://technet.microsoft.com el artículo titulado "Improved interoperability with SAML 2.0" o siga el vínculohttps://technet.microsoft.com/en-us/library/mt728956.aspx

Active Directory Lightweight Directory Services (AD LDS)

1. Conceptos fundamentales

Los servicios AD LDS (*Active Directory Lightweight Directory Services*) incluidos con Windows Server 2008 R2 y versiones posteriores, tales como Windows Server 2012 R2 y Windows Server 2016, permiten aplicar los servicios LDAP v3 estándar utilizables por las aplicaciones diseñadas para utilizar servicios de directorio. Los componentes AD LDS desempeñan el papel de proveedores de servicios de identidades para atender a los escenarios de tipo directorio o para almacenar las identidades externas (como las de socios, proveedores, etc.). La idea de partida proviene de la necesidad o la voluntad de arquitectura de separar estas identidades particulares del almacenamiento de las identidades de la empresa que por norma se almacenan y gestionan empleando los servicios de dominio Active Directory - AD DS.

AD LDS es importante en más de un sentido. En efecto, además de su papel de servicio de directorio LDAP estándar, está soportado por los servicios de federación AD FS así como en el marco de la gestión de directivas de autorización implementadas a través del componente Windows Authorization Manager, también llamado AzMan. Además, en los entornos donde los servicios AD DS se emplean, los servicios AD LDS pueden invocar a los servicios de Active Directory para la autenticación de usuarios que dispongan de una autenticación Windows.

Ventajas aportadas por los servicios AD LDS

Los servicios AD LDS aportan muchos beneficios tanto en términos de funcionalidad como en términos de facilidad de aplicación operativa.

Presentamos estos diferentes puntos a continuación:

- Los servicios AD LDS utilizan la misma tecnología utilizada con los servicios de dominios de Active Directory AD DS.
- Los servicios AD LDS permiten atender mejor las problemáticas complejas separando a los servicios de directorio para la infraestructura Windows de los servicios de directorio necesarios para las aplicaciones.
- Los servicios AD LDS soportan los nombres de tipo X.500, como los O=mycompany y C=ES, donde O significa Organización y C significa País.
- Los servicios AD LDS pueden utilizar las estructuras de seguridad de Windows para los controles de acceso y autenticación. El modelo de administración es idéntico al utilizado desde hace muchos años con Active Directory.
- Los servicios AD LDS son muy fáciles de desplegar en comparación con las limitaciones impuestas a veces con los servicios de dominio Active Directory. Además, no hay ningún efecto secundario o impacto en los servicios AD DS.
- Los servicios AD LDS pueden instalarse y desinstalarse en caliente sin reiniciar el servidor.
- Los servicios AD LDS se instalan en la forma de instancias que pueden funcionar de forma concurrente en el mismo servidor. Cada instancia puede personalizarse en función de las necesidades de las aplicaciones. Por ejemplo, cada instancia tiene su propio nivel de esquema, independiente de forma total de las demás instancias AD LDS y AD DS.

2. AD LDS: Novedades aportadas por Windows Server 2008 R2

En sus principios, Windows Server 2003 soportaba la primera versión de servicios LDAP de forma independiente de la infraestructura de Active Directory. Esta versión, llamada ADAM (*Active Directory Application Mode*), también estaba disponible en el -segundo CD-ROM de Windows Server 2003 R2.

Esta versión fue actualizada de forma significativa con Windows Server 2008 R2. Las nuevas características se detallan a continuación:

- Los servicios AD LDS pueden instalarse como rol en una instalación de Windows Server 2008 R2 en modo Core. Este punto es importante, en particular para los servidores expuestos en Internet. Una instalación en modo Core permite limitar la superficie de ataque del servidor Windows Server 2008 R2, así como el conjunto de las tareas de mantenimiento (actualizaciones críticas, service packs, etc.).
- La instalación de los servicios AD LDS soporta un nuevo modo Install from Media (IFM), el cual permite crear instalaciones personalizadas de los servicios AD LDS.
- Los servicios AD LDS utilizan los servicios de respaldo y restauración de Windows Server 2008 R2. Los servicios AD LDS disponen de las mismas funciones nuevas de auditoría avanzada de cambios que las integradas en los nuevos servicios de dominio Active Directory de Windows Server 2008 R2. Una subcategoría denominada Directory Service Changes se añade para registrar los valores antes y después de modificación de los valores de atributos y objetos AD LDS.
- Los servicios AD LDS asumen un nuevo mecanismo de ayuda a la recuperación, permitiendo la comparación de los datos almacenados en las instantáneas o copias de seguridad a las producción actual. Esta herramienta, DSAmain.exe, llamada *Active Directory database mounting tool*, permite eliminar las innecesarias múltiples restauraciones.
- Los servicios AD LDS soportan el componente MMC Sitios y Servicios de Active Directory. Esta herramienta, conocida por los administradores de Active Directory, puede ahora usarse para administrar la replicación de las diferentes instancias AD LDS.
- Los servicios AD LDS soportan la adición de archivos LDIF personalizados durante la fase de instalación. Estos archivos se desplazan a la carpeta %System Root%\ADAM.
- Los servicios AD LDS soportan las consultas recursivas en los atributos relacionados. Esta funcionalidad permite el soporte de consultas LDAP empleando atributos entrelazados.

AD LDS y AD DS: puntos importantes

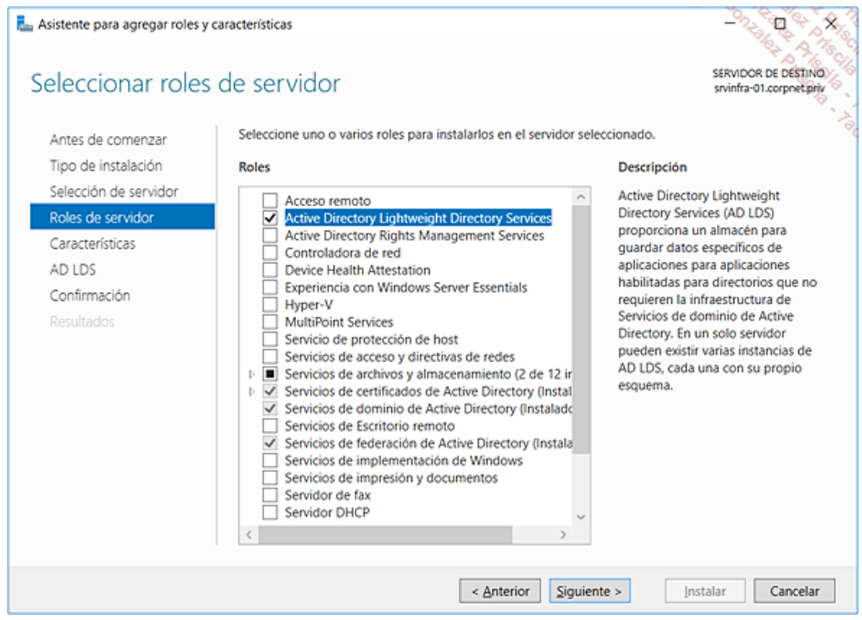
Acabamos de ver que los servicios AD LDS y AD DS comparten la misma tecnología y los mismos principios fundamentales. Sin embargo, es necesario percibir las diferencias que hacen que se trate de componentes funcionales y técnicas radicalmente diferentes. Presentamos estos puntos a continuación:

- Los servidores, los controladores de dominio Active Directory, así como los servidores autónomos pueden ser configurados para incluir los servicios AD LDS.
- Los servicios de dominio AD LDS y los servicios AD DS soportan funcionalidades comunes tales como el modelo de replicación multimaestro, el modelo y las interfaces de programación ADSI (*Active Directory Service Interfaces*), las particiones del directorio de aplicaciones, así como el soporte del protocolo LDAP en modo cifrado LDAP *over Secure Sockets Layer (SSL)*.
- Los servicios de dominio AD LDS y los servicios AD DS son diferentes en los siguientes importantes puntos: los servicios AD LDS no almacenan las estructuras de seguridad de Windows como los usuarios o grupos de usuarios de dominio de Active Directory. Sin embargo, se pueden utilizar en las listas de control de acceso ACL para controlar el acceso a los objetos AD LDS. Dentro del mismo concepto, los sistemas Windows no pueden autentificar usuarios almacenados dentro de los servicios AD LDS, o utilizarlos en sus listas de control de acceso.
- Los servicios AD LDS no tienen ninguna relación directa, ni soportan, las funciones de dominios y bosques de Active Directory, las directivas de grupo, o los catálogos globales.

3. Instalación del Rol AD LDS

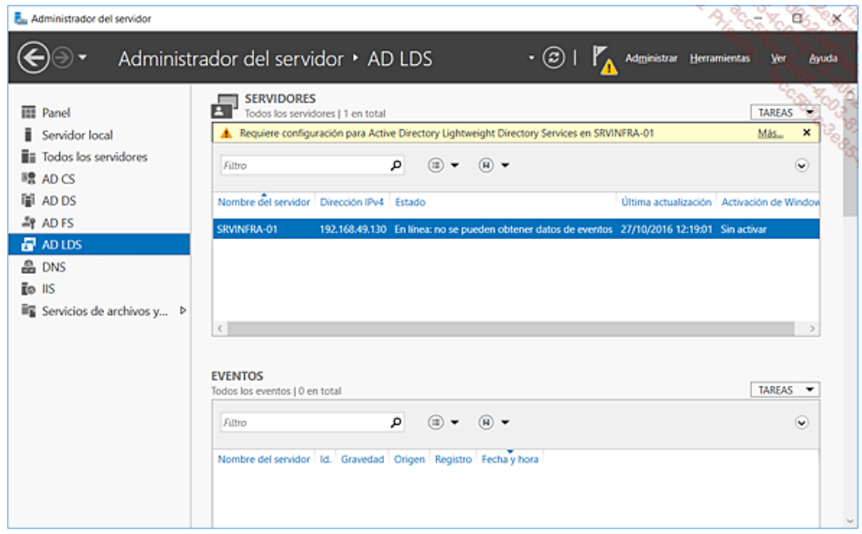
La implementación de los servicios AD LDS se realiza empleando el Administrador de servidores de Windows Server 2016, a través de la

gestión de roles. El único requisito que debe satisfacerse para instalar AD LDS en un servidor es formar parte del grupo de administradores del equipo local.



Añadir los servicios LDAP v3 AD LDS empleando el Administrador del servidor

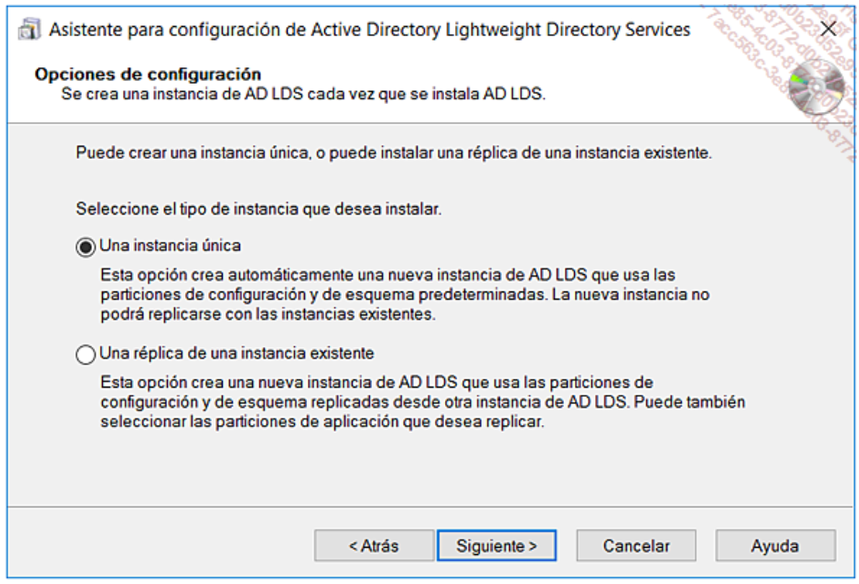
Una vez instalados los componentes AD LDS, podremos instalar varias instancias AD LDS y luego proceder a la carga de nuestro directorio AD LDS. La adición de nuevas instancias es posible de forma directa empleando el Asistente para instalación de servicios AD LDS accesible mediante el acceso directo **Herramientas administrativas** del menú **Inicio**. Durante el inicio de la instalación de una nueva instancia AD LDS empleando el Asistente para instalación de servicios AD LDS, es necesario declarar todos los parámetros relativos a cada una de ellas.



Configuración de los requisitos del sistema después de la instalación de los servicios AD LDS

Como se muestra en la figura anterior, una vez el implementado el rol AD LDS en el servidor, no se crea ninguna instancia AD LDS , y sólo los componentes internos están presentes en el servidor.

Arranque del asistente de instalación de los servicios AD LDS



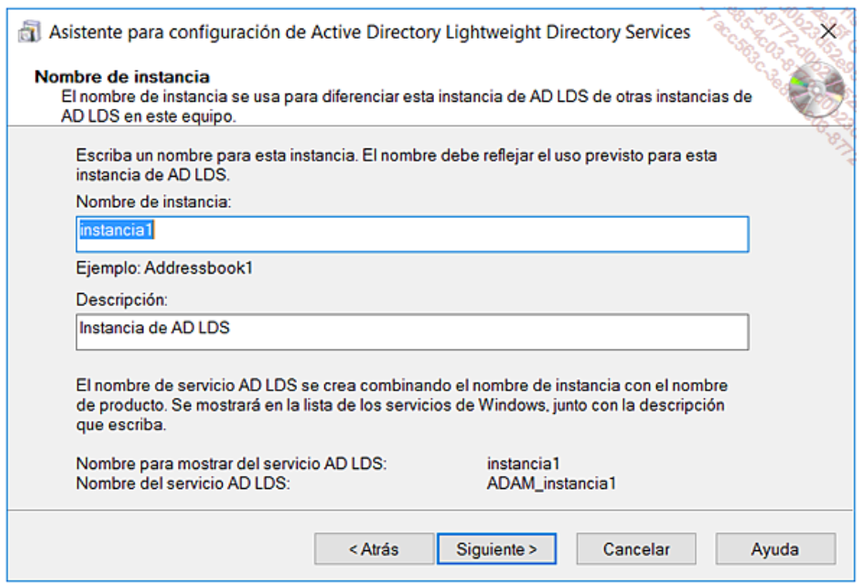
Opciones de instalación de la instancia (Única o Réplica)

Creación de una nueva instancia de AD LDS

El Asistente de instalación de servicios AD LDS permite crear instancias de servicios AD LDS. Una "instancia de servicio" se refiere a una copia de ejecución única AD LDS. Varias instancias AD LDS pueden ejecutarse de forma simultánea en el mismo servidor, lo que no es el caso con los servicios de dominio de Active Directory AD DS. Cada instancia AD LDS tiene su propio motor de almacenamiento privado, un nombre de servicio único en Windows y su propia descripción.

Al término de esta instalación de primera instancia, podemos crear una partición de directorio de aplicaciones. Esta operación es una opción, ya que es posible que esta operación se lleve a cabo durante la instalación de la aplicación utilizando la instancia AD LDS.

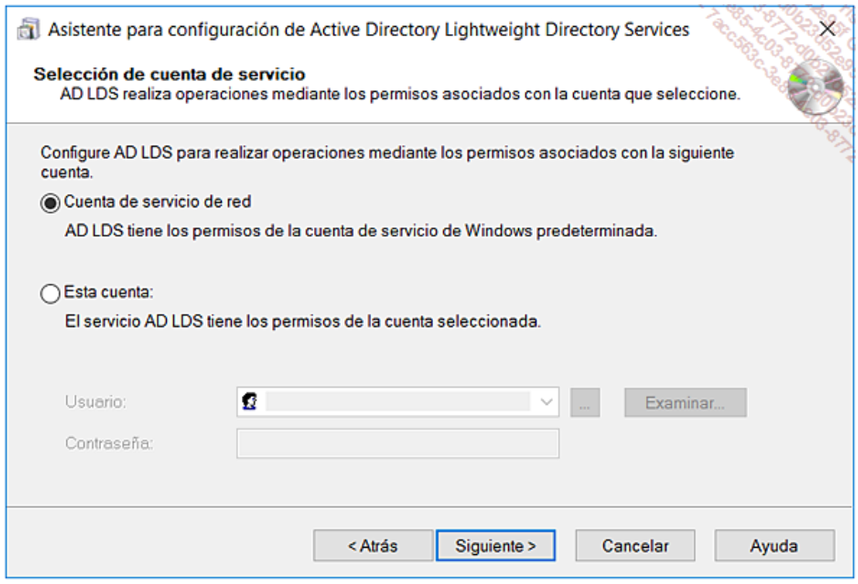
Para llevar a cabo este procedimiento, debemos formar parte del grupo Administradores.



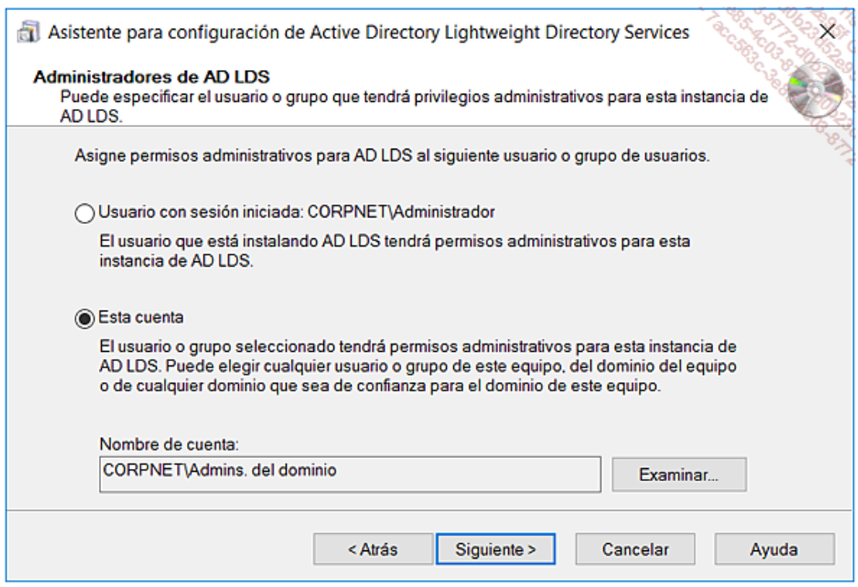
Selección del nombre de la instancia AD LDS

Nombre de la instancia AD LDS y caracteres autorizados

¡Observe! Los nombres de instancias existen en la forma de un contexto de nombres LDAP, como ocurre cuando hablamos de las particiones Active Directory. Por lo tanto, los nombres deben respetar las normas de nombres DNS. Este requisito previo permite declarar los registros SRV asociados a las diferentes particiones y servidores LDAP (RFC 2782 y antes 2052).



Selección de la cuenta de servicio para la instancia AD LDS



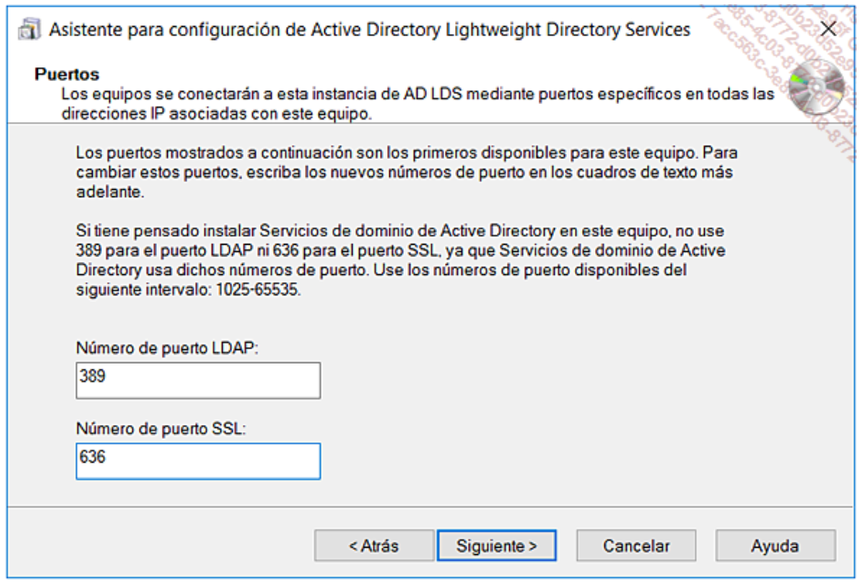
Definición de los privilegios de administración para la instancia AD LDS

Tenga en cuenta que, por defecto, solo el administrador conectado en el momento contará con los permisos de administración sobre la instancia AD LDS en curso de creación. Una mejor práctica consistirá en especificar un grupo de usuarios que tengan a su cargo la administración de esta instancia -en este ejemplo, el Grupo Admins. del dominio- u otro grupo especializado para "la administración de esta aplicación".

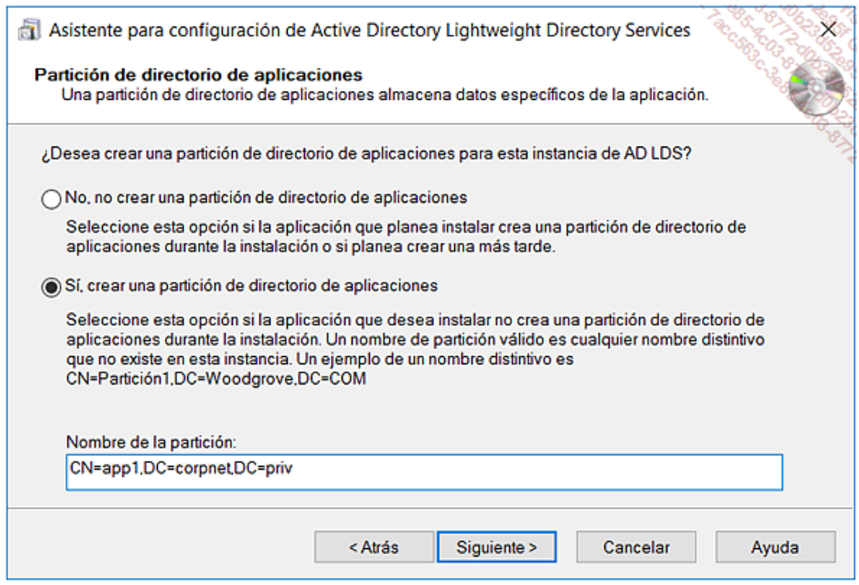
Creación de una nueva réplica AD LDS

Para ofrecer una buena tolerancia a fallos y asumir las funciones de equilibrio de carga, las instancias AD LDS pueden pertenecer a un conjunto de configuración. Todas las instancias de un conjunto deben replicar una partición de configuración común, una partición de esquema, así como cualquier número de particiones de directorio de aplicaciones AD LDS. Para crear la nueva instancia AD LDS y adjuntarla a un conjunto existente, utilice el Asistente para instalación de servicios AD DLS y seleccione la opción **Instalar una réplica de instancia AD LDS**. Necesitará conocer el nombre DNS del servidor que ejecuta la instancia AD LDS perteneciente al conjunto de configuración así como el puerto LDAP especificado durante la creación de la instancia.

También podemos proporcionar el DN (distinguished name) de las particiones del directorio de aplicaciones que deseamos copiar desde el conjunto de configuración a la nueva instancia AD LDS a crear. Tenga en cuenta que para lograrlo debe pertenecer al grupo Administradores.

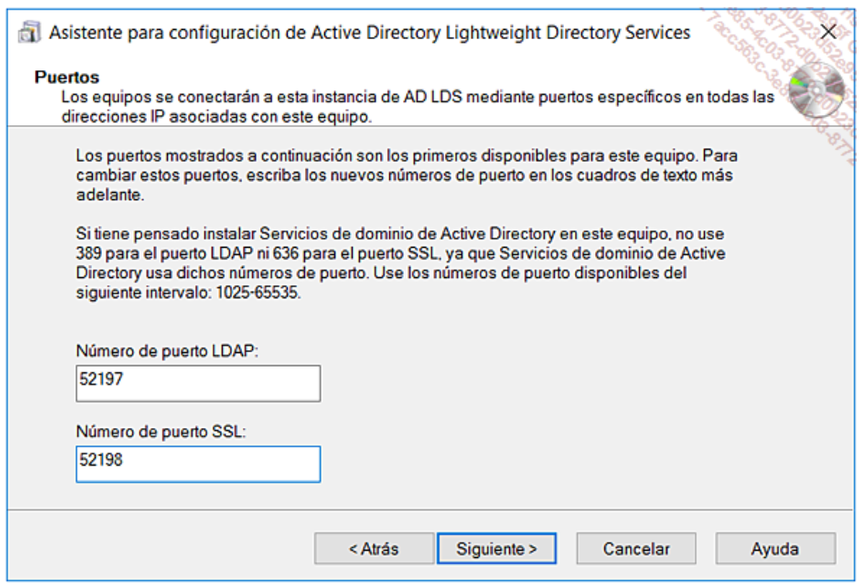


Puertos propuestos por defecto por el Asistente de instalación de servicios LDS en una equipo "no-DC", autónomo o miembro de un dominio Active Directory



Creación de una partición de directorio de aplicaciones empleando el asistente de instalación de los servicios AD LDS

Mientras que las antiguas versiones de los servicios AD LDS, tales como la suministrada con Windows Server 2008, utilizaban los puertos 50000 para LDAP y 50001 para LDAP con SSL, cada instancia de un mismo servidor debe disponer de sus propios puertos. El hecho de que los puertos por defecto AD LDS sean diferentes de los puertos por defecto LDAP permite instalar una o varias instancias AD LDS en un equipo que actúe como controlador de dominio.



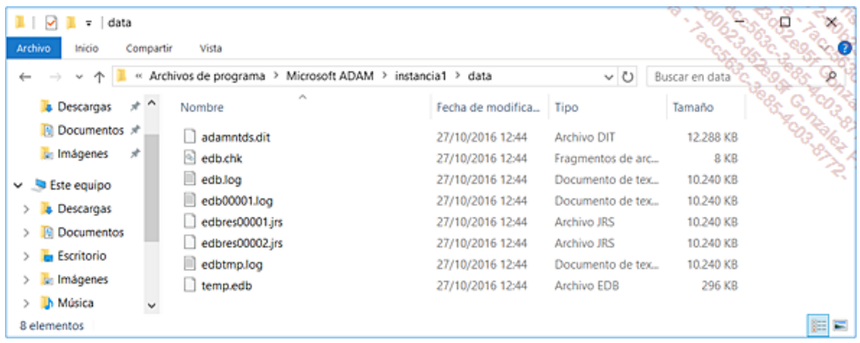
Puertos propuestos por defecto por el Asistente de instalación de servicios LDS en una equipo que dispone del rol de controlador de dominio Active Directory

Una vez declarados estos parámetros, necesitaremos validar la ubicación de los archivos asociados a la instancia AD LDS, elegir la cuenta de servicio asociada a la instancia (por defecto, se trata de la cuenta integrada de Servicio de red), y declarar la cuenta de administración de la instancia.

Ubicación de los archivos de la instancia AD LDS

En la página Directorios, podemos modificar los directorios de instalación por defecto de los archivos de datos (*.DIT) y los archivos de

transacciones (*.log) de la instancia AD LDS. Por defecto los archivos están instalados en el directorio siguiente: C:\Program Files\Microsoft ADAM\instancia1\data.

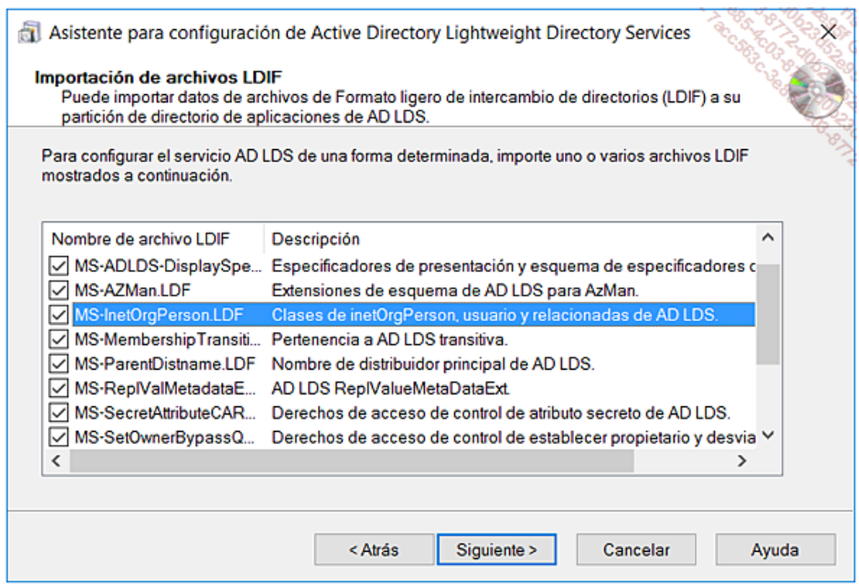


Archivos de la base de datos AD LDS (adamntds.dit) de la Instancia llamada "instancia1".

Observe que los archivos de sistema que contiene las herramientas de administración y los programas AD LDS están instalados en la carpeta C:\Windows\ADAM

Importación de archivos LDIF en la partición AD LDS

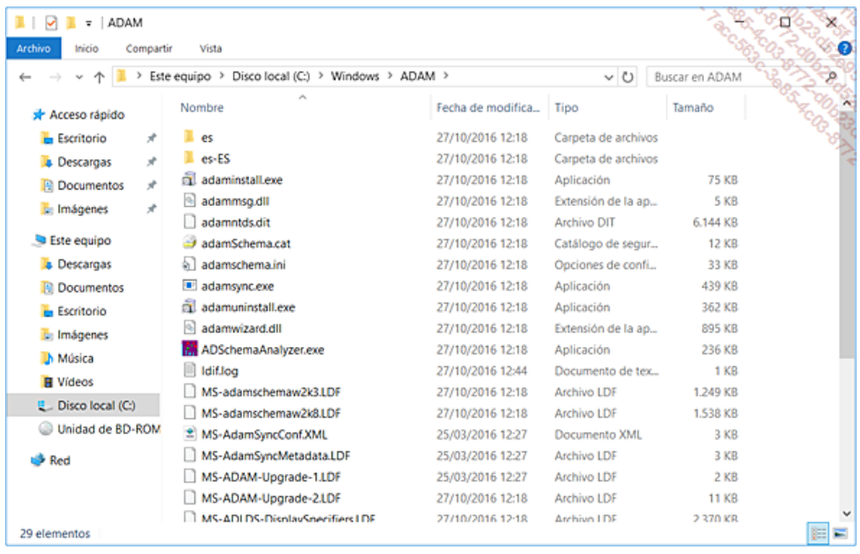
La última etapa consiste en integrar un esquema de directorio adaptado a las necesidades futuras de la instancia.



Definición del esquema LDAP de la instancia AD LDS e importación de archivos LDIF

Esta ventana de selección permite elegir qué archivos .LDF deseamos importar en la instancia AD LDS. A continuación presentamos el detalle de cada uno de los archivos:

- **MS-InetOrgPerson.ldf**: este archivo contiene las definiciones de la clase de objeto "inetOrgPerson".
- **MS-User.ldf**: este archivo contiene las definiciones de la clase de objeto "user".
- **MS-UserProxy.ldf**: este archivo contiene las definiciones de la clase de objeto "userProxy", solo con los atributos obligatorios.
- **MS-UserProxyFull.ldf**: este archivo contiene las definiciones de la clase de objeto "userProxy".
- **MS-ADLDS-DisplaySpecifiers.ldf**: este archivo contiene las definiciones de la clase de objeto "Display specifiers". Este archivo es necesario para el soporte de las herramientas de administración tales como la consola MMC Sitios y Servicios de Active Directory.



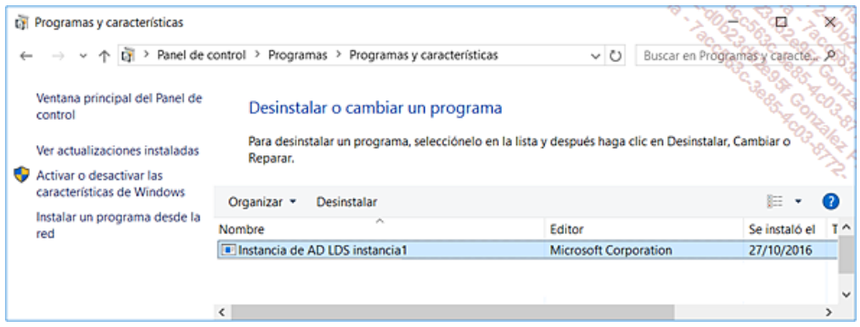
Carpeta C:\Windows\ADAM que contiene los archivos de sistema y herramientas de los servicios AD LDS

Tenemos la posibilidad de integrar los archivos LDIF (*LDAP Data Interchange Format*) personalizados durante la fase de instalación de las instancias AD LDS. Basta con colocar los archivos LDF (LDIF files), además de los suministrados de base, y añadirlos en la carpeta

%SystemRoot%\ADAM. Podemos crear nuestros propios archivos personalizados empleando la herramienta ADSchema Analyzer.

Desinstalación de una instancia AD LDS

La eliminación de las instancias AD LDS creadas se realiza de forma sencilla empleando el icono **Programas y características** del Panel de control del servidor Windows Server 2016.



Uso del Panel de control / Programas y características para eliminar la instancia AD LDS llamada "instancia1".

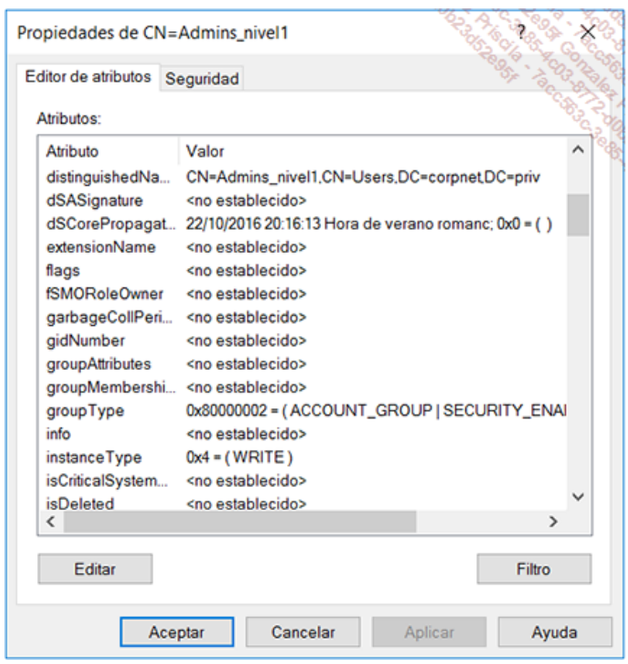
¡Observe! Antes de eliminar el rol AD LDS, use **Programas y características** en el Panel de control para eliminar todas las instancias AD LDS instaladas con anterioridad.

Utilización de la autenticación y control de acceso con AD LDS

El control de acceso a los servicios AD LDS se realiza en dos etapas sucesivas. En primer lugar, AD LDS valida a los usuarios que solicitan el acceso al servicio de directorio, autorizando solo a los usuarios autenticados. Luego, los servicios AD LDS utilizan los descriptores de seguridad ACL en los objetos del directorio para controlar a que objetos tiene acceso el usuario autenticado.

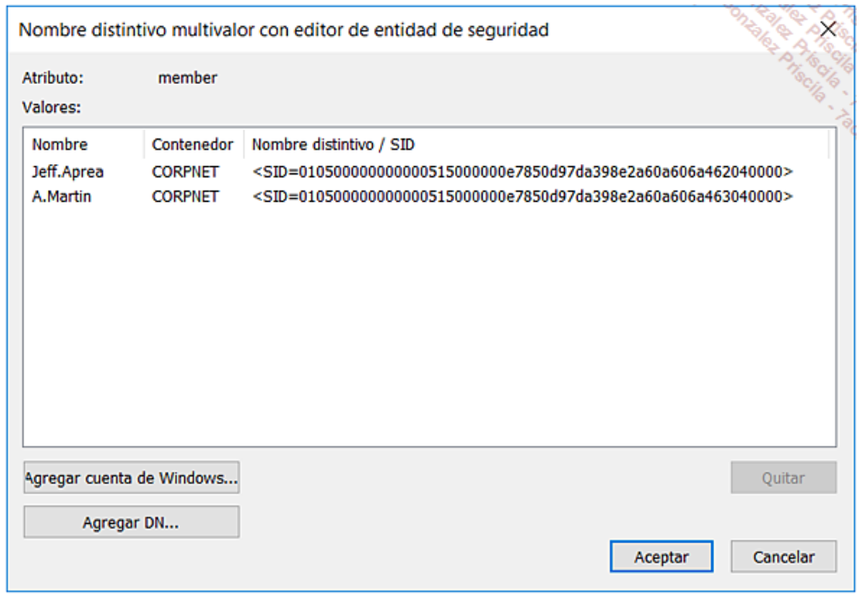
Los usuarios interactúan con los datos del directorio AD LDS a través de las aplicaciones de directorio que acceden a la instancia AD LDS utilizando el protocolo LDAP en el puerto indicado para la instancia. Antes de acceder a los datos, la aplicación muestra la información de identificación del usuario para autenticación o enlace. Esta solicitud incluirá el nombre de usuario, su contraseña y, según el tipo de enlace, un nombre de dominio o nombre de equipo.

Los servicios AD LDS soportan los mecanismos de autenticación y de enlace, así como las solicitudes AD LDS locales y las entidades Windows locales y de dominio.

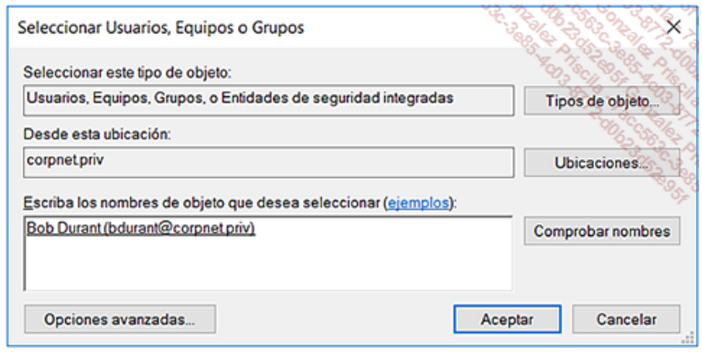


Propiedades del objeto Grupo Admins_nivel1

En este ejemplo, el administrador debe modificar un objeto grupo cuyo DN LDAP es CN=Admins_nivel1,CN=Users,DC=corpnet,DC=priv. La operación a realizar consiste en añadir un usuario miembro de un dominio Active Directory, así como un usuario LDAP existente dentro de la instancia AD LDS actual. Existen varios métodos para realizar esta tarea de administración corriente. Esta vez, el administrador va a utilizar el componente ADSI Edit: Adsiedit.msc.



Modificación del atributo member del Grupo de Directores y añadir cuentas de usuarios locales o miembro del dominio de Active Directory corpnet.priv.



Añadir un usuario de Active Directory dentro de un grupo AD LDS

La ventana de modificación del atributo member permite seleccionar las cuentas de Windows o los nombres únicos, declarados de forma directa, con toda sencillez.

Herramientas de administración AD LDS

Hemos visto que los servicios AD LDS de Windows Server 2012 R2 y Windows Server 2016 proporcionan servicios de directorio genéricos cuyo objetivo principal es proporcionar a los desarrolladores una cierta flexibilidad para la integración de aplicaciones de directorio, sin ninguna dependencia, ni restricciones en relación con los servicios de dominio de Active Directory, AD DS. También hay que recordar el hecho de que los servicios AD LDS tienen su propia topología de replicación y un esquema administrado por separado de los servicios de dominio de Active Directory.

Por estas razones, las herramientas de administración de servicios AD LDS son algo más "bastas", si se compara con las herramientas de administración de Windows Server. Las herramientas que podemos usar para administrar y gestionar las instancias AD LDS son las siguientes:

- **ADSI Edit**: el editor ADSI es un componente MMC integrado de forma directa con Windows Server 2012 R2 y Windows Server 2016. Para ejecutar esta herramienta, puede ejecutar el comando `AdsiEdit.msc`, o bien en un equipo donde esté instalado el rol AD LDS (*Active Directory Lightweight Directory Services*), hacer clic en **Inicio - Herramientas administrativas - Editor ADSI**.
- **Ldp**: el comando `Ldp` no es un componente de software sino un archivo ejecutable. Para arrancar `Ldp`, hacemos clic en **Inicio**, luego con el botón derecho sobre **Símbolo del sistema**, y hacemos clic en **administrador** y escribimos `Ldp` en el intérprete de comandos. El cuadro de diálogo **Ldp** tiene dos componentes: el árbol de la consola y la solapa de información. El árbol de la consola contiene el objeto básico y los posibles objetos secundarios. La solapa de información presenta los resultados de las operaciones LDAP.
- **Csvde**: el comando `csvde` permite importar y exportar datos a partir de los servicios AD LDS o AD DS empleando archivos que contengan datos separados por comas (CSV, *Comma Separated Value*).
- **Ldifde**: el comando `Ldifde` permite crear, modificar y eliminar objetos de directorio. También podemos usar `Ldifde` para extender el esquema, exportar la información relativa a los usuarios y grupos hacia otras aplicaciones o servicios, así como para rellenar AD LDS o AD DS con datos procedentes de otros servicios de directorio.
- **Adamsync**: el comando `Adamsync` permite sincronizar los objetos de los servicios de dominio AD DS con una instancia de los servicios de directorio AD LDS.

¡Observe! Para poder utilizar este comando, debemos importar las definiciones de las clases de usuario que figuran en el archivo MS-AdamSyncMetadata.LDF.

El conjunto de estas herramientas nos permitirá administrar los usuarios y grupos AD LDS, importar las clases de usuario proporcionadas con los servicios AD LDS, sincronizar las instancias AD LDS con los servicios de dominio de AD DS, añadir un usuario AD LDS en el directorio, añadir un grupo AD LDS en el directorio, añadir miembros de un grupo AD LDS o eliminar, visualizar o definir los permisos de un objeto directorio, desactivar o activar un usuario AD LDS, definir o modificar la contraseña de un usuario AD LDS y también añadir una unidad organizativa en el directorio.

4. Referencias para AD LDS con Windows Server

Para más detalles acerca de las operaciones de administración y de gestión de los servicios AD LDS podremos referirnos a los enlaces siguientes:

- Active Directory Lightweight Directory Services Overview: https://technet.microsoft.com/en-us/library/hh831593(v=ws.11).aspx
- Using Active Directory Lightweight Directory Services: https://technet.microsoft.com/es-es/aa772138
- Active Directory Lightweight Directory Services Reference: https://technet.microsoft.com/es-es/aa705889

- Active Directory Collection: https://technet.microsoft.com/en-us/library/cc780036(v=ws.10).aspx
- Using Active Directory Lightweight Directory Services: https://msdn.microsoft.com/en-us/library/aa772138(v=vs.85).aspx
- Why Use Active Directory Lightweight Directory Services?: https://msdn.microsoft.com/en-us/library/aa772141(v=vs.85).aspx

La mayoría de lo enlaces están disponibles en ingles y ubicados en los sitios Microsoft Technet US y Microsoft MSDN US.

5. Evoluciones del rol AD LDS

La evolución más notable de los servicios AD LDS desde Windows Server 2003 hasta Windows Server 2016 se refiere sin duda a la versión entregada con Windows Server 2008 R2. En efecto, con esta versión, los servicios AD LDS aprovechan los avances logrados en los servicios de dominio AD DS. Estas nuevas características se detallan a continuación:

- el soporte de la funcionalidad de papelera Active Directory está implementado para permitir a los administradores recuperar objetos borrados por error.
- los cmdlets PowerShell Active Directory también son utilizables en las instancias LDAP AD LDS;
- el soporte del Servicio Web Active Directory: estos servicios proporcionan una interfaz web service para los dominios Active Directory, las instancias AD LDS y también las instantáneas de Active Directory.

Las versiones incluidas con Windows Server 2012 R2 y Windows Server 2016 no aportan ninguna evolución funcional significativa a los servicios LDAP incluidos con los servicios AD LDS.

Active Directory Rights Management Services (AD RMS)

1. Introducción

Windows Server 2016 y las versiones anteriores como Windows Server 2012 R2 y Windows Server 2008 R2 incorporan los servicios de gestión de derechos digitales, los cuales estaban disponibles en su primera versión con Windows Server 2003, en la forma de una descarga gratuita.

Los servicios de gestión de derechos digitales de Active Directory, AD RMS (*Active Directory Rights Management Services*), permiten a las empresas abordar la problemática de protección de la información digital. Esta tecnología permite a las aplicaciones compatibles proteger los documentos digitales de accesos no autorizados, ya estén estos documentos situados dentro o fuera de la red de la empresa y las operaciones sean efectuadas en modo conectado o desconectado. Los servicios AD RMS son en particular necesarios para las empresas que deben proteger datos sensibles que pueden tomar cualquier forma digital, o incluso mensajes confidenciales.

Ofrecen también la definición de directivas de derechos digitales persistentes que permitirán a las empresas respetar las directivas de seguridad definidas al mas alto nivel. Esta tecnología permite aproximarse a las exigencias en materia de seguridad de la empresa, sobre todo cuando se trata de documentos confidenciales que deben transmitirse a socios o proveedores.

Para conseguirlo, los servicios AD RMS nos permiten crear los elementos siguientes:

- **Entidades autorizadas**: la empresa podrá declarar entidades de confianza como usuarios, equipos o grupos. Todas estas entidades tienen la capacidad de participar en la infraestructura AD RMS.
- **Los permisos de uso y condiciones**: podemos asignar permisos de uso y condiciones que las entidades autorizadas podrán utilizar para acceder a los documentos bajo el control de RMS. La tecnología AD RMS nos permite gestionar los derechos de uso más elementales, como los derechos de reproducción, copia, impresión y copia de seguridad o edición. También es posible gestionar los permisos más específicos, como por ejemplo el permiso de transmitir un mensaje por correo electrónico, o fijar una fecha de expiración que haga que el documento no pueda ser utilizado.
- **Las exclusiones específicas**: el administrador tiene la posibilidad de impedir que entidades particulares o aplicaciones accedan a datos protegidos por AD RMS.
- **Cifrado de datos**: el hecho de proteger los datos digitales empleando la tecnología RMS implementa de forma automática el cifrado de datos. La única manera de acceder a los datos es conseguir una autenticación que valide la identidad de una entidad aprobada.

2. Conceptos fundamentales

Una infraestructura AD RMS se compone de componentes servidor, componentes cliente y por supuesto aplicaciones compatibles con la tecnología de gestión de derechos AD RMS, como Microsoft Office 2012, 2013, 2016 y O365, pero también aplicaciones que gestionan formatos específicos como los archivos Adobe PDF. El conjunto de estos componentes realiza las funciones siguientes:

- **Emisión de licencias de publicación**: cuando un documento está protegido, se crea una licencia de publicación para el contenido en cuestión. La licencia emitida corresponde a los derechos de uso específicos de un documento de forma tal que este puede ser distribuido y esta se encuentra integrada de forma directa en el interior del documento protegido. De esta forma, los usuarios pueden transmitir los documentos digitales protegidos a los colaboradores de la empresa o a destinatarios situados en el exterior de la empresa. Los usuarios externos pueden formar parte de otro bosque Active Directory aprobado mediante los servicios de federación AD FS o en Internet empleando una cuenta Microsoft. Esta cuenta permitirá al usuario acceder de forma gratuita a los servicios ubicados en la nube pública Microsoft Azure tales como la mensajería Outlook.com. También podrá utilizarse con Skype, Windows Phone, OneDrive y Xbox.
- **Adquisición de licencias**: cuando los usuarios acceden a un contenido protegido, los componentes AD RMS son invocados y las consultas son enviadas a éstos. El Servicio de licencias AD RMS funcionando en el clúster emitirá entonces una licencia de uso correspondiente a los derechos y condiciones de uso especificados en la licencia de publicación. Los derechos y condiciones de uso se convierten en persistentes y serán aplicados de forma automática con independencia de dónde se utilice el documento.
- **Creación de plantillas de directivas de derechos**: los usuarios autorizados dentro de la plataforma AD RMS pueden crear y gestionar los documentos protegidos utilizando aplicaciones compatibles con la tecnología de gestión de derechos digitales AD RMS basándose en plantillas de derechos de uso predefinidos y aplicables con facilidad.

3. ¿Por qué utilizar los servicios AD RMS?

Por ejemplo, un director de marketing o un Responsable financiero crea archivos ofimáticos Microsoft Office o archivos PDF Adobe Acrobat Reader que contienen información muy confidencial. Estos archivos almacenados en un servidor de empresa están copiados en una llave USB y utilizados en otra máquina, por ejemplo, en casa. En este momento, cualquiera puede acceder a esta llave USB o a un equipo que no forma parte de la red de la empresa y puede abrir los archivos, leerlos, o también imprimirlos. La solución de gestión de derechos digitales AD RMS nos permitirá responder a esta problemática para que por una parte los documentos sean codificados, y por otra parte no puedan ser abiertos por usuarios no autorizados.

Para más información sobre la gestión de derechos digitales consulte la página de Microsoft " Design, Deploy, and Use Rights Management" en la dirección: https://technet.microsoft.com/en-us/dn175750

4. AD RMS: novedades aportadas por Windows Server 2016

Con esta nueva versión de Windows Server 2016 los servicios AD RMS disponen de nuevas funcionalidades y un posicionamiento que evoluciona en función de las ofertas de servicios propuestos por Microsoft en Azure. Estos se listan a continuación.

Nuevo rol AD RMS para Windows Server 2016 y nueva consola MMC

Los servicios AD RMS se implementan en la forma de un nuevo rol de servidor: el hecho de que los servicios AD RMS se integren en Windows Server 2016 y Windows Server 2012 R2 en la forma de un rol dentro del administrador de servidor facilita de manera significativa la configuración de servicios AD RMS. La nueva consola MMC Administrador del servidor lista e instala todos los servicios y componentes necesarios, tales como Message Queuing e IIS, e instalará incluso los servicios de la base de datos interna de Windows (WID para *Windows Internal Database*), si no se especifica el uso de una base de datos remota de tipo SQL Server.

La administración se realiza a través de un nuevo componente MMC 3.0, mucho más intuitivo que la anterior administración web utilizada con las antiguas versiones de la solución.

Integración AD RMS / AD FS

Los servicios de federación AD FS cuentan ahora con una integración total con AD RMS. El soporte de los mecanismos de federación dentro de la plataforma AD RMS permite a las empresas la posibilidad de escenarios de colaboración con una seguridad máxima donde las identidades y accesos externos son necesarios.

Ahora, la integración de los servicios de federación AD FS permite crear las aprobaciones de federación entre los distintos socios.

¡Observe! Para que un cliente AD RMS pueda utilizar las aprobaciones ofrecidas por los servicios de federación AD FS, es indispensable utilizar el módulo cliente AD RMS incluido en Windows 7 o las versiones de Windows posteriores. Los antiguos clientes RMS no soportan

los servicios de federación AD FS.

Auto-inscripción de los servidores AD RMS

Los servidores AD RMS entregados con Windows Server 2008 R2 hasta Windows Server 2016, tienen la posibilidad de activarse de forma automática, haciendo inútil el procedimiento de inscripción en línea o fuera de línea de los servicios RMS ante la autoridad Raíz RMS situada en la nube de Microsoft.

La inscripción de un servidor AD RMS es una tarea esencial que incluye la creación y la firma de un certificado de licencia de servidor - SLC (*Server Licensor Certificate*) - que permite al servidor AD RMS emitir los certificados y licencias.

AD RMS y acceso a Internet para la inscripción: en las versiones anteriores, el certificado SLC era firmado por un servicio de inscripción en línea que se implementa a través de Internet por Microsoft (Microsoft Enrollment Service). Este punto requería que el servidor RMS u otro equipo tuviera acceso a Internet. Esta limitación se ha suprimido al permitir que el servidor AD RMS firme su propio certificado SLC (*Server Licensor Certificate*).

Nuevos roles administrativos AD RMS

Para mejorar el soporte de los mecanismos de delegación y por lo tanto mejorar el control del entorno, contamos con nuevas funciones de administración. Estos nuevos roles administrativos se implementan a través de nuevos grupos locales adaptados a cada nuevo rol.

¡Observe! Cuando los servicios AD RMS se instalan en un controlador de dominio, el programa de instalación crea grupos de dominio locales. Aunque esta configuración está soportada, se recomienda aplicar los servicios AD RMS en una VM dedicada para no contaminar los roles de tipo Controlador de Dominio, DNS y catálogo global.

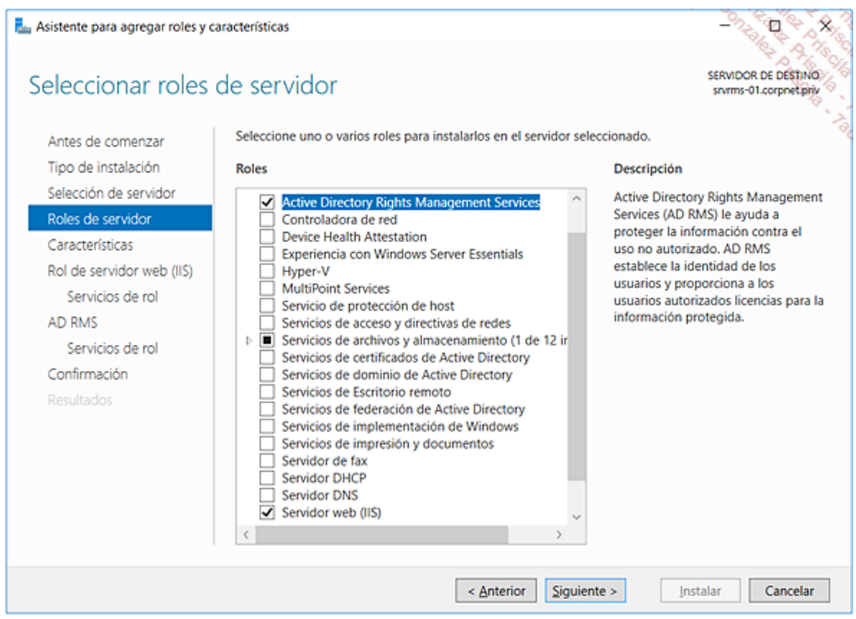
Los nuevos grupos AD RMS son los siguientes:

- **Grupo de servicio AD RMS**: los miembros de este grupo pueden ejecutar los servicios que hayan sido detenidos por los servicios AD RMS.
- **Administradores de empresas AD RMS**: los miembros de este grupo pueden gestionar todas las directivas y parámetros AD RMS.
- **Administradores de plantillas AD RMS**: los miembros de este grupo solo pueden gestionar las plantillas AD RMS.
- **Auditores AD RMS**: los miembros de este grupo solo pueden gestionar los registros y la creación de informes AD RMS.

Mejores prácticas en relación con los grupos AD RMS: la cuenta de servicio declarada durante la instalación de los servicios AD RMS se inserta de forma automática en el grupo Grupo de servicio AD RMS. Del mismo modo, la cuenta de usuario que realiza la instalación de servicios AD RMS se inserta de forma automática en el grupo Administradores de empresas AD RMS. Si contamos con varios servidores AD RMS, se recomienda la creación de grupos de seguridad en el dominio Active Directory y añadirlos a sus grupos locales respectivos en los diferentes servidores AD RMS.

5. Agregar el rol AD RMS

Al igual que otros roles incluidos con Windows Server 2016, la instalación se inicia mediante el Administrador del servidor y la función Agregar roles.



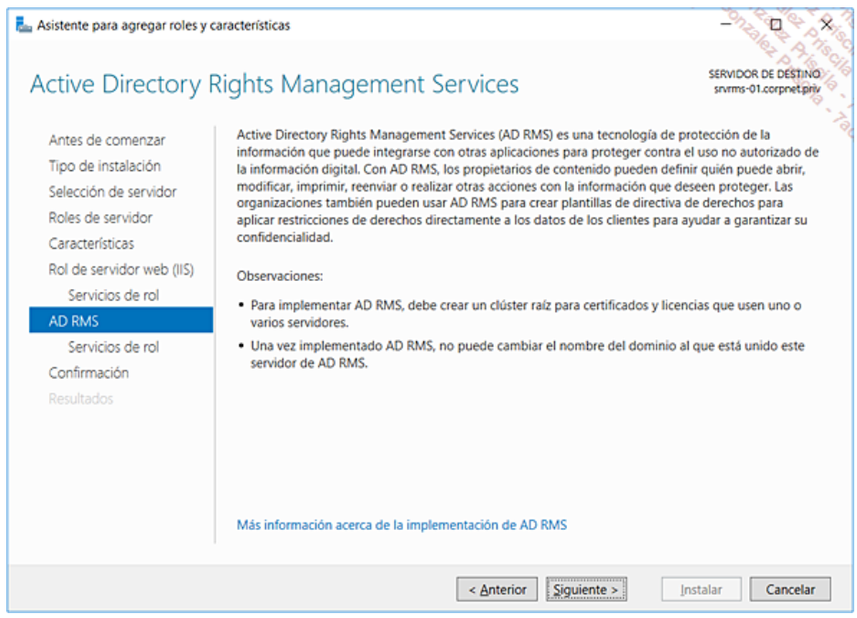
Agregar el rol AD RMS (Active Directory Rights Management Services)

Para instalar AD RMS, el servidor debe cumplir con los siguientes requisitos previos:

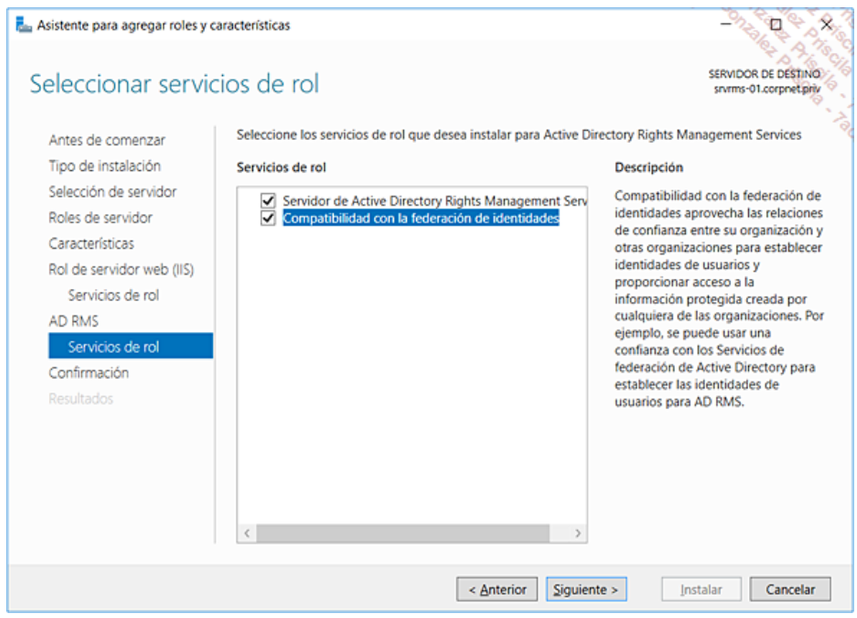
- Usar Windows Server 2016 o Windows Server 2012 R2 en cualquier edición, Estándar o Datacenter.
- Usar NTFS como sistema de archivos para soportar los servicios AD RMS.
- Utilizar el .NET Framework 4.6 con las siguientes características: Services WCF / Activation HTTP y ASP.NET 4.6.
- El servidor Web IIS 10 debe estar instalado con las siguientes opciones:
  - Desarrollo de aplicaciones: ASP.NET 4.6, Extensions ISAPI, Filtros ISAPI y Extensibilidad .NET 4.6.
  - Funcionalidades HTTP comunes: documento por defecto, exploración de directorios, Errores HTTP, Redirección HTTP, Contenido estático.
  - Integridad y diagnóstico: registro HTTP, Seguimiento de trazas, herramientas de conexión, Observador de solicitudes.
  - Rendimiento: compresión del contenido estático.
  - Seguridad: filtrado de las solicitudes, Autenticación de Windows.

- Servicio de activación de los procesos de Windows: API de configuración, Modelo de proceso.

- Los servicios AD RMS deben instalarse en un dominio Active Directory, sabiendo que los controladores de dominio deben utilizar Windows Server 2008 SP1 como mínimo, o cualquier versión posterior.
- Los usuarios deberán obtener las licencias y publicar documentos protegidos siendo imperativo contar con una dirección e-mail como atributo de Active Directory.

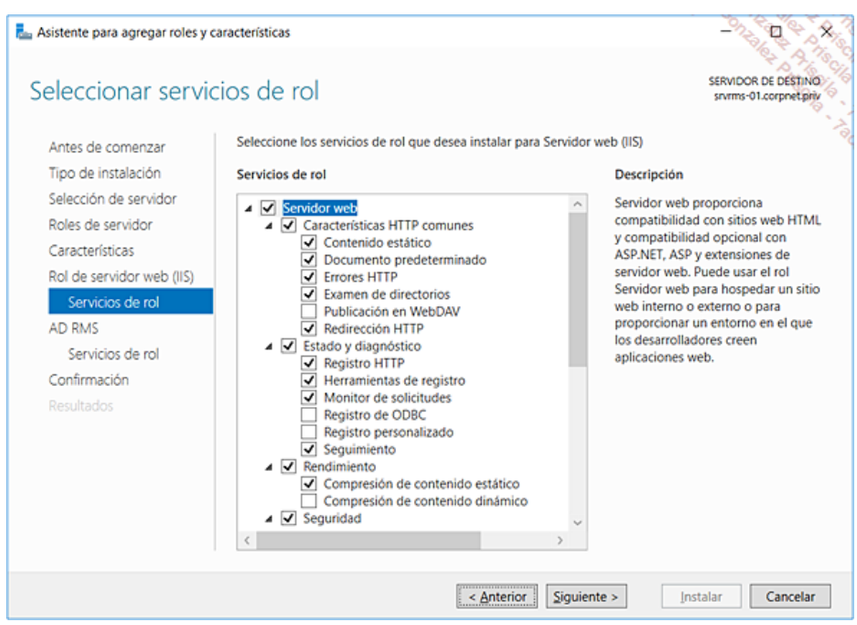


Configuración de los servicios AD RMS



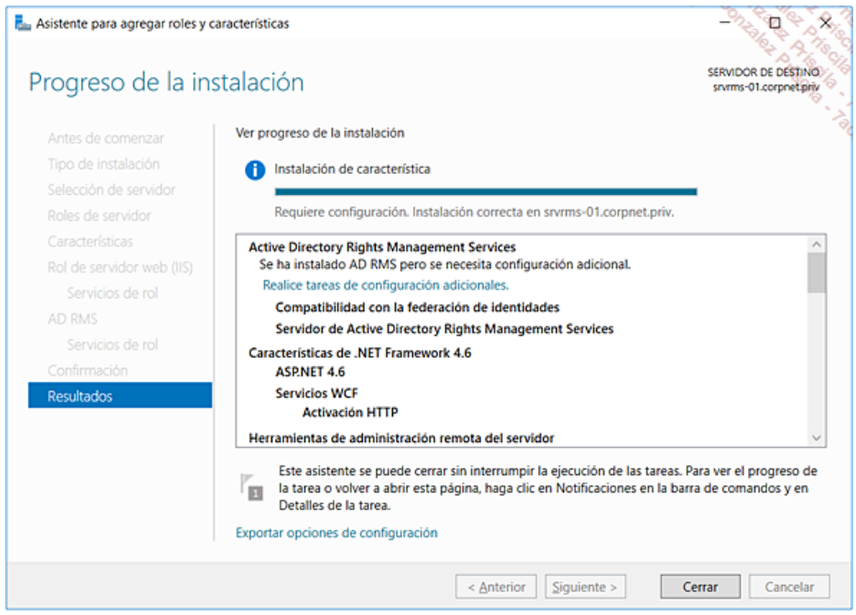
Agregar los servicios de rol AD RMS y soporte de servicios de federación AD FS

La opción para el soporte de la federación de identidades no es obligatoria. Permite ofrecer los servicios AD RMS a usuarios de otra empresa que no disponen de servicios AD RMS, y esto a través de Internet.



Agregar los servicios de rol de IIS 10 para soportar AD RMS

Los servicios de rol necesarios para el buen funcionamiento de AD RMS son seleccionados de forma automática por el Asistente de roles y características.



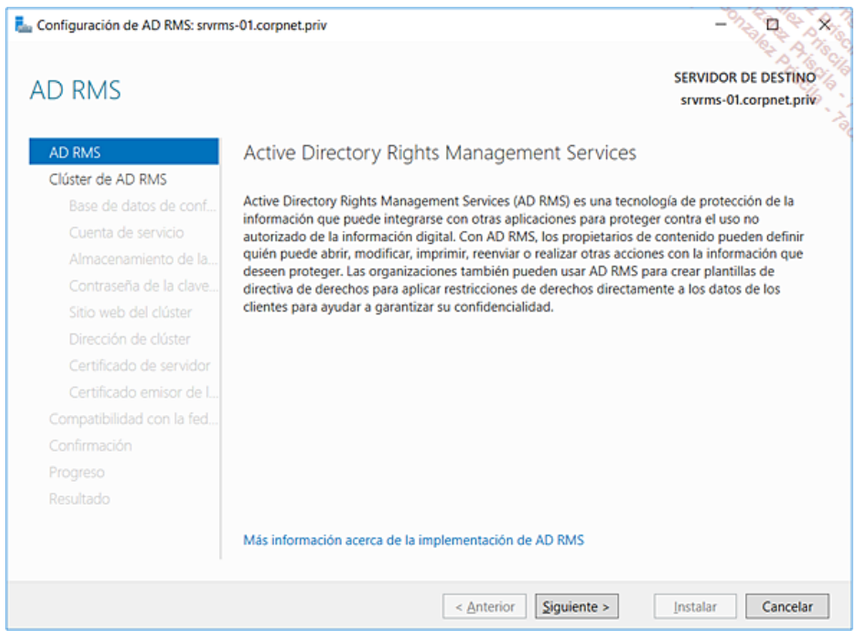
Final de la adición de la función AD RMS y arranque de la configuración del Clúster AD RMS

6. Creación del clúster AD RMS

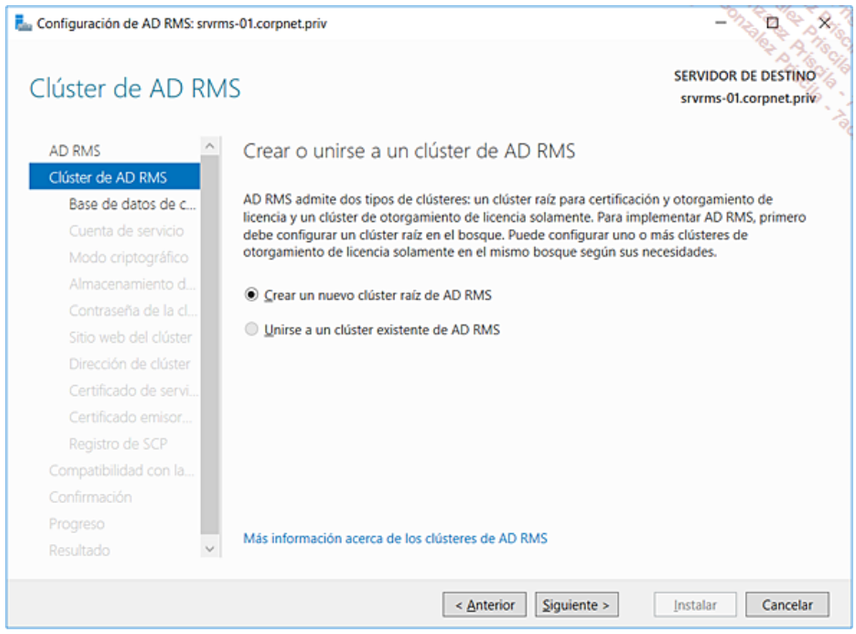
Una vez añadido el rol AD RMS al servidor, podemos comenzar con la configuración del clúster AD RMS. A continuación listamos los pasos de la configuración:

1. Instalación de una base de datos para contener la configuración de la plataforma AD RMS.
2. Declaración de la cuenta de servicio.
3. Almacenamiento de la clave del clúster y la contraseña asociada.
4. Configuración de la URL del sitio web del clúster.
5. Configuración de la URL del sitio web del clúster.
6. Configuración de los servicios de federación AD FS

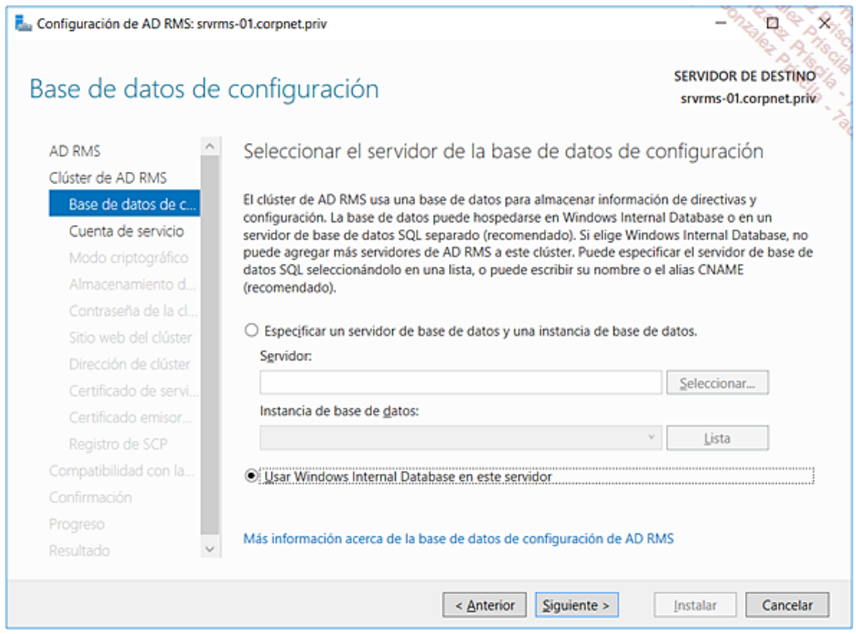
Las imágenes siguientes muestran el proceso de creación y configuración del clúster AD RMS.



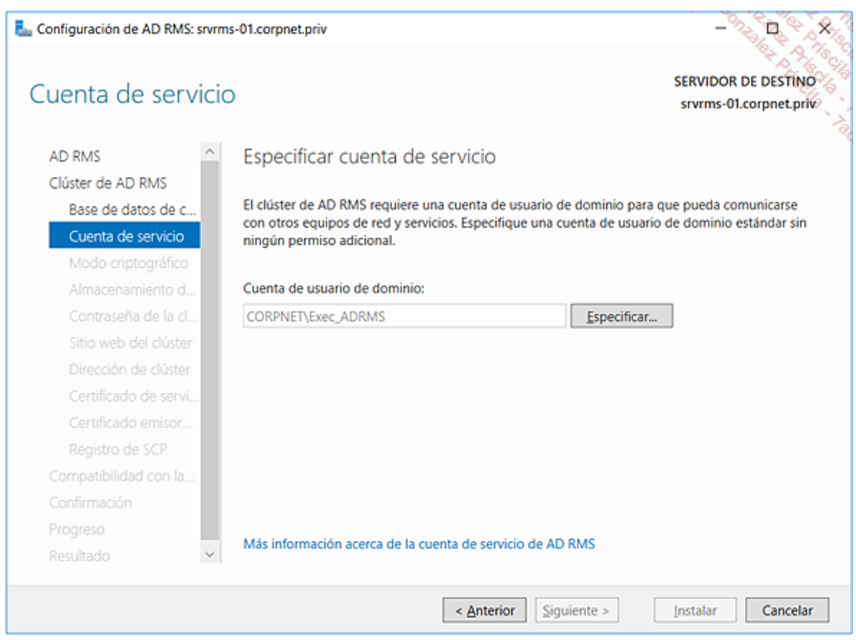
Arranque de la configuración AD RMS



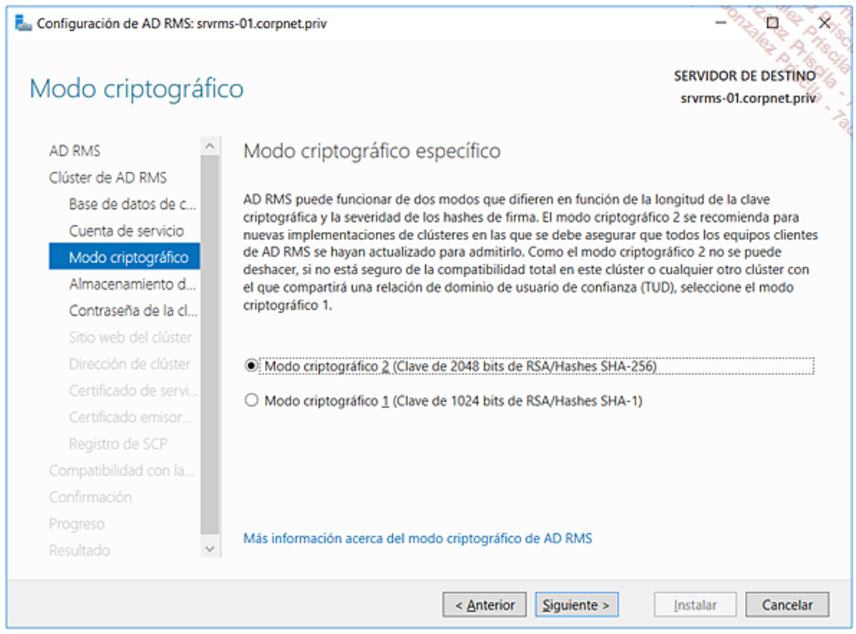
Creación de un nuevo clúster raíz AD RMS



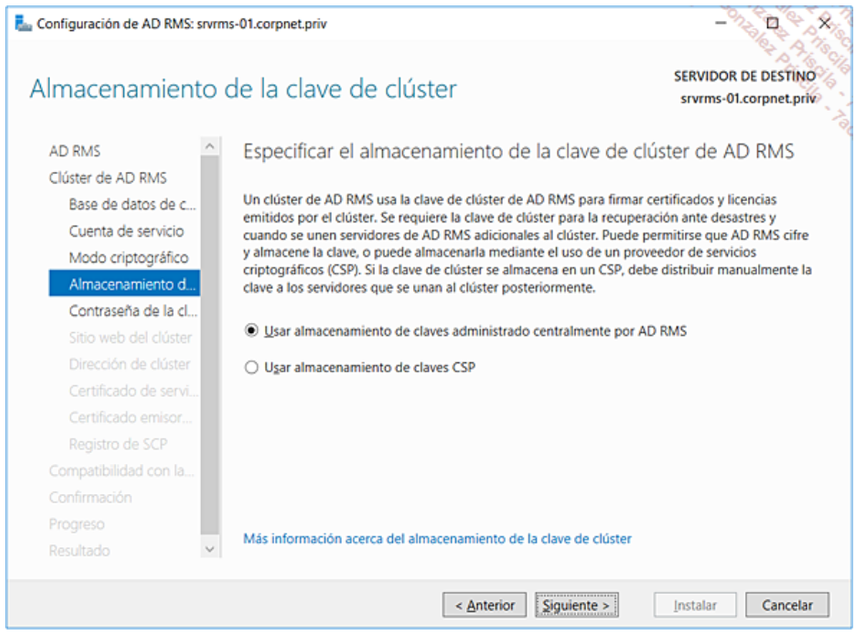
Selección de un servidor de base de datos de configuración



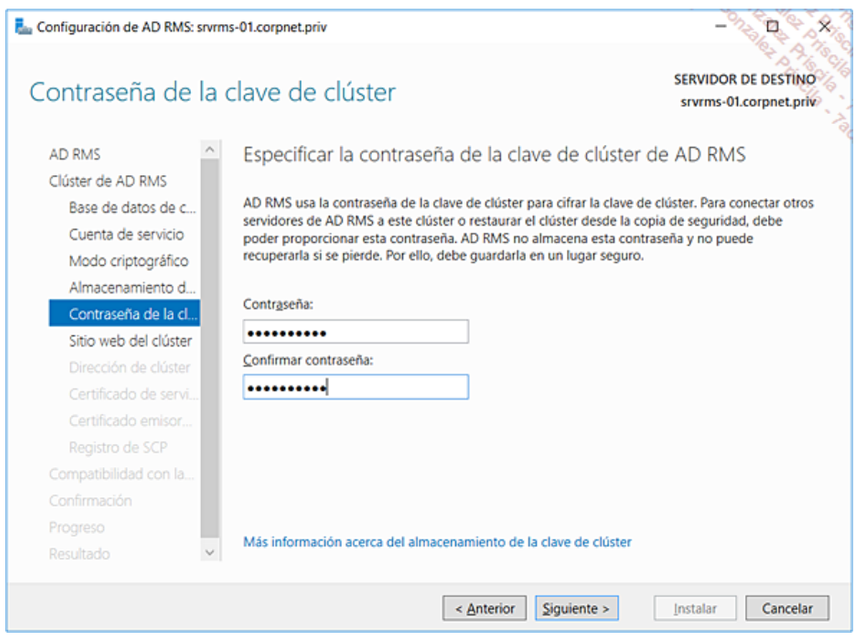
Declaración de la cuenta de servicios AD RMS.



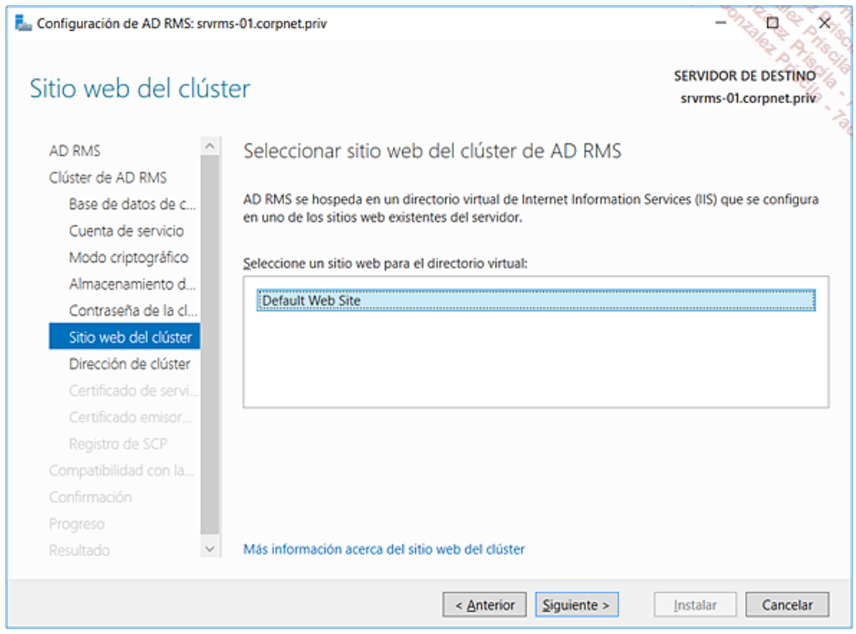
Selección del modo de cifrado 1 (SHA-1) o 2 (SHA-256)



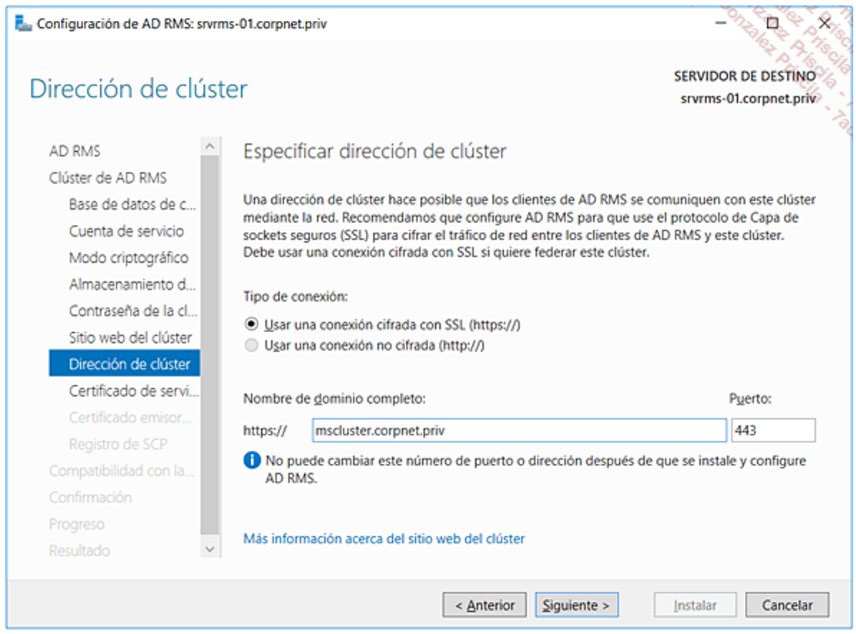
Selección del almacenamiento centralizado para albergar la clave del clúster



Definición de la contraseña de recuperación de la clave del clúster AD RMS

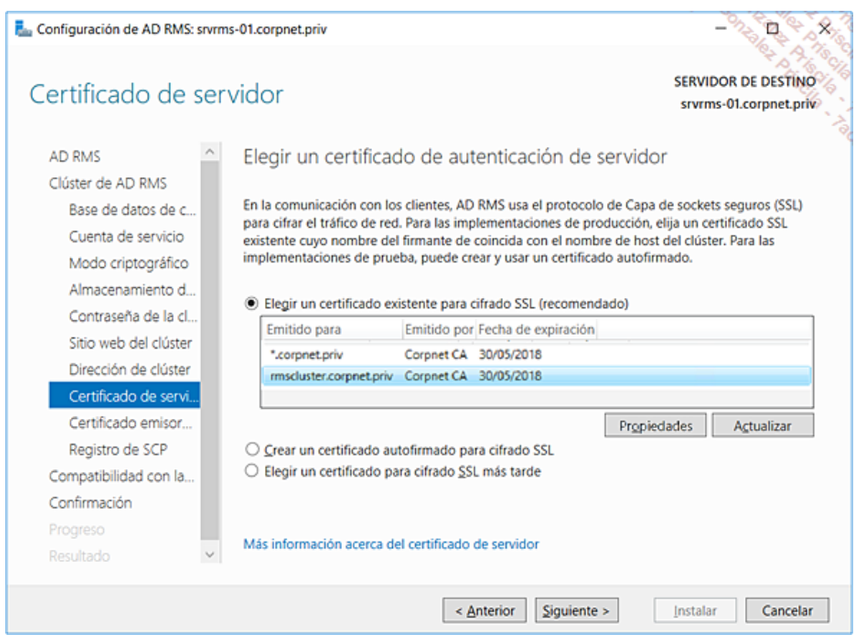


Selección del sitio Web IIS para albergar al directorio virtual AD RMS



Definición de la URL HTTPS del Clúster

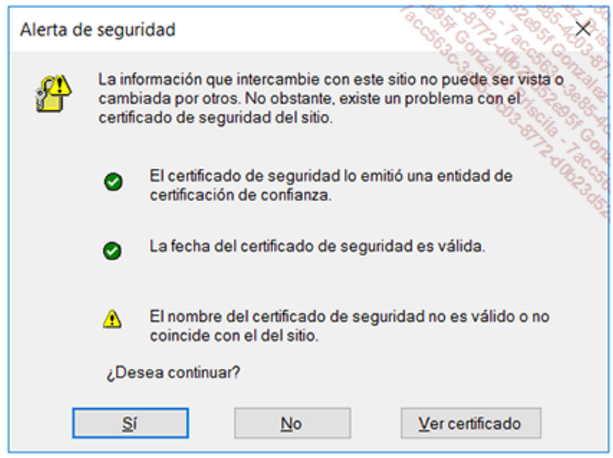
En cuanto al tipo de conexión: observe que el certificado deberá ser instalado antes de la configuración de esta etapa. En caso contrario, el Asistente de configuración AD RMS solo permitirá elegir el protocolo HTTP y no el Protocolo HTTPS.



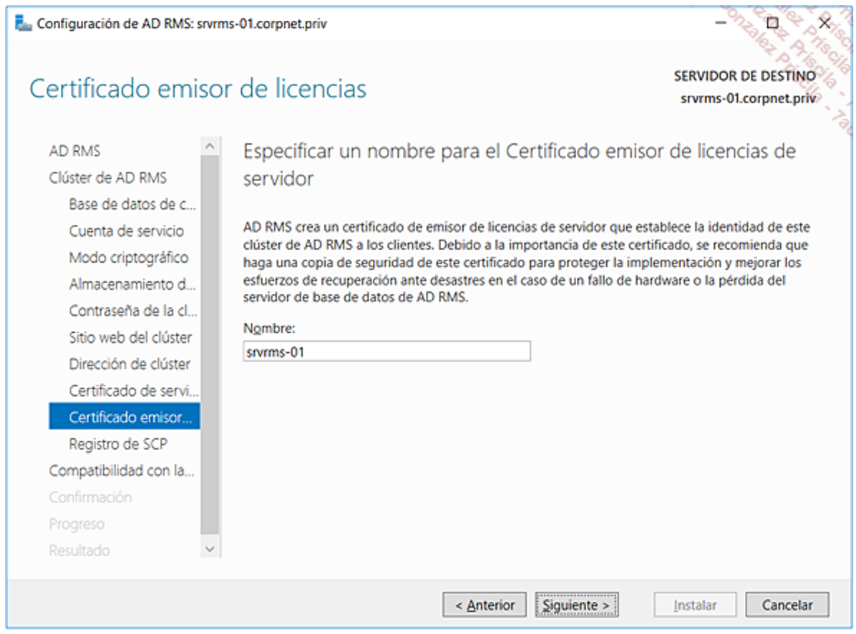
Selección del certificado para el cifrado SSL

La elección del certificado es importante: para las configuraciones AD RMS de producción, Microsoft recomienda utilizar un certificado emitido por una autoridad certificadora de confianza y declarar el nombre del clúster AD RMS como nombre de sujeto. Tenga en cuenta que la utilización del nombre del clúster AD RMS es indispensable. La utilización de un certificado de tipo wildcard como *.corpnet.priv no es

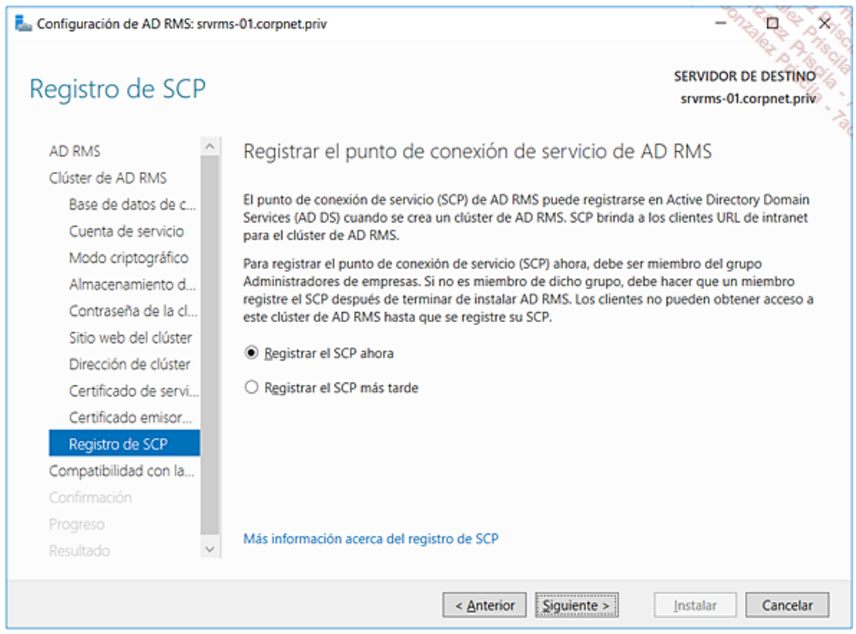
adecuada y provocará un error de forma sistemática indicando que el nombre es incorrecto.



Error cuando el nombre del sujeto utilizado en el certificado no es el del clúster AD RMS



Nombre del certificado de licencia servidor del clúster AD RMS



Inscripción del SCP AD RMS en Active Directory

En relación con el registro del SCP (*Service Connection Point*) en Active Directory: este parámetro es muy importante porque permite a los clientes integrados en Active Directory localizar los servicios AD RMS sin ninguna configuración del puesto de trabajo. Esta operación requiere privilegios de tipo Administradores de empresas ya que los parámetros se graban en la partición de Configuración. El objeto SCP necesario para los clientes AD RMS es creado de forma automática durante la configuración del clúster AD RMS, pero esta operación puede realizarse en un segundo tiempo por un administrador con los privilegios necesarios. En este caso, proceda como sigue:

Conéctese al clúster a través del servidor para el que debemos registrar el punto de conexión de servicio.

Abra la consola de gestión MMC servicios AD RMS.

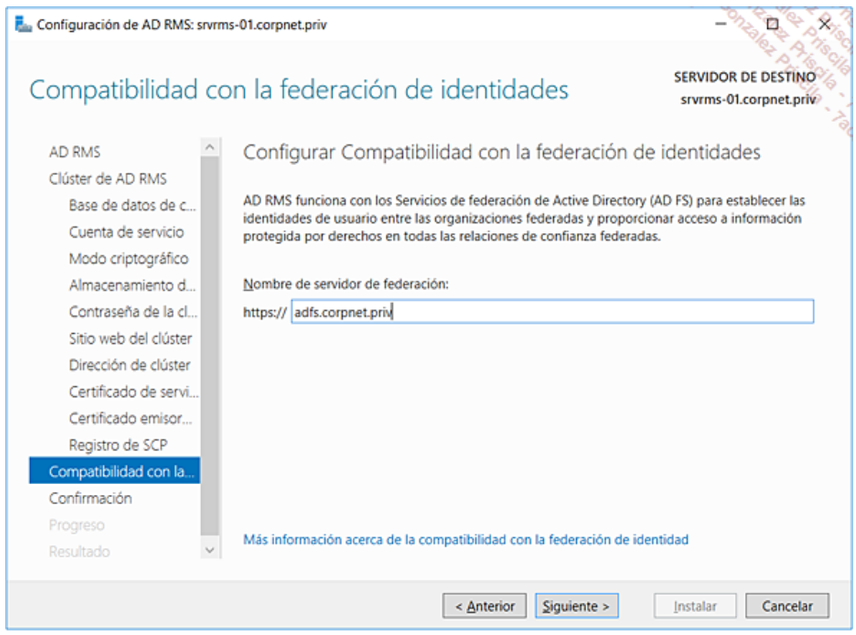
Acceda a las **Propiedades** del clúster AD RMS.

Seleccione la pestaña **SCP**.

Active la opción **Cambiar SCP**.

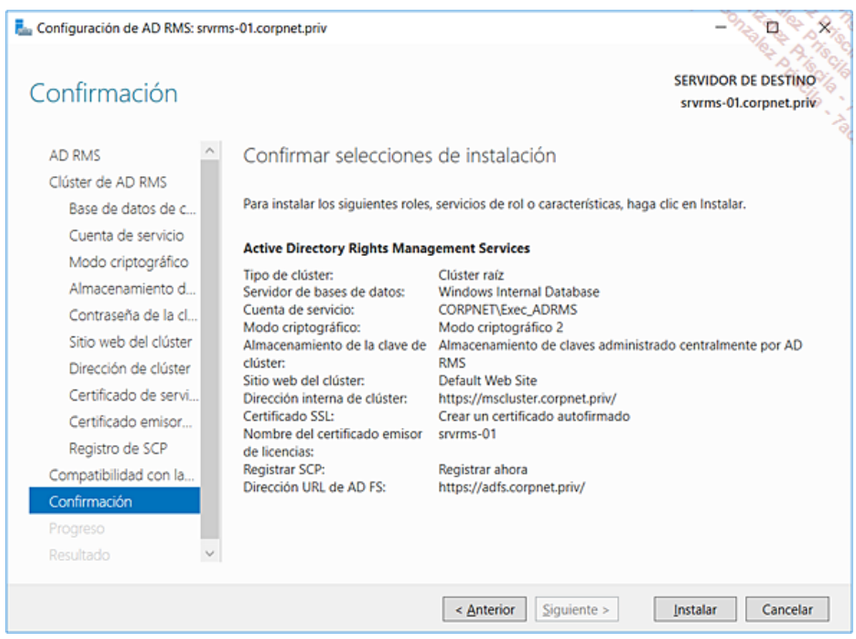
Haga clic en la opción **Establecer SCP** en el clúster de certificación actual.

Confirme su selección y haga clic en **Aceptar** para confirmar.

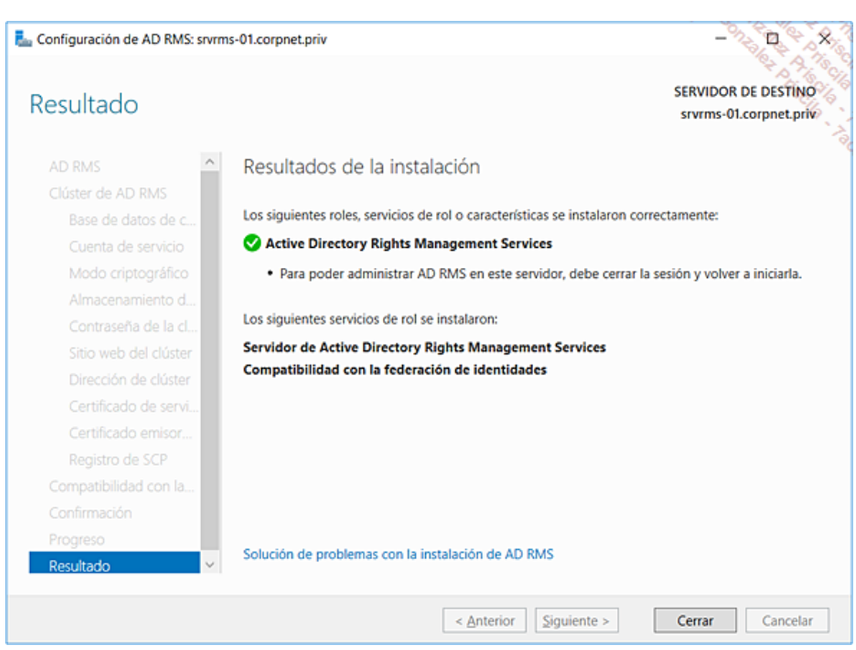


Declaración de la URL de acceso a los servicios de federación AD FS

Esta etapa no es obligatoria. Observe que debe ser introducida si el servicio de rol para el soporte de los servicios de federación se ha seleccionado en el momento de agregar la función AD RMS.



Confirmación de los parámetros de configuración y arranque de la fase de instalación



Fin de la instalación de los servicios AD RMS

En este punto, el rol AD RMS está instalado y configurado.

7. Administración del clúster AD RMS

Una vez que el clúster AD RMS se encuentra operativo, el administrador podrá utilizar la consola MMC AD RMS para realizar las tareas de administración:

Configurar las propiedades del clúster AD RMS: cuenta de servicio, modo de cifrado, URL de la intranet y extranet del clúster, exportación del certificado del clúster, configuración de registros y configuración del SCP (*Service Connection Point*).

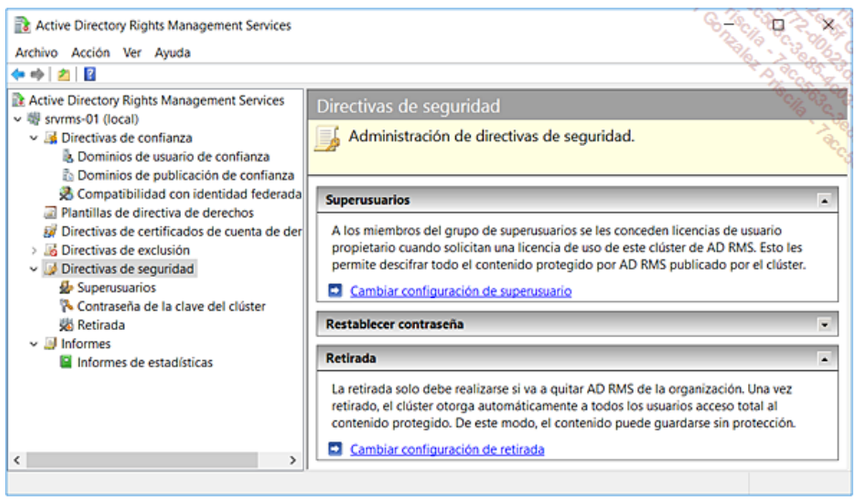
Configuración de las directivas de aprobación: dominios de usuarios autorizados y dominios de publicación aprobados, así como el soporte de identidades federadas.

Configurar los modelos de directivas de permisos.

Configurar las directivas de certificados de cuenta de permisos.

Configurar las directivas de exclusión para los usuarios, las aplicaciones y el referencial seguro

Configurar las directivas de seguridad para los super usuarios, la contraseña de la clave del clúster AD RMS y las opciones de clausura.



Administración del clúster RmsCluster.corpnet.priv

Para más información sobre las diferentes opciones de administración AD RMS, busque "Servicios AD RMS" en el sitio Microsoft Technet en la dirección: https://technet.microsoft.com o siga el enlace siguiente: https://technet.microsoft.com/fr-fr/windowsserver/dd448611.aspx

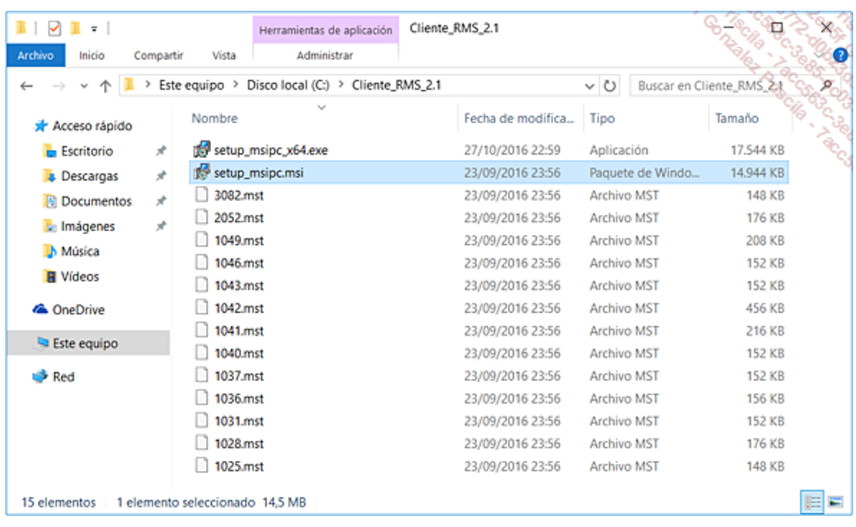
8. Agregar el cliente AD RMS

El cliente AD RMS es un componente esencial de la plataforma AD RMS. La versión 2.1 del cliente se publicó en diciembre de 2015 y permite a los puestos de trabajo Windows proteger y utilizar los documentos digitales soportados por las aplicaciones capaces de utilizar la tecnología AD RMS in-situ y también con Azure RMS. El cliente AD RMS desempeña el papel de framework para soportar la tecnología AD RMS y puede ser distribuido de manera libre con software de terceros diseñados para explotar AD RMS.

El cliente AD RMS está soportado por los sistemas operativos Windows 10, Windows 8.1, Windows 8, Windows 7 SP1, así como para las versiones de Windows Server 2008 R2 hasta 2016.

El cliente AD RMS se encuentra en un archivo ejecutable llamado Setup_msipc_x64.exe que puede ser descomprimido empleando el parámetro /extract para obtener el paquete MSI. En este momento, podemos desplegar el cliente AD RMS en modo por completo silencioso empleando un objeto GPO o un script utilizando - los siguientes comandos:

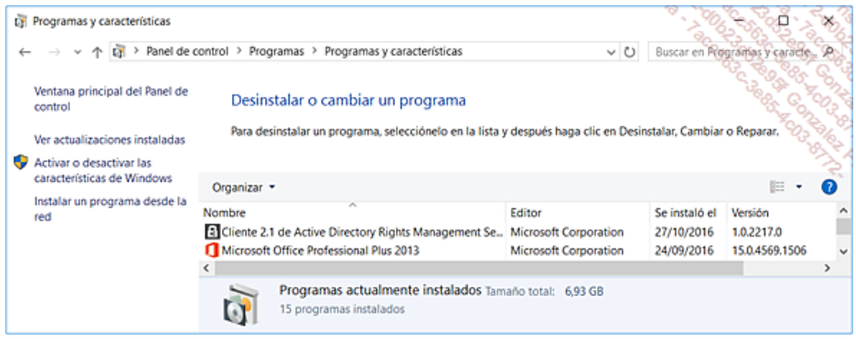
```
setup_msipc_x64.exe /quiet
msiexec /qn c:\downloads\setup_msipc.msi
```



Contenido del paquete del cliente AD RMS 2.1

Descarga del cliente AD RMS 2.1 y actualización del cliente AD RMS 2.0: el paquete que contiene el cliente AD RMS 2.1 está disponible para su descarga en el sitio de Microsoft en la siguiente dirección: https://www.microsoft.com/en-us/download/details.aspx?id=38396. Tenga en cuenta que este paquete soporta también la actualización del antiguo cliente AD RMS 2.0.

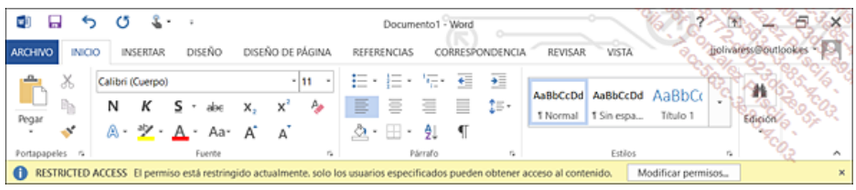
Para más información sobre los detalles del cliente AD RMS, consulte el vínculo "RMS Cliente deployment notes" disponible en la dirección:https://docs.microsoft.com/en-us/rights-management/rms-client/client-deployment-notes



*Cliente AD RMS en **Programas - Programas y características***

9. Validación del correcto funcionamiento de la plataforma RMS

Al término de la instalación, podemos validar el correcto funcionamiento de la plataforma AD RMS empleando un puesto de trabajo Windows 7 profesional o una versión más moderna, tal como Windows 10, en el habremos instalado el cliente AD RMS, así como una aplicación compatible con la tecnología AD RMS como Microsoft Office Profesional 2013 o 2016.



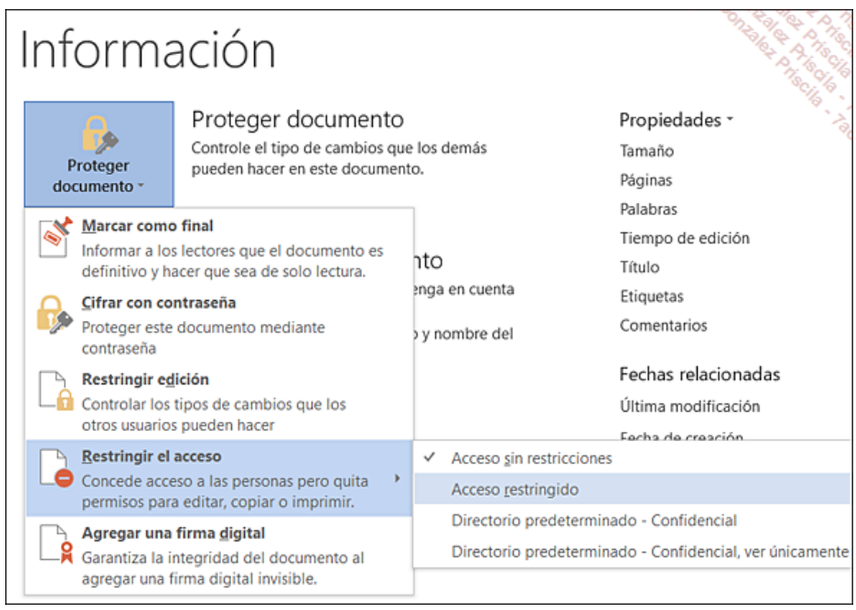
Cinta de Word 2013 y opciones de permisos restringidos empleando AD RMS

Este ejemplo ilustra la aplicación de derechos digitales empleando una aplicación como Microsoft Word 2013. Proceda de la siguiente manera:

Cree o abra un documento.

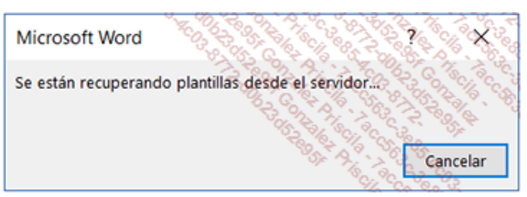
Empleando el menú **Archivo** y luego el botón **Proteger el documento**, seleccione la opción **Restringir el acceso**.

Al término de esta operación, la aplicación AD RMS inicializa de manera transparente la caja fuerte AD RMS del equipo.



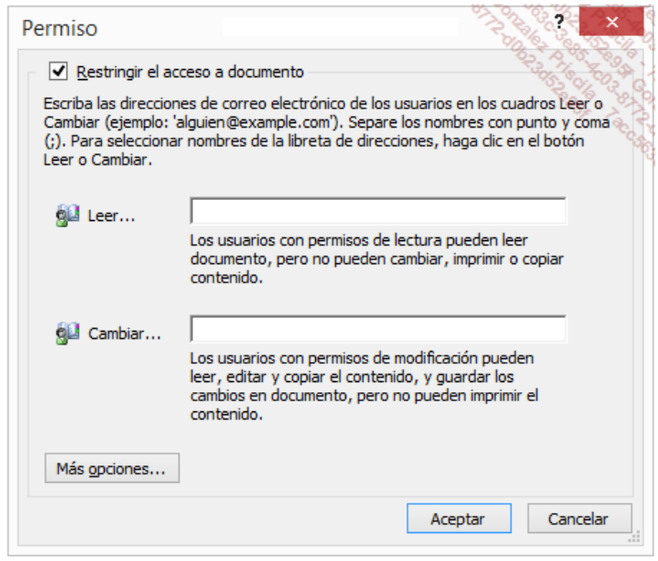
*Menú **Archivo** - **Proteger documento** - **Restringir el acceso***

La selección de acceso restringido invoca la plataforma AD RMS que se inicializa por primera vez.

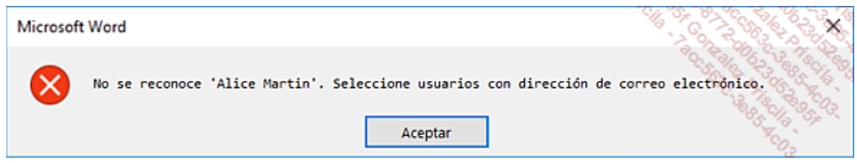


Conexión y recuperación de las plantillas desde el entorno AD RMS

Los accesos restringidos controlados por AD RMS pueden definirse en base a las direcciones de correo de Internet de los usuarios internos existentes en Active Directory o en un bosque aprobado a través de los servicios de federación AD FS por ejemplo, o también a través del conector "Azure Rights Management connector".

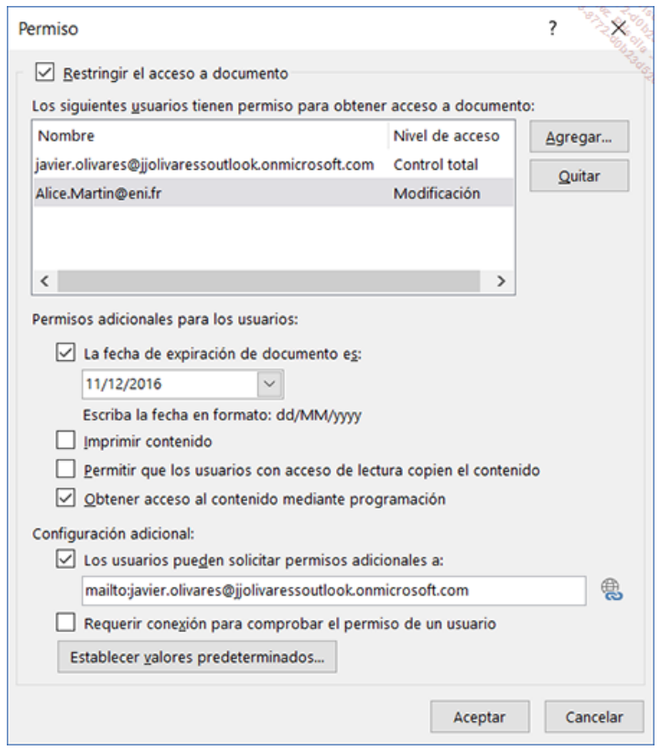


Añadir las direcciones de correo de los usuarios



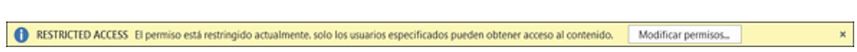
Los usuarios deben disponer de una dirección e-mail en Active Directory

Cuentas de Usuario AD RMS y direcciones de correo electrónico: observe que todos los usuarios y consumidores de documentos protegidos por los servicios de gestión de derechos digitales AD RMS deben disponer de una dirección e-mail en Active Directory, en un bosque aprobado Active Directory o en el cloud público Microsoft Azure.

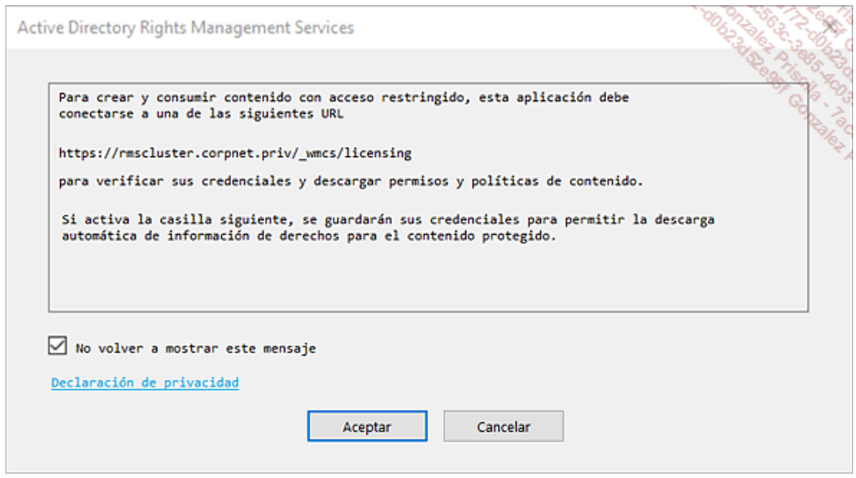


Definición de los permisos de Administración de los derechos digitales AD RMS

Los detalles previos ponen de relieve el hecho de que el documento creado por el usuario jeff.aprea@grouperdi.com (permiso de Control total) está sujeto a autorización y restricciones AD RMS que dan respectivamente a Alice Martin y Bob Durand acceso limitado, para solo modificación y lectura. También observará que el documento está sujeto a una fecha de expiración fijada el 11 de diciembre de 2016 y que la impresión del contenido también está restringida.



Una vez las inscritas las autorizaciones en el documento, el componente de Microsoft Office 2013 se actualiza para significar que la autorización concedida está restringida y que sólo los usuarios que aparecen pueden acceder al documento.

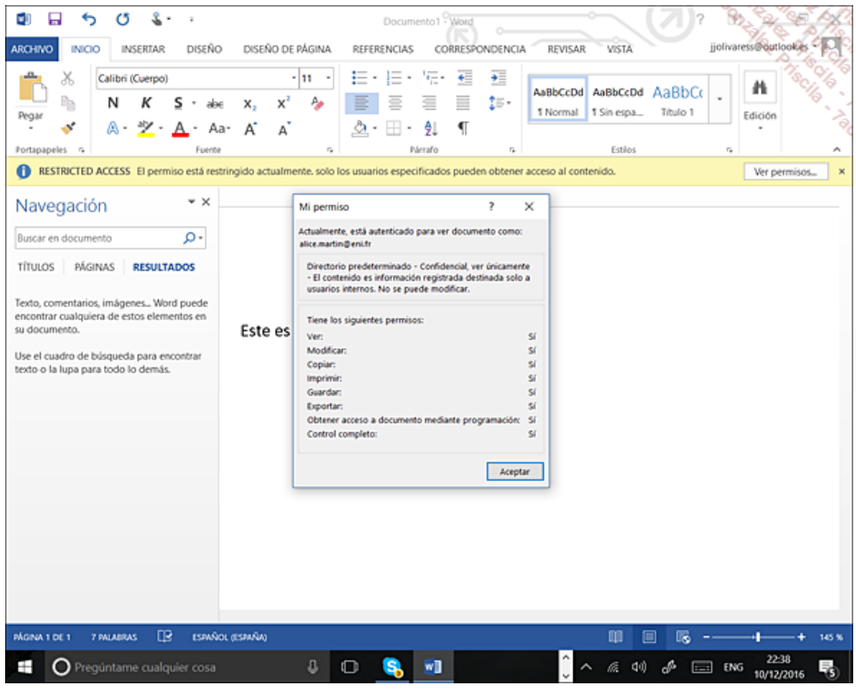


Conexión del puesto de trabajo a la tubería AD RMS

Durante el primer uso del pipeline AD RMS entre el cliente AD RMS y el servidor de licencias AD RMS, aparece una ventana de diálogo informando al usuario que la autorización de acceso al documento está limitada actualmente y que la aplicación, en nuestro ejemplo Microsoft Office, debe conectarse a la URL del clúster de licencia AD RMS para verificar la información de identificación del usuario y, en caso de éxito, descargar la autorización del usuario para dicho documento.

Una vez realizado con éxito el control de acceso, el documento puede ser abierto en función de las autorizaciones concedidas al usuario.

La figura siguiente detalla los permisos de Alice Martin.

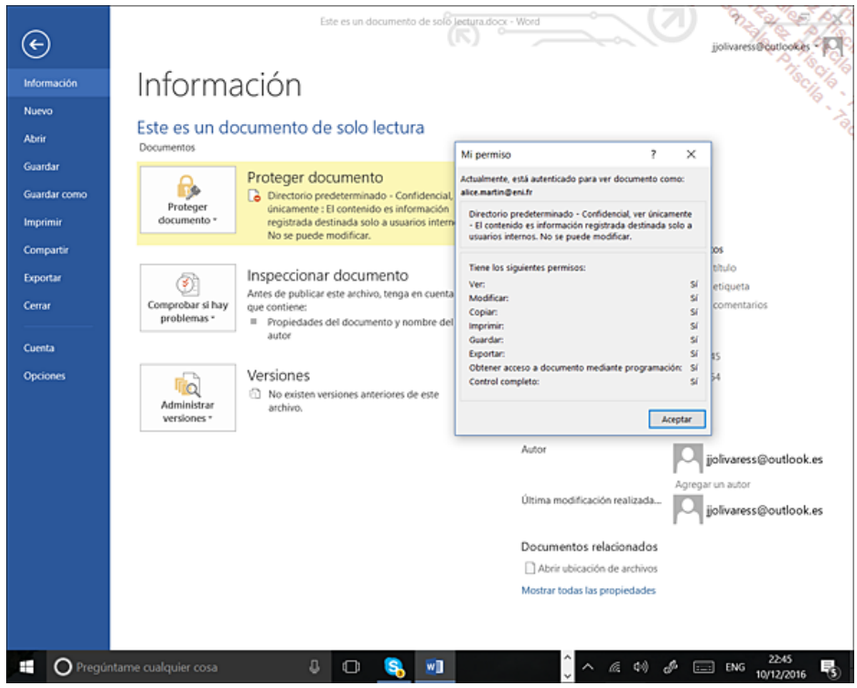


Permisos de Alice Martin - alice.martin@eni.fr

La usuaria dispone solo de derechos de lectura, permisos de visualización, modificar, copiar, imprimir y guardar; acceder a través de un programa y control total están denegados.

También puede señalar la fecha de vencimiento del documento, que significa que a partir de ésta no será posible que Alice efectúe ninguna acción sobre el documento, incluida la apertura y la lectura de éste.

La parte cliente AD RMS integrada en los sistemas operativos cliente Windows 7 profesional y posteriores tales como Windows 8.1 o Windows 10 permiten el cambio de identidad. Esta característica es muy útil para los usuarios que disponen de varias cuentas de usuario en el mismo bosque, en un bosque diferente o cuando se trata de una cuenta Office 365 en Azure.



Permisos de Alice Martin a través del menú Archivo de Word 2013

Las funcionalidades probadas anteriormente permiten validar el buen funcionamiento de la plataforma clúster AD RMS y un cliente genérico que funciona en un puesto cliente Windows 10. Para probar todas las funcionalidades AD RMS, también podemos usar las herramientas del kit de recursos técnicos AD RMS disponibles para descarga en el sitio de Microsoft.

Información de préinstalación para desplegar los servicios AD RMS

La instalación de los servicios AD RMS requiere cumplir con los siguientes puntos técnicos:

- El servidor AD RMS deberá ser miembro de un dominio Active Directory como el que podría contener las cuentas de usuarios que utilicen los documentos controlados por AD RMS.
- Debemos crear una cuenta de dominio que no disponga de ningún privilegio adicional. Esta cuenta se utilizará como cuenta de servicio para los servicios AD RMS.

¡Observe! La cuenta utilizada durante la instalación de los servicios RMS debe ser distinta de la declarada como cuenta de servicio AD RMS.

- Tendremos que registrar un objeto SCP (*Service Connection point*) durante o después de la instalación del servidor AD RMS. Para realizar este paso, debemos ser miembros del Grupo Active Directory Administrador de empresas o disponer de privilegios equivalentes.
- El programa de instalación de los servicios AD RMS permite declarar la base de datos SQL que será utilizada por los servicios AD RMS, incluso si el servidor de bases de datos está en una equipo diferente del servidor AD RMS. Para lograrlo, la cuenta de usuario usada para instalar los servicios AD RMS deberá disponer de los permisos para crear bases de datos en el servidor de bases de datos. En el caso de Microsoft SQL Server, el usuario debe disponer del rol administrador del sistema o equivalente.

AD RMS: recomendaciones de instalación en materia de seguridad

La instalación de los servicios AD RMS de Windows Server 2016 o Windows Server 2012 R2 es soportada por un asistente mucho más evolucionado que el que conocíamos en las versiones anteriores del producto. Gracias a este asistente, se pueden evitar muchas trampas. Las recomendaciones siguientes, nos permitirán lograr una instalación operativa de los servicios AD RMS:

- Debemos configurar la URL que se utiliza para representar el nombre del Clúster RMS. Este nombre debe mantenerse a lo largo de la utilización de la plataforma AD RMS. En general, un nombre diferente del nombre real del equipo será declarado en la configuración del clúster AD RMS y declarado con un registro de tipo A en el DNS.
- El servidor de base de datos debe ser instalado en un equipo diferente del servidor que presta servicios AD RMS, aunque no se trata de un requisito.
- Las comunicaciones entre un cliente AD RMS y el clúster utilizan por defecto el protocolo HTTP. Se recomienda instalar un certificado SSL para encriptar y autenticar los flujos entre las entidades.

Podemos utilizar un certificado autofirmado o emitido por una autoridad de certificación aprobada. Observe que un certificado autofirmado no debe ser empleado salvo para fines de pruebas, esta configuración no es soportada por Microsoft. En el momento de añadir un nuevo servidor a un clúster AD RMS, el certificado SSL debería estar implementado en el nuevo servidor antes de iniciar el proceso de instalación de los servicios AD RMS.

Cifrado fuerte para los servicios AD RMS: el cifrado fuerte para los servicios AD RMS es una nueva funcionalidad aparecida con Windows Server 2012 R2 y Windows Server 2016. Nos permitirá aumentar el nivel de cifrado de la plataforma AD RMS. La ejecución de los servicios AD RMS con el método de cifrado fuerte, llamado Modo 2 en la plataforma AD RMS se basa en el cifrado RSA y la utilización de claves más fuertes que pasan de 1.024 bits a 2.048 bits. Además, las claves de cifrado utilizadas para el hash pasan de 160 bits a 256 bits y utilizan el algoritmo SHA-256, en lugar de SHA-1 en vías de quedar obsoleto. Estas mejoras criptográficas siguen las mejores prácticas en materia de seguridad definidas por el NIST (*National Institute of Standards and Technology*).

En relación con el NIST: desde enero de 2011, el NIST publicó el artículo 800-57 que recomienda la utilización de claves RSA de 2.048 bits. En los Estados Unidos, las agencias federales deben cumplir las recomendaciones del NIST. La mayoría de las empresas privadas aplican a su vez estas recomendaciones.

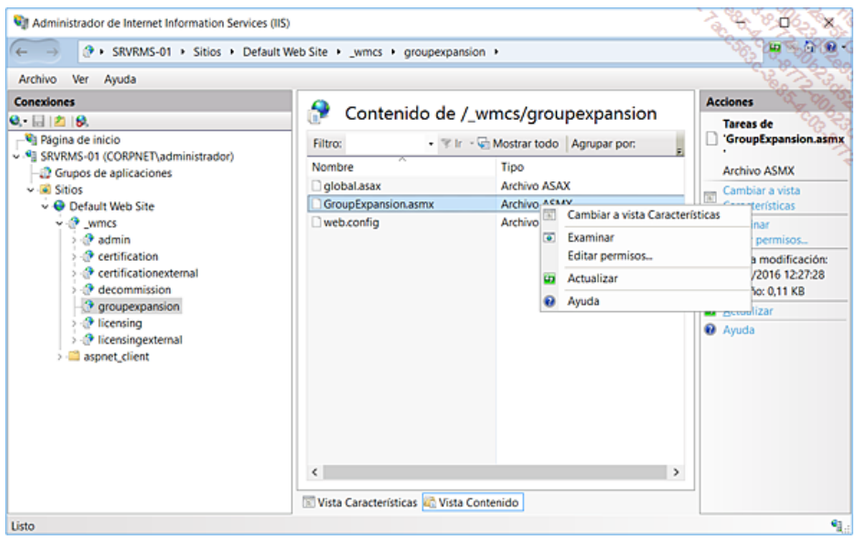
- Para disfrutar de una independencia de cara al futuro o de la aplicación de procedimientos de recuperación de emergencia, cree un registro DNS de tipo A o de tipo alias (CNAME) para referenciar la URL del clúster AD RMS y otro registro del mismo tipo para referenciar el nombre del servidor que alberga la base de datos de configuración AD RMS. En caso de cambiós en la plataforma (adición o eliminación de servidores dentro del clúster AD RMS), basta con actualizar los registros de alias DNS.

¡Observe! No podemos usar una URL empleando "localhost" durante la instalación de los servicios AD RMS. Es por completo necesario usar una URL basada en un nombre DNS cuya resolución DNS puede efectuarse con éxito.

Despliegue de servicios AD RMS en entornos de bosques múltiples

Un único clúster AD RMS puede estar inscrito dentro de un bosque de Active Directory. Cuando una empresa desea utilizar documentos protegidos en un entorno integrado por más de un bosque, será necesario desplegar un clúster AD RMS para cada bosque. A continuación se describen las recomendaciones relativas a este tipo de escenario:

- Todas las URL de los diferentes clústeres AD RMS deberán implementar SSL para encriptar todos los intercambios.
- Todos los bosques que no utilicen Exchange Server deben ser objeto de una extensión del esquema Active Directory.
- La cuenta de servicio AD RMS debe tener el permiso para acceder al conjunto de extensiones de los grupos.



Permisos a configurar en el archivo GroupExpansion.smx

- La cuenta de servicio AD RMS debe tener el permiso para acceder al conjunto de extensiones de los grupos. Esta operación se realiza configurando los permisos de acceso del archivo GroupExpansion.asmx ubicado en la carpeta C:\inetpub\wwwroot_wmcs\groupexpansion. Por ejemplo, si debemos soportar varios bosques necesitaremos declarar las cuentas de servicio AD RMS de los diferentes bosques en todos los servidores de los diferentes clústeres AD RMS.

Soporte de servicios de federación AD FS con AD RMS

Para garantizar un buen funcionamiento de los servicios de federación AD FS en un entorno AD RMS, necesitaremos considerar los siguientes temas:

- Una relación de confianza de la Federación debe configurarse antes de que podamos no configurar el soporte de Federación de identidades. Durante la instalación de esta funcionalidad, necesitaremos especificar la URL que permita el acceso a los servicios de federación.
- AD FS requiere comunicaciones seguras entre servidores AD RMS y los servidores AD FS.
- La cuenta de servicio AD RMS deberá disponer del permiso Generar auditorías de seguridad.
- Los URL extranet de clústeres AD RMS deben estar accesibles a las cuentas de la empresa aprobada a través de los servicios AD FS.

Para obtener más información sobre los escenarios AD RMS y AD FS busque "Deploying Active Directory Rights Management Services with Active Directory Federation Services" en el sitio Microsoft Technet en la dirección https://technet.microsoft.com o utilice el siguiente enlace:https://technet.microsoft.com/en-us/library/dn758110.aspx. Los procedimientos descritos nos permitirán configurar una relación de federación entre ambas organizaciones a través de Internet. En este escenario, una de las empresas dispone de una plataforma AD RMS mientras que la otra no. Sin embargo, podremos, mediante la relación de la Federación AD FS, consumir contenidos digitales protegidos por la otra empresa.

Para obtener más información sobre los escenarios AD RMS y Azure RMS, consulte el vínculo "Deploying the Azure Rights Management connector" en la dirección: https://docs.microsoft.com/es-es/rights-management/deploy-use/deploy-rms-connector

10. Referencias para AD RMS con Windows Server 2016

Los servicios de Active Directory Rights Management Services son objeto de todo el esfuerzo por parte de los equipos de Microsoft. En efecto, los equipos informáticos, responsables de la protección de la información digital deberán tener una buena visión de la noción de protección digital, las tecnologías implicadas y las mejores prácticas relacionadas con la tecnología AD RMS y con el estándar XrML (*eXtensible rights Markup Language*).

Para más información sobre los servicios AD RMS, podemos utilizar los enlaces a continuación:

- Rights Management Documentation: https://docs.microsoft.com/es-es/rights-management/
- Active Directory Rights Management Services Overview: https://technet.microsoft.com/en-us/library/hh831364.aspx
- Descarga del cliente RMS 2.1: https://www.microsoft.com/en-us/download/details.aspx?id=38396
- RMS Client deployment notes: https://docs.microsoft.com/en-us/rights-management/rms-client/client-deployment-notes
- Deploying a AD FS Federation Server Farm: https://technet.microsoft.com/en-us/library/dn486775.aspx

Gestión de identidades y entornos híbridos

1. Azure: CAPEX vs OPEX

Hace ya varios años que los proveedores de soluciones ofrecen a las empresas la modernización de sus infraestructuras a través de servicios ofrecidos en la nube. Para solo citar a los tres grandes actores: se trata de Microsoft, Google o Amazon. Podemos constatar que con cada vez mas frecuencia algunas empresas consideran como una solución viable desplazar ciertos costes a una nube cercana, operada por un partner local, o porque no, una nube pública como por ejemplo Microsoft Azure.

La idea es beneficiarse al máximo de la nube para aprovechar los nuevos servicios, nuevos escenarios de uso, que serían más difíciles de establecer de manera tradicional *on-premise*, invirtiendo de forma "diferente".

En cuanto a las infraestructuras IT y despegue de las soluciones cloud, la cultura estadounidense hace cada vez más a menudo referencia a la oposición de los modelos CAPEX (gastos relacionados con inversiones) y OPEX (gastos de funcionamiento). Esta problemática, o esta nueva reflexión, está cada vez más presente en las discusiones, en particular con el éxito creciente de las soluciones SaaS (*Software as a Service*) como ofice 365. La cuestión de fondo es, pues "¿es mejor elegir el modelo CAPEX invirtiendo en una infraestructura de virtualización completa o, en cambio, elegir el modelo OPEX que permite pagar solo por el uso de los servicios consumidos en un momento concreto dentro de un Cloud público?"

En general, cuando comparamos el coste de adquisición con respecto al de una ubicación durante un periodo de tiempo bastante largo, entonces constatamos que la ubicación del servicio es más cara. Sin embargo, no debemos concluir con rapidez que este primer enfoque puede ser falso. En efecto, debemos tener en cuenta todos los costes indirectos como la electricidad, refrigeración, administración, implementación de alta disponibilidad, sin olvidar todos los contratos de mantenimiento asociados. De esta forma, cuanto todo está «sumado en real», es posible que sea más económico alquilar el servicio sobretodo porque este no se utiliza a plena capacidad o puede evolucionar de forma importante en el tiempo.

Los analistas hacen notar también que el hecho de que la actividad económica se encuentra en un estado poco ideal hoy en día pudiendo favorecer las soluciones basadas en el alquiler, modelo OPEX, más que en la adquisición, siendo el acceso a la financiación difícil o más comprometido.

Por último, ampliando el campo de reflexión entre los modelos de arquitecturas IT on-premise o híbridos, y los modos de financiación entre CAPEX y OPEX, se incluye el éxito creciente de las soluciones de colaboración propuestas, tanto por Microsoft como Google, por ejemplo.

La continuación de este capítulo presenta la visión propuesta por Microsoft con su plataforma Azure y en especial cómo Azure Active Directory puede ayudar a facilitar la gestión de identidades y la gestión de accesos on-premise y dentro de la plataforma Azure, para utilizar las aplicaciones SaaS Microsoft y también no Microsoft.

2. Evolución del modelo, utilización y gestión de identidades

Cada vez más las empresas ponen el acento en la movilidad que se convierte en una fuente de proyectos recurrente entre ellos. La idea de esta evolución del uso se repercute al mismo tiempo en las aplicaciones y servicios ofrecidos en la nube para minimizar los costes, al menos las inversiones a corto plazo.

De esta forma, encontramos en el centro de todas las problemáticas, los usuarios, sus necesidades en términos de movilidad y de acceso a sus datos y la utilización de dispositivos móviles como ordenadores portátiles al igual que las tablets y otros teléfonos, iOS, Android y en menor medida hoy en día, Windows Phone. La idea principal es ofrecer servicios abiertos, extensibles, modulares que permitan a los empleados acceder a sus datos y aplicaciones sin importar la ubicación, en todo momento y, por supuesto con total seguridad.

Con Azure AD, Microsoft se posiciona e introduce su visión de los servicios IT a través de los servicios de Active Directory y los componentes que participan en el centro de una nueva estrategia que hay que evaluar, medir, comprender y quizás, pensar en su plan director.

Al final, si las soluciones propuestas y evaluadas están previstas, o por el contrario excluidas, entonces se debe dejar de considerar el impacto de estas opciones sobre las limitaciones impuestas a múltiples niveles, bien se trate de aplicaciones e impactos, e incluso consecuencias, en relación a las tareas de administración que pueden ser más complejas.

a. Gestión de identidades

El aprovisionamiento y la gestión recurrente de los usuarios con una tarea simple y compleja a la vez. Simple, ya que basta con unos segundos para crear un nuevo usuario en Active Directory, pero compleja cuando se considera con la perspectiva necesaria en el sentido de "gestión de identidades" en una empresa que mantiene muchos sistemas Windows, no Windows, y aplicaciones de todo tipo.

Por supuesto, muchas empresas ya disponen de un modelo organizado que permite con "facilidad" gestionar de manera uniforme las identidades y también la administración de permisos de acceso a los recursos. Sin embargo, cuando esto no es el caso, la productividad puede verse reducida a sabiendas de que esto ocurra a menudo cuando es necesario configurar muchas identidades, en concreto en entornos complejos formados por varias empresas filiales, es decir, bosques de Active Directory.

Para evitar estos excesos, es responsabilidad de los equipos IT de asegurarse de que todo está hecho según las normas. Así, cada vez que un empleado necesita utilizar una nueva aplicación o bien acceder a determinados datos, entonces el equipo IT debe hacerse cargo de la demanda de manera específica.

Los beneficios de una verdadera estrategia de gestión de identidades son numerosos y listados a continuación:

- La estandarización de los procedimientos y herramientas permite reducir el tiempo necesario para la integración de nuevos usuarios.
- Una solución híbrida capaz de gestionar las identidades on-premise y en la nube puede ser determinante para acompañar la puesta a disposición de nuevas aplicaciones en modo SaaS, tal como por ejemplo Office 365.
- Podremos reducir el acceso a los recursos necesarios para las actividades de las diferentes poblaciones de usuarios.
- La utilización de instrumentos centralizados y unificados permitirá limitar la carga de administración asociada a la gestión de identidades.
- Una gestión centralizada y simplificada de las identidades mejorará la seguridad en su conjunto minimizando el uso de cuentas de usuario obsoletas.
- El acceso a las aplicaciones on-premise y en la nube podrán ser gestionados de manera homogénea.
- Los principios de delegación y auditoría de conexiones y acceso a los recursos también serán gestionados de manera uniforme en cualquier lugar que estén situadas las identidades y los recursos.

b. Azure AD, centrado en las identidades e indispensable para colaborar

En el momento en que es cada vez más solicitado intercambiar información con sus colaboradores y asociados, una infraestructura híbrida dotada de servicios de gestión de identidades y acceso a recursos parece ser cada vez más necesaria.

Cuando la empresa está en desarrollo y cuando es necesario abrirse al exterior, el hecho de estar en punto muerto en los servicios centrales podría reducir la capacidad de los empleados para comunicarse y por lo tanto ganar en creatividad y productividad. La idea es en realidad lograr que los servicios de identidad estén al servicio de las aplicaciones y de la infraestructura en su conjunto.

De esta manera, será posible:

- mejorar los intercambios entre los usuarios, los departamentos y los socios,
- elevar el nivel de servicios ofrecidos a sus usuarios a través de una respuesta correcta en relación a sus demandas.
- por último minimizar los costes de operación utilizando las tecnologías más modernas en un modelo basado en el uso.

Para más información y detalles sobre Azure AD y los servicios de colaboración, busque "Collaboration B2B Azure Active Directory" en el sitio Microsoft Azure: https://azure.microsoft.com

3. Movilidad de los usuarios y dispositivos con EMS y Azure AD

La movilidad es también un tema candente en el centro de todos los debates. En efecto, hoy en día, los usuarios demandan cada vez más -e incluso son exigentes en relación con el acceso a servicios, aplicaciones y datos a partir de dispositivos móviles que utilizan, ya se trate de dispositivos móviles personales o distribuidos dentro de la empresa.

Con una estrategia capaz de desarrollar la movilidad de los usuarios y dispositivos, la empresa podrá aprovechar los siguientes avances:

- reducción de las inversiones en hardware,
- mejora de la satisfacción de los empleados,
- reducción de los gastos de desplazamiento,
- reducción de costes de instalación,
- mejora de la gestión del tiempo,
- mejora de la agilidad en su conjunto.

Para dar una respuesta a esta problemática, Microsoft ofrece la suite EMS (*Enterprise Mobility Suite*). Empleando EMS, y Azure AD en su versión Premium, la empresa podrá aprobar iniciativas de tipo BYOD (*Bring Your Own Device*) que pueden considerarse de forma serena mediante una gestión segura. En primer lugar, la solución permite garantizar la protección de los datos y la conformidad de los dispositivos móviles de la empresa o personales. Luego, cuando una suite de aplicaciones como Office 365 se utiliza, los dispositivos aprobados serán validados y pasan a ser utilizables como verdaderos puestos de trabajo dentro de la empresa.

La información a continuación ilustra el contenido de la suite Microsoft EMS:

a. Servicios ofrecidos a través de Azure Active Directory Premium (AAD)

- Reinicio como auto servicio de contraseñas para minimizar las llamadas a los equipos de soporte.
- Autenticación multifactor para aumentar el nivel de seguridad relacionado con el uso de contraseñas simples.
- Utilización de la autenticación SSO y grupos para controlar el acceso a las aplicaciones SaaS.
- Informes de seguridad para detectar posibles amenazas.
- Sincronización de directorios on-premise y en la nube.

b. Servicios ofrecidos a través de Microsoft Intune

- Gestión de aplicaciones para dispositivos móviles.
- Soporte de dispositivos móviles iOS, Android, Windows y Windows Phone.
- Borrado selectivo de los dispositivos para protección y seguridad mejorada de datos.
- Integración con System Center Configuration Manager y Endpoint Protection.

c. Servicios ofrecidos a través de Azure Rights Management (RMS)

- Protección de datos digitales en el Cloud Azure y también on-premise para una protección total de los documentos en los entornos híbridos.
- Inclusión de los derechos de uso -CAL Cliente RMS, requeridos para el servidor Windows Server con los servicios AD RMS.
- Kit de Desarrollo de software disponible para integrar aplicaciones existentes.

d. Servicios ofrecidos a través de Microsoft Advanced Threat Analytics (ATA)

- Sistema de análisis de comportamiento para la detección temprana de las amenazas.
- Detección de ataques y problemas de seguridad.
- Información, alertas y recomendaciones relativas a actividades sospechosas.
- Integración de los sistemas de análisis existentes.

Para más información sobre la implementación de los entornos móviles dentro del Cloud Azure via EMS, diríjase al sitio de Microsoft Enterprise Mobility Suite a través del vínculo siguiente: https://www.microsoft.com/es-es/server-cloud/enterprise-mobility/overview.aspx

A título indicativo, el coste de utilización por mes y usuario de la suite EMS en Azure, incluyendo Azure AD Premium, Microsoft Intune, Azure Rights Management y Microsoft Advanced Threat Analytics es de 7,8 € - en comparación con la tarificación separada de cada servicio que corresponde a un total de 15,6 euros.

4. Directiva de administración global de las identidades

La gestión de identidades define los principios según los que los usuarios tendrán la capacidad de utilizar los recursos puestos a su disposición. Ya se trate de equipos, dispositivos móviles, aplicaciones y otros servicios que se puedan ofrecer, se tratará de definir, administrar y controlar los accesos a todos esos recursos.

Definir una directiva de administración global de las identidades debe especificar las modalidades de ejecución de estas operaciones de gestión y administración y su seguimiento en el tiempo para, al final, gestionar el ciclo de vida de las identidades. Estas operaciones pueden ser utilizadas en Azure AD a través del portal Azure como base de la gestión de identidades.

Con Azure, Azure AD, y los servicios de dominio AD DS on-premise, la empresa dispondrá de toda la seguridad y toda la flexibilidad necesaria para hacerse cargo de sus necesidades tanto en la Nube como dentro de su entorno local.

Para más información sobre Azure Active Directory, diríjase al sitio de Microsoft en la siguiente dirección: https://www.microsoft.com/es-es/server-cloud/products/azure-active-directory/default.aspx

5. La hibridación con Azure es fuente de nuevas soluciones para la empresa

La hibridación es el corazón de los nuevos modelos de infraestructura IT. En efecto, la idea no es "**pasar de una infraestructura existente a la Nube**" sino enriquecer la misma con los "**servicios disponibles bajo demanda**" mediante la Nube.

Con los servicios ofrecidos por el cloud Microsoft Azure y un enfoque de este tipo, los servicios IT de la empresa se posicionan más como proveedores de servicios operativos que proveedores de tecnología que deberán de partida garantizar todos los costes de adquisición, así como las etapas de aplicación, de despliegue y mantenimiento en condiciones operativas. En efecto, Azure AD hace posible la creación de soluciones híbridas para administrar las identidades y controlar los accesos a los recursos on-premise y en el cloud. Hasta ahora, los recursos de la empresa se controlaban por medio de los servicios de dominio Active Directory on-premise permitiendo otorgar acceso externo a los usuarios para el ejercicio de su actividad.

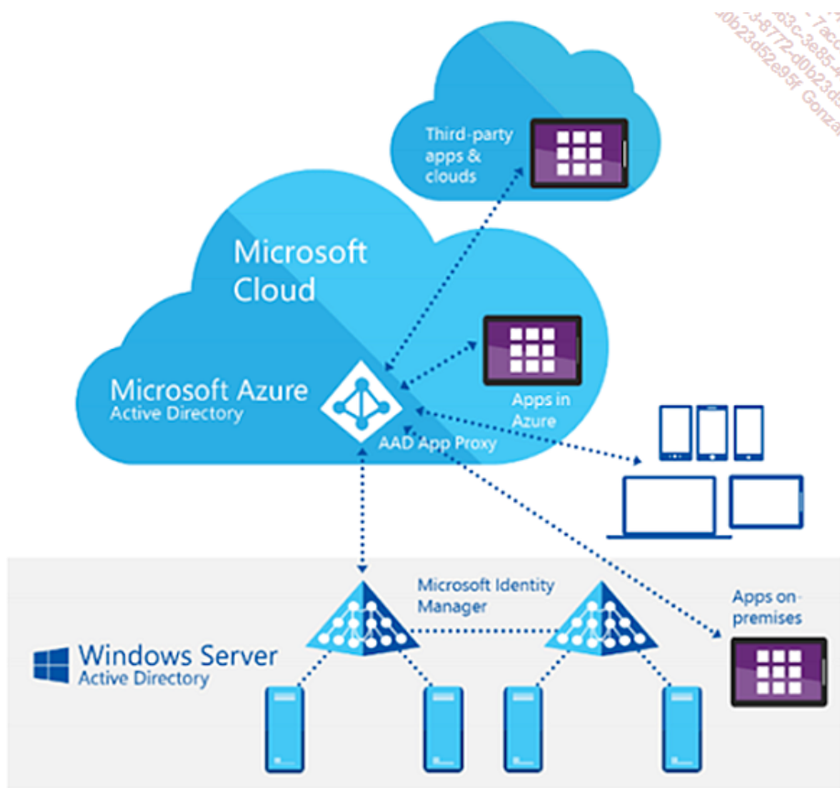
Toda la potencia de Azure AD consiste en ampliar el entorno Active Directory on-premise al cloud Azure para permitir a la empresa disfrutar de nuevos escenarios y nuevas soluciones fáciles de desplegar porque se encuentran "listos para su uso" dentro de la plataforma Azure.

De esta forma, el cloud Azure combina la capacidad de sobra conocida y bien controlada de Active Directory en Windows Server 2012 R2 y Windows Server 2016 con las de Microsoft Identity Manager 2016 (MIM) y Azure AD para la gestión de identidades. Este conjunto de bloques ofrece un sistema completo de gestión de identidades para entornos híbridos con los servicios de infraestructura de directorios AD, los servicios de federación AD FS y, a través de EMS (*Enterprise Mobility suite*), los servicios de registro y gestión de dispositivos móviles (Intune) y de gestión de derechos digitales (Azure RMS, *Azure Rights Management Services*).

6. En el centro del cloud Azure, Azure Active Directory

Esta introducción nos permite ver hasta qué punto Azure AD es el centro del cloud de Microsoft. Como sistema de gestión de identidades para Office 365, Intune y todos los cientos de aplicaciones SaaS disponibles en la plataforma Azure, Azure AD es hoy la plataforma de gestión de identidades empresarial más importante, por delante de Google o Amazon.

Más allá del hecho de que los servicios de directorio, la autenticación fuerte con factores múltiples, los portales de autoservicio y los mecanismos de Federación y de sincronización de directorios son una de las plataformas más ricas del mercado, el punto más importante es sin duda el hecho de que se trata de una plataforma abierta basada en estándares de industria, tales como la interfaz de desarrollo Graph API y las interfaces SAML, OAuth 2.0, OpenID Connect y Odata 3.0.



Vista del entorno Azure Active Directory

Con respecto a Graph API: la interfaz de desarrollo AAD Graph API es un servicio de tipo OData 3.0 que permite acceder a las funciones de lectura, modificación y creación de objetos tales como usuarios, grupos y contactos dentro de un inquilino Azure. La interfaz AAD Graph API expone los puntos de acceso REST que nos permiten comunicar a través de mensajes empleando los protocolos HTTP y/o HTTPS.

Acceso a Outlook, OneDrive, OneNote: Tenga en cuenta que las funcionalidades AAD presentadas a través de la interfaz Graph API son muy interesantes para los desarrolladores ya que están también disponibles para las aplicaciones de Microsoft como Outlook, OneDrive, o OneNote a través de un único punto de acceso REST y un solo token de acceso.

Con respecto a Graph API: para más información sobre la interfaz Graph API, busque "Active Directory Graph API REST" en el sitio MSDNhttps://msdn.microsoft.com o siga el vínculo https://msdn.microsoft.com/es-es/library/azure/hh974476.aspx.

En cuanto a la interfaz OData: para más información sobre los métodos OData (*Open Data Protocol*), basadas en el estándar OASIS, consulte el sitio http://www.odata.org/.

Azure Active Directory:¿para qué hacerlo?

Azure AD es rico en funcionalidades. Esta introducción presenta las características más notables, así como los beneficios que pueden aportar a las empresas que deseen orientarse hacia un modelo híbrido.

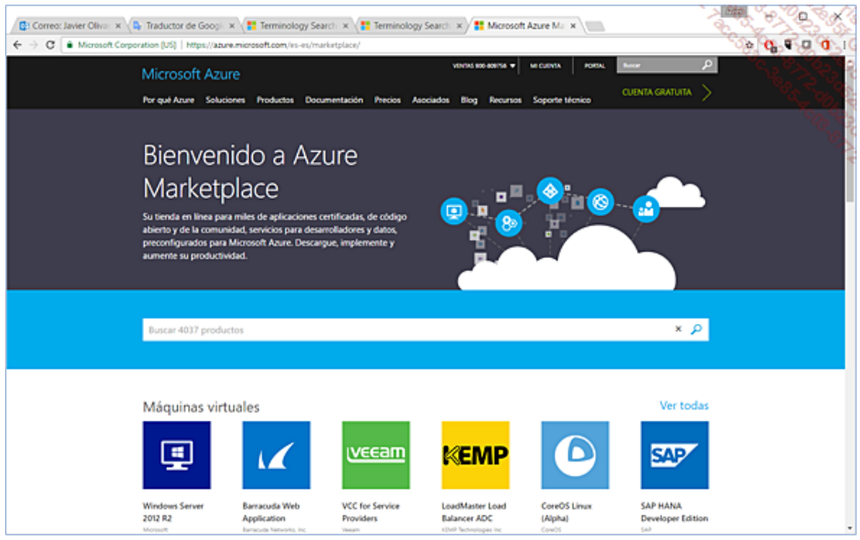
1. Gestión de identidades, hibridación, SSO y aplicaciones SaaS

Active Directory es ya la tecnología de servicios de directorio más utilizada a nivel empresarial, y esto desde hace muchos años. Con frecuencia utilizada como sistema de autenticación y control de acceso para el acceso a los recursos de Windows, también lo es como fuente de identidades para diversas soluciones y añadidos mediante un buen soporte de los protocolos LDAP y Kerberos, Azure Active Directory extiende las posibilidades básicas con muchas capacidades adicionales.

De la misma forma que los servicios de dominio Active Directory ofrecen sus servicios de gestión de identidades para el entorno on-premise de la empresa, Azure AD ofrece sus servicios para controlar el acceso a las aplicaciones y datos situadas en el cloud ya se trate de aplicaciones de Microsoft o de aplicaciones no-Microsoft pero publicadas a través de la plataforma Microsoft Azure. Azure AD permite beneficiarse de una experiencia de autenticación SSO para las aplicaciones SaaS más conocidas.

Hoy en día, podemos integrar más de 2.000 aplicaciones, de forma independiente de su ubicación, mediante los servicios de Federación existentes dentro del cloud Microsoft Azure.

Todos los parámetros de configuración están listos para su uso al estar preparados dentro de la galería de aplicaciones Azure.



Galería de aplicaciones Azure - Azure Marketplace

Para examinar la galería, siga el enlace: https://azure.microsoft.com/es-es/marketplace/

Entre las aplicaciones más conocidas encontraremos por supuesto la suite Office en su evolución Office 365, los servicios de infraestructura como Azure AD Connect, Azure RemoteApp Intune, y también muchas aplicaciones como las ofrecidas por SAP, Salesforce, Google y otros muchos proveedores de aplicaciones accesibles en modo SaaS a través de Azure.

Todo el interés de Azure en comparación con una extensión del entorno IT on-premise ya basado en servicios de dominio de Active Directory AD DS reside en la capacidad de inicio de sesión único de tipo SSO para ofrecer a los usuarios una experiencia transparente basada en la utilización de sus identificadores habituales (UPN, *Principal User Name* y Password Active Directory). Luego, los permisos se basan como de costumbre en la pertenencia a los grupos de Active Directory que son sincronizados de forma automática en Azure AD para controlar el acceso a los recursos.

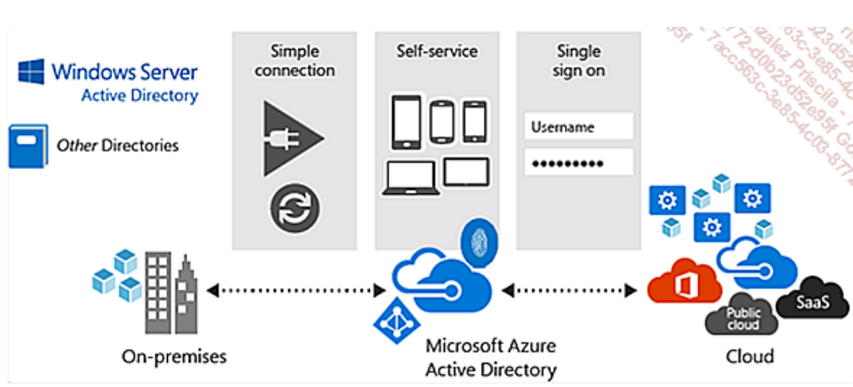
Pero más allá del control de acceso a las aplicaciones SaaS alojadas en Azure, el más importante es que podemos utilizar los servicios Azure AD para controlar el acceso a las aplicaciones que están ubicadas on-premises. Esta funcionalidad se soporta mediante el componente Azure AD Aplicación Proxy que garantiza la publicación de aplicaciones internas de tipo web tales como la mensajería Outlook en modo OWA, los sitios de tipo SharePoint o también todo tipo de aplicaciones web basadas en IIS.

Para más detalles sobre la operación de la funcionalidad Azure AD Aplicación Proxy, busque "Single sign-on with Aplicación Proxy" en el sitio Microsoft Azure Documentation Center en la dirección https://azure.microsoft.com/en-us/documentation/ o siga el enlace:https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-proxy-sso-using-kcd/

2. Optimizado para la suite Office 365 en entorno híbrido

Las soluciones de aplicación ofrecidas por Microsoft mediante el cloud público Azure son por naturaleza destinadas a grandes volúmenes de usuarios. Sin embargo, muchas empresas que deseen desplegar un entorno híbrido obtendrán mayores beneficios.

Por ejemplo, la funcionalidad de gestión de grupos a partir del portal de autoservicio ofrecida a través de Azure AD Premium permite delegar fácilmente los derechos de acceso a Office 365. Una vez éste se añade a un grupo Azure AD autorizará al mismo para utilizar Office 365 a través de la obtención de una licencia. Fíjese también que el administrador podrá administrar grupos tanto en el cloud como dentro del entorno Active Directory on-premise. Luego, Azure AD garantizará la sincronización de los grupos, así como el seguimiento necesario para estas operaciones de administración críticas en materia de seguridad de acceso a los documentos.



Para más información sobre la integración de Microsoft Office 365 con entornos on-premise siga el enlace: https://support.office.com/en-us/article/Office-365-integration-with-on-premises-environments-263faf8d-aa21-428b-aed3-2021837a4b65?ui=en-US&rs=en-US&ad=US

3. Para los desarrolladores, las API Azure AD fáciles de usar

Azure AD fue concebido con el espíritu del cloud para servir de referencia de identidades para el ecosistema Microsoft pero no de forma exclusiva. Para desempeñar ese papel de federador y de plataforma abierta, Azure AD se construye como una plataforma que soporta todas las API estándar del mercado. De esta forma, los desarrolladores de las plataformas Windows, Linux y Unix pueden operar con los distintos componentes y funciones de administración de Azure AD.

Las interfaces de tipo REST (*REpresentational State Transfer*), ofrecen a los desarrolladores todos los mecanismos para integrar las funciones de gestión de identidad empleando la librería ADAL (*Azure AD Authentication Library*) para .NET. Con este componente central, los desarrolladores pueden invocar los protocolos de identidad más modernos como OpenID y OAuth. Sobre esta base, podrán entonces construir o conectar aplicaciones móviles y aplicaciones web seguras. Todas estas librerías cliente están disponibles en open source para entornos iOS, Android, .NET y Windows Store.

En resumen, Azure AD ofrece a los desarrolladores un gran número de interfaces que permiten el soporte de todos los entornos actuales y futuros:

- La API Graph: según el formato del protocolo LDAP, esta API permite a las aplicaciones demandar al entorno Azure AD y recibir una vista de los objetos del directorio y las relaciones que pueden existir entre los objetos. Esta interfaz soporta Office 365, SharePoint, Exchange, así como las aplicaciones no Microsoft.
- La librería .NET ADAL: esta librería permite a las aplicaciones cliente autenticarse en Active Directory on-premises o en Azure AD y disfrutar de funcionalidades de seguridad muy poderosas sin requerir grandes conocimientos en materia de protocolos de seguridad.
- La API Azure Service Management API (SMAPI): esta interfaz de programación permite a los desarrolladores basarse en un conjunto de API para acceder a todas las funciones de administración de Azure Active Directory. En base a esta API, los administradores pueden a su vez utilizar el módulo Windows PowerShell Azure Active Directory para realizar todas las operaciones de administración relativas a la gestión de los usuarios, grupos, dominio y las opciones de SSO.
- El SDK MFA (*Multi-Factor Authentication*): este kit de desarrollo permite a los desarrolladores integrar el soporte de autenticaciones de factores múltiples en las aplicaciones móviles para confirmar una autenticación a través de una llamada telefónica o enviar un SMS.
- Integración simplificada de las aplicaciones existentes: las empresas que ya utilizan aplicaciones de tipo SaaS a partir de un entorno cloud no integrado dentro de Azure AD pueden a menudo añadir sus aplicaciones, y activar la autenticación SSO, después de algunos pasos de configuración. Bajo el mismo espíritu, las aplicaciones web integradas en el entorno on-premises podrán publicarse de forma segura en Internet usando el proxy de aplicaciones Azure AD, en inglés *Azure AD Aplication proxy*.

Versiones de Azure AD: gratuita, básica y Premium

Microsoft ofrece tres variantes de su oferta Azure AD a través de las versiones gratuita, básica y Premium. El cuadro siguiente resume las diferentes posibilidades de Azure Active Directory en función de las versiones. Observe que la oferta Azure AD Premium es la oferta más rica, puesto que incluye los servicios de gestión de identidades para entornos on-premises, híbridos y cloud.

Funcionalidades	Azure AD versión gratuita	Azure AD versión básica	Azure AD Premium
Service Azure Active Directory (AD as a Service)	Hasta 500k objetos	Ilimitado	Ilimitado
Gestión de los grupos / usuarios (añadir / actualizar / eliminar) / aprovisionamiento basado en el usuario, grabación del dispositivo empleando UI y Windows PowerShell	Si	Si	Si
Acceso SSO / Portal Access Panel para presentar las aplicaciones SaaS y aplicaciones de terceros	10 aplicaciones por usuario	10 aplicaciones por usuario	Ilimitado
Gestión y aprovisionamiento de aplicaciones en modo usuario	Si	Si	Si
Cambio de contraseña Cloud en modo autoservicio	Si	Si	Si
Herramienta de sincronización del directorio entre AD on-premises y Azure Active Directory	Si	Si	Si
Informes de seguridad estándar	Si	Si	Si
SLA de alta disponibilidad del 99.9%		Si	Si
Aprovisionamiento y acceso de aplicaciones basadas en grupos		Si	Si
Personalización de las páginas de inicio de sesión y panel de acceso a aplicaciones con imagen empresarial (logotipo, colores, …).		Si	Si
Reinicio de contraseña para los usuarios Cloud		Si	Si
Aplicación Proxy		Si	Si
Gestión de grupos en modo autoservicio para los usuarios Cloud		Si	Si
Reinicio de la contraseña para los usuarios on-premises con funcionalidad de sincronización al entorno on-premises (*write-back*)			Si
Licencias MIM (*Microsoft Identity Manager*) para realizar la sincronización de bases de datos & directorios entre los entornos on-premises y Azure Active Directory			Si
Informes de seguridad avanzados para actividades anormales (*machine learning*)			Si
Informes de utilización avanzados			Si
Autenticación de factores múltiples MFA para usuarios Cloud			Si
Autenticación de factores múltiples MFA para usuarios on-premises			Si

Escenarios de uso con Azure Active Directory

1. Introducción

Muchos escenarios de usos relacionados con la gestión de identidades corresponden directamente a las problemáticas conocidas por los administradores. Los más importantes se listan a continuación y nos permitirán comprender la importancia funcional de los servicios Azure Active Directory:

- Experiencia de autenticación e integración de la suite collaborative Office 365.
- Soporte de usuarios móviles y acceso a aplicaciones.
- Soporte de los usuarios y también de los partners en entornos heterogéneos y acceso a aplicaciones de la misma manera que para los usuarios de la empresa.
- Simplificación de las operaciones relativas a las fusiones y adquisiciones de empresas.
- Respeto de los principios de gobierno, gestión de riesgos y conformidad.
- Reducción de costes de administración a través del aprovisionamiento simplificado de usuarios.
- Gestión de acceso a aplicaciones SaaS ofrecidas en Azure y también a otros cloud, como por ejemplo las aplicaciones Google Apps.
- Gestión de identidades y uso del conector MIM Azure AD: Microsoft Identity Manager, antiguamente FIM (*Federation Identity Manager*), permite el uso de reglas de sincronización, la creación de workflows, la aplicación de directivas, el uso de conectores y ofrece a los usuarios un portal de autoservicio fácil de usar para las operaciones como el reinicio de contraseña en caso de pérdida. Para los administradores, soporta la creación de informes híbridos, la gestión de contraseñas y grupos de usuarios. Incorpora también una nueva gestión de certificados reprogramada en su totalidad, lo que es muy útil, por ejemplo, al tratarse de la gestión de tarjetas inteligentes. MIM puede utilizarse a su vez para sincronizar las identidades con los entornos no Microsoft como SAP, PeopleSoft, Oracle, por citar sólo los más importantes. Por último, Azure AD Connect se utiliza en principio para sincronizar las identidades desde Active Directory hacia AAD, o configurar los servicios de federación AD FS, lo que permitirá al usuario disfrutar de una experiencia única de autenticación de tipo SSO, para acceder a todas las aplicaciones SaaS Microsoft y no Microsoft situadas en el cloud Azure.

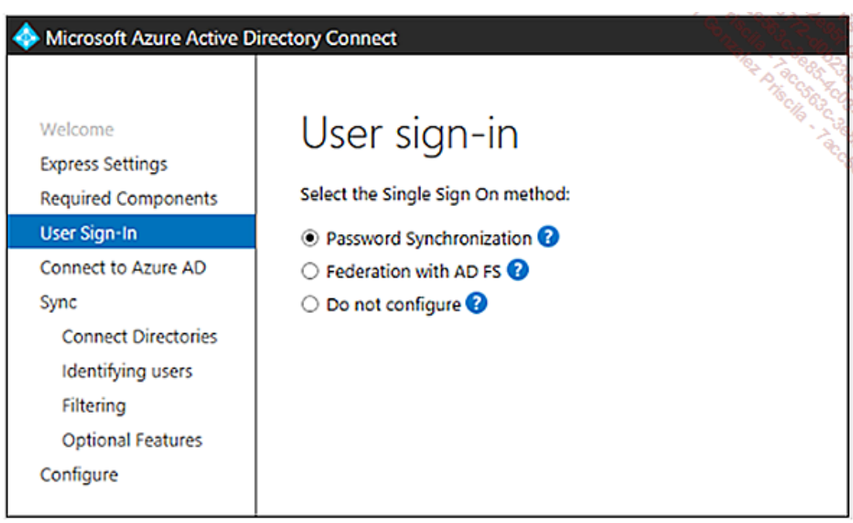
Con respecto a las licencias Microsoft Identity Manager 2016, AD Premium y EMS: cada usuario cuya identidad se gestione requiere una licencia de acceso a cliente (CAL) para MIM 2016. Observe que los empaquetamientos de soluciones Microsoft son muy interesantes. En efecto, Microsoft Identity Manager 2016 también se incluye con Azure AD Premium, que a su vez forma parte de la oferta EMS (*Enterprise Mobility Suite*). Al final, el paquete Microsoft EMS es sin duda la forma más rentable de adquirir todos los servicios de cloud Microsoft Azure con Azure Active Directory Premium, Azure Rights Management y también Intune, para el soporte de los dispositivos móviles Windows, Android y iOS.

2. Autenticación y experiencia de inicio de sesión (logon) de usuario

Uno de los puntos más importantes es sin duda el uso de la suite ofimática Office 365 y la experiencia del usuario que se ofrecerá en función del modelo de integración híbrido elegido para integrar el entorno on-premises con el cloud Azure.

Por supuesto, no se trata de un ejemplo de la problemática de SSO que será propia de cada aplicación. De igual forma, ya se trate de servicios de federación AD FS o bien de sincronización de directorios, la ampliación de los servicios Office 365 para construir nuevas soluciones es un potente eje para enriquecer la experiencia de usuario con las herramientas y soluciones basadas en la suite Office 365.

La imagen siguiente ilustra las posibilidades de hibridación propuestas por el asistente de configuración del componente de Azure AD, Azure AD Connect.



Configuración de Azure AD Connect: Sincronización o Federación

3. Sincronización de identidades

Con este modelo, las identidades de los usuarios existen dentro de los servicios de dominio Active Directory en el entorno on-premises. Luego, a través de un servidor local y el empleo de Azure AD Connect, la sincronización de cuentas y las posibles contraseñas se realiza hacia el cloud Azure. En este punto, la solución permitirá al usuario introducir una contraseña idéntica en local y en el cloud. En el momento de la conexión, Azure AD verifica la contraseña. Por último, el modelo basado en la sincronización de identidades permite responder a las situaciones enumeradas a continuación:

- La empresa posee un directorio local de Active Directory y desea sincronizar las cuentas de usuario, y si es posible las contraseñas. Si se activa esta opción, entonces los usuarios utilizarán un contraseña idéntica para acceder a los recursos locales y el entorno Office 365 en Azure.
- En primera instancia, sin duda, no deseamos desplegar los servidores necesarios para la puesta en marcha de los servicios de federación AD FS, esta operación puede realizarse más adelante.

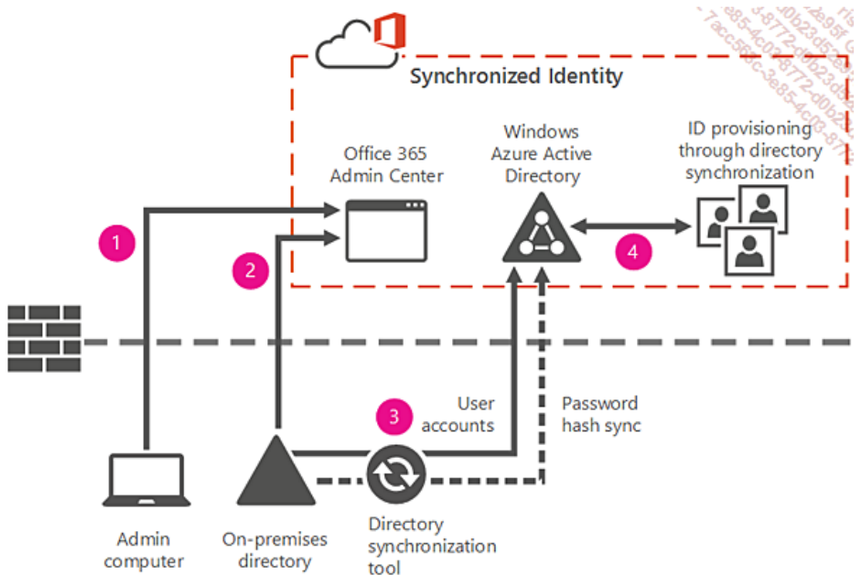
El esquema siguiente muestra un escenario donde las identidades se sincronizan y donde la sincronización de contraseñas se encuentra a su vez activada. En esta solución, la herramienta de sincronización mantiene la sincronización de las identidades de los usuarios en local y en la Nube.

- En el primer paso , se despliega el componente Azure AD Connect.

Azure AD Connect se encuentra disponible para descarga desde el sitio Microsoft en la siguiente dirección: https://www.microsoft.com/en-us/download/details.aspx?id=47594

Para obtener más información sobre la configuración de AD Connect para la sincronización de identidades, busque "configurar la sincronización de directorios" en el sitio Microsoft Office o siga el enlace: https://support.office.com/es-es/article/Configurar-la-sincronizaci%C3%B3n-de-directorios-en-Office-365-1b3b5318-6977-42ed-b5c7-96fa74b08846?fromAR=1&omkt=es-ES&ui=es-ES&rs=es-ES&ad=ES

- En las etapas 2 y 3, las cuentas de usuarios existentes dentro del servicio de directorio Active Directory en el entorno on-premises. A intervalos regulares, Azure AD Connect controla las nuevas identidades creadas de forma local, los sincroniza en Azure y luego los presenta dentro del Centro de Administración Office 365.
- Por último, en el paso 4, se sincronizan sólo las modificaciones en Azure AD y se presentan dentro del Centro de Administración Office 365.



Implementación de AD Connect para la sincronización de identidades

4. Federación de identidades

Este segundo escenario es el más logrado ya que permite una verdadera interoperabilidad de la autenticación del usuario entre los dos entornos, por una parte AD DS on-premises y por otra parte AAD - Azure AD, en el cloud.

Este es el esquema que ilustra este principio. La arquitectura híbrida utiliza los servicios de federación AD FS donde las identidades del entorno local que actúan como inquilino de Azure están federadas.

El primer punto importante es que la aplicación de los servicios de federación AD FS requiere la sincronización previa de las identidades presentadas antes. Luego, una vez sincronizadas las identidades, solo se verificará la contraseña del usuario por el proveedor de identidad local. Las consecuencias son dobles, ya que por una parte, del lado del usuario, la mejor experiencia se ofrece al usuario que solo proporciona su contraseña una vez, y por otra parte, desde el lado de la infraestructura, solo es necesario sincronizar la contraseña AD DS en Azure AD.

La utilización de los servicios AD FS con Azure y las aplicaciones SaaS Microsoft y no Microsoft estará en especial justificada en los casos enumerados a continuación:

- La infraestructura existente on-premises ya dispone de servicios AD FS para otros usos. En este caso, la misma plataforma puede ser utilizada para Ofice 365 u otras aplicaciones compatibles con los servicios de federación.
- La infraestructura existente tiene otra solución compatible capaz de proporcionar las identidades. En este caso, será posible utilizar esta identidad federada con Office 365 u otras aplicaciones compatibles.
- La empresa dispone de varios bosques Active Directory y prevé la utilización de los servicios de federación.
- Los usuarios utilizan en el entorno Active Directory on-premises la autenticación fuerte basada en certificados y tarjetas inteligentes.
- La empresa ya utiliza un entorno híbrido con una aplicación de empresa como, por ejemplo, Microsoft Exchange Server. También en este caso, se recomienda la implementación de los servicios de federación AD FS.

Para más información sobre los entornos híbridos con Exchange Online, Exchange Server 2013 o Exchange Server 2016, podemos consultar el enlace "Hybrid deployment prerequisites" disponible en la dirección: https://technet.microsoft.com/en-in/library/hh534377(v=exchg.150).aspx

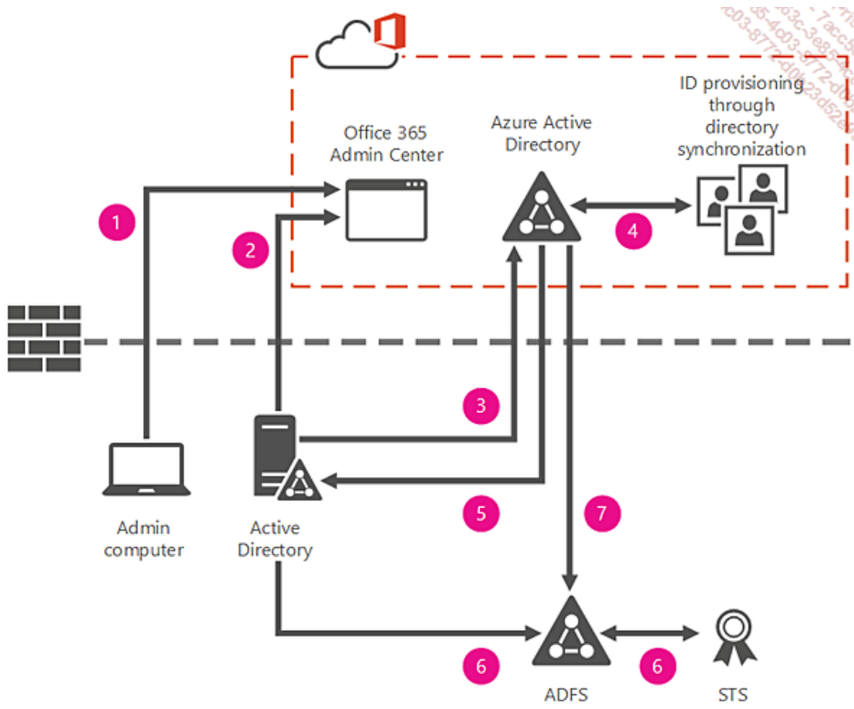
- Es importante auditar las conexiones de los usuarios.
- Se requiere que sea posible desactivar / activar de forma inmediata una o más cuentas de usuario sin necesitar una sincronización de identidades.
- Se requiere una experiencia SSO con una autenticación única.
- Se requieren restricciones de autenticación basadas en las horarios de trabajo o ubicaciones de red.

El siguiente diagrama ilustra la hipótesis de un despliegue híbrido donde las identidades están federadas en local y en el cloud Azure. En este ejemplo, aunque los servicios de dominio de Active Directory se utilizan en realidad on-premises, desde un punto de vista Azure AD, el directorio local es AD FS. En este momento, la herramienta de sincronización AD Connect mantiene la sincronización de identidades locales y en el cloud.

- Como en el caso de la primera implementación basada en la sincronización de identidades y contraseñas, es necesario instalar Azure AD Connect. Esta etapa permite mantener al día Azure AD con las últimas modificaciones introducidas en el directorio on-premises.
- Los pasos 2 y 3 muestran que los usuarios deben haber sido creados dentro de los servicios de directorio AD DS de forma local. Como en el escenario anterior, la sincronización desempeña su papel para que los objetos usuarios estén disponibles en Azure AD, y que aparezcan en el Centro de Administración Office 365.
- Los pasos 4 y 5 muestran que la sincronización entre los servicios AD DS y Azure AD sigue manteniendo los objetos al día entre ambos

entornos.

- Por último, los pasos 6 y 7 ilustran el hecho de que los usuarios federados se conectan a través de los servicios de federación AD FS que fabrican un token de acceso facilitado a Azure AD. Una vez verificado y validado el token, el usuario está autorizado para utilizar Office 365.



Implementación de AD Connect para la federación de identidades

Con respecto a los proveedores de identidades de terceros: otros proveedores de identidades distintos de los servicios AD FS de Microsoft están soportados dentro de la plataforma Azure de aplicaciones y servicios SaaS como Office 365 u otros recursos Microsoft Online Services como, por ejemplo, Intune. Entre éstos, encontramos los productos estándar de mercado como IBM Tivoli Federated Identity Manager, NetIQ Access Manager, BIG-IP o también VMware Workspace Portal.

¡Observe! Microsoft ha probado y validado estos productos de terceros solo con respecto a la funcionalidad de la Federación para el soporte de SSO. Con más precisión, esto significa que sólo la interoperabilidad basada en los protocolos WS-Federation y WS-Trust se ha validado. Por ejemplo, el protocolo SAML, utilizable también por algunas aplicaciones disponibles en el cloud, no se ha probado y validado en producción.

Microsoft establece que las funcionalidades de sincronización o autenticación de factores múltiples asociadas a estas soluciones de terceras partes no han sido validadas. Tenga en cuenta que en cuanto a soluciones de terceros, Microsoft no ofrece soporte técnico.

Para más información sobre los proveedores de identidad compatibles con las soluciones SaaS como Microsoft, Office 365, busque "Lista de compatibilidad de federación Azure Active Directory" en el sitio de Microsoft o siga el enlace: http://go.microsoft.com/fwlink/p/?LinkID=510953