Microsoft

Windows® 2000 Server

Sistema operativo de servidor

Documento preliminar de las consideraciones de diseño e implementación de Active Directory

Documento estratégico preliminar

Resumen

Windows® 2000 Server ofrece varias funciones y tecnologías que deben considerarse al diseñar e implementar Windows 2000 como una infraestructura y como una parte funcional de una organización. Este documento analiza el diseño de espacio de nombre DNS, diseño de espacio de nombre de Active Directory, planeación de seguridad y consideraciones de Políticas de grupo.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1098

PREFACIO 3
COMPONENTES ACTIVE DIRECTORY 4
Dominios 5
Unidades organizacionales 6
Domain contra OU 8
Consideraciones de diseño OU 9
ARBOLES Y CAMPO 9
Arboles 11
Campos 12
Revisión 15
NOMBRE DE ESPACIO Y JERARQUIA DE OU 14
Diseño de espacio de nombre DNS 15
Pros y contras de los dos modelos 18
Requerimientos DNS 19
Recomendaciones DNS 19
Zonas y dominios DNS adicionales 20
Revisión 21
INTRODUCCION A VARIOS METODOS DE DISEÑO Y SUS IMPLICACIONES 20
Dominio de raíz 22
Geográfico 23
Política 27
Geopolítica 30
Política geográfica 32
Funcional 35
Ubicación del controlador de dominio 37
Determinación sobre dónde colocar los controladores de dominio y catálogos globales 37
PLOT THICKENS: CONSIDERACIONES PARA SITIOS 36
Limitantes de sitio 38
Duplicación de sitio 39
Vínculos de sitio 43
Puentes de vínculos de sitio 45
Creación de topología 47
Ubicación de servicios 48
Enfoques de sitio 49
Revisión 51
SEGURIDAD 50
Roles del servidor 52
Políticas de seguridad Active Directory 54
Derechos y permisos 54
Herencia 55
Control de acceso 56
Administración delegada 58
Infraestructura de clave pública 60
Propiedades de seguridad 61
Componentes de seguridad de clave pública 62
Criptografía y claves públicas 63
Certificados 64
Servicios de certificado 65
IPSec 67
Kerberos 73
Planeación Kerberos 78
Revisión 78
GRUPOS 77
Estructura de seguridad 79
Uso de grupos 79
Revisión 85

Prefacio

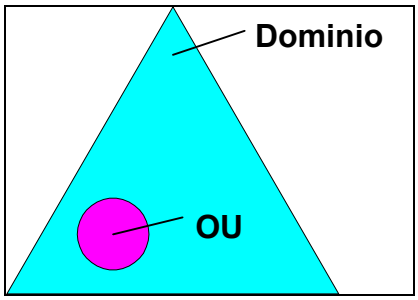
Existen diversas maneras de percibir el diseño y la implementación de Windows 2000 y Active Directory. En este documento preliminar intentaremos echar a volar la imaginación de la arquitectura del sistema y otros aspectos que tienen que considerar el enfoque y planeación del diseño e implementación. Como tal, este documento no ahondará en la información crítica que se va a utilizar al considerar el diseño e implementación de Windows 2000.

Este documento está clasificado por temas y se utiliza un flujo lógico durante el diseño de las secciones por temas las cuales son:

- Active Directory y componentes relacionados: Un panorama general en los campos, dominios y unidades organizacionales. Analizaremos su propósito, definición y uso.
- Diseño de espacio de nombre DNS: Un análisis de los diseños únicos y de espacio de nombres DNS separados. Los pros y contras de cada diseño y algunas recomendaciones básicas sobre cómo pueden ayudar a la organización.
- Diseño de espacio de nombre de Active Directory: Un análisis de los cinco modelos diferentes del diseño de espacio de nombre. La manera en que están clasificados y cómo pueden acoplarse dentro de la estructura de las organizaciones.
- Sitios: Una visión sobre cómo trabajan los sitios, su finalidad y la manera en que afectan en el diseño del espacio de nombre y estructura de dominio Windows 2000.
- Seguridad: Un panorama general sobre los aspectos básicos de seguridad y cómo afectarán el diseño del ambiente Windows 2000.
- Grupos: Un análisis de la introducción de los nuevos tipos de grupos. La planeación sobre cómo se utilizan estos grupos y cómo considerar su uso de manera cuidadosa.

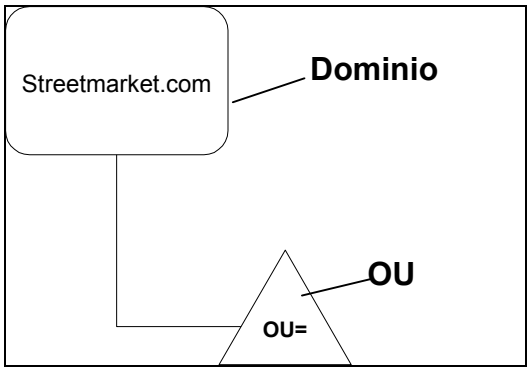
En este documento: Uso de gráficos

Con frecuencia, los gráficos utilizados en este documento muestran dominios Windows 2000 y Unidades organizacionales. Los símbolos preferentes que se utilizan para ilustrar esos componentes son normalmente un triángulo para un Dominio y un círculo para una OU.



■ Figura 1

Estas representaciones se utilizan cuando la discusión se enfoca estrictamente en árboles y campos. Lamentablemente, no es posible aplicar estos símbolos a diseños de árbol complejos. Por lo tanto, para la mayoría de los gráficos que muestran estructuras de árbol, se utilizan rectángulos redondeados para representar dominios y triángulos para representar las OUs.



■ Figura 2

El uso particular de estos símbolos deberá ser clara al ser visualizados en el contexto de las discusiones.

Componentes Active Directory

Existen diversos componentes dentro de Active Directory los cuales deben ser comprendidos a fin de que se utilicen adecuadamente. Los Dominios y Unidades organizacionales son las bases de Active Directory y definirán tanto la estructura como la funcionalidad. Asimismo, también se establecerá la manera en la que se organizan los dominios dentro de los Arboles y Campos según la intención de la política administrativa e interoperabilidad entre diversas áreas de una organización.

Esta sección da una introducción a estos componentes desde una perspectiva de arquitectura. Sus objetivos y usos serán analizados posteriormente en este documento.

Dominios

Los dominios representan una partición lógica dentro de Active Directory tanto para la duplicación de seguridad como para la de directorio. Los dominios se relacionan directamente al espacio de nombre DNS y pueden direccionarse a través de DNS.

Todos los objetos de red que existen dentro del dominio, y cada dominio contiene un grupo completo de sus objetos dentro del Contexto de denominación de dominios (NC). Teóricamente, un directorio de dominio puede contener hasta 10 millones de objetos.

Los dominios proporcionan un enlace para una seguridad y enfoque para la duplicación del NC de Dominio. Todas las políticas y configuraciones de seguridad, como derechos administrativos, políticas de seguridad y Listas de control de acceso (ACLs), no se cruzan de un dominio a otro. El administrador de dominio tiene derechos absolutos para establecer las políticas únicamente dentro del mismo dominio.

El uso particular de los dominios se puede derivar de su función. Por lo regular, los dominios se establecen ya sea para proporcionar un enfoque a la autoridad administrativa o para vincular la información duplicada como parte del NC de Dominio. Como ejemplo de lo anterior, los dominios se enfocan con frecuencia en vinculaciones geográficas a fin de proporcionar una optimización de red.

En la medida de lo posible se deberá evitar la creación de dominios para reflejar silos divisionales. En ocasiones, será necesario establecer dominios por razones políticas,

pero esto formará parte de una estrategia más amplia.

Excepto durante la migración y consolidación, los dominios nunca deberán estar establecidos a los recursos *host*. Estos se conocían como dominios de recurso en Windows NT 4.0 y ya no son necesarios en un ambiente Windows 2000.

Tener varios dominios incrementa en gran medida el exceso de trabajo administrativo asociado con la administración de Active Directory. Como un principio de diseño común, siempre debería haber alguien que comience con el número mínimo de dominios y agregue adicionales únicamente para cumplir con criterios específicos.

Unidades organizacionales

Las Unidades organizacionales (OUs) en Windows 2000 Active Directory representan todo un concepto nuevo para los administradores Windows NT. Las OUs son bienvenidas además de que proporcionan una gran cantidad de flexibilidad. Se espera que las OUs desempeñen un papel principal en la consolidación de dominio de recurso durante las migraciones de Windows NT 4.0 a Windows 2000.

Delegación de administración

Las OUs permiten la delegación granular de tareas administrativas. Esto habilita la aplicación inteligente de control administrativo en varios niveles, con lo que se permite a los usuarios, computadoras y demás objetos ser recopilados dentro de una OU, y que la administración de la misma sea delegada al administrador adecuado.

Enfoque de la política

La Política de grupo se puede aplicar a los Sitios, Dominios y Unidades organizacionales, y filtrarse con base en la membresía de grupo. De éstos, las OUs son posiblemente el depósito más funcional que pueda aceptar la política.

Al tiempo que la partición de los Objetos de política de grupo se encuentra realmente en el dominio, las OUs también, pueden formar parte de las particiones para la política. Dependiendo del fin con el que fue creada la OU, la aplicación de la política puede reflejar las reglas de negocios, obligaciones de la política técnica o automatización de tareas.

Por ejemplo, las OUs separadas deben establecerse para los empleados de tiempo completo y contratados. La política podría crearse específicamente para cada clase de empleado y aplicarse a las OUs individuales.

Consideraciones de OU

Las estructuras OU deberán ser provechosas y tener un significado. Debido a que la estructura de directorio queda expuesta a los usuarios, se deberán evitar las OUs arbitrarias. En otras palabras, no cree una estructura sólo por la estructura misma.

Asimismo, habrá que recordar que la estructura OU dentro de un dominio es independiente de cualquier otro dominio. Por lo tanto, cada dominio puede implementar su propia jerarquía OU. Esto es un arma de dos filos. Si los dominios *peer* múltiples existen con un fin similar, es muy probable que dichos dominios requieran la misma

estructura OU básica, como la establecida para *Streetmarket*.

Mientras no exista una restricción inherente a fondo sobre las OUs dentro de un dominio, existirán algunas directrices generales.

- Las estructuras OU poco profundas se desempeñan mejor que las profundas.
- No deberán existir más de 10 niveles de OUs.
- La aplicación de una política degradará a fondo las estructuras OU.

Al considerar las estructuras OU, también tome en cuenta que el propietario de una OU tiene total autoridad sobre ella y puede restringir a la aplicación de la política desde un depósito principal. Al establecer la estructura OU básica, piense en quién va a administrar la OU, así como también quién podrá visualizarla.

Estructuras OU

Las OUs dentro de Active Directory sirven para dos fines básicos:

1) Como particiones para delegación administrativa.

2) Como depósitos para la aplicación de la política.

La creación de Unidades organizacionales por cualquier otra razón deberá ser justificada. Esto significa que las Unidades organizacionales no deberán establecerse únicamente para reflejar el origen de la estructura de la compañía. ¿Por qué? Porque las OUs no son pasivas por naturaleza. Se analizan en cuanto a la política y permisos, con lo que se produce la sobrecarga del procesador. A mayor profundidad de la estructura OU, mayor límite de rendimiento. Ya que Active Directory no permite de manera natural la creación de depósitos, trata de utilizar las OUs para este fin y en algunos casos esto puede ser lo más adecuado.

Existen varias posibilidades para la creación de las OU, las cuales no infringen las reglas del fin:

- Para reflejar la estructura organizacional como departamento. En la mayoría de los casos, los departamentos son de hecho el primer nivel de la delegación administrativa.
- Función de negocios: Tal como se describe en el modelo de directorio Funcional. En ocasiones, una organización de acuerdo con su función de negocios se desempeñará por Grupos, por lo que pueden justificar las OUs creadas por esta razón.
- Basadas en objeto: Las OUs representan grupos de objetos similares como Usuarios, Computadoras, Impresoras, Enrutadores etc. Una vez más dependiendo de su estructura de directorio principal, esto puede no ser adecuado ya que el nivel más bajo de asignación de política y delegación puede ser la OU divisional.
- Basadas en proyecto: Las OUs temporales para organizar datos de proyecto relacionados, personal, etc. Las OUs ofrecen un mecanismo excelente para recolectar objetos para administración y política. Con frecuencia, los proyectos tienen requerimientos especiales que necesitan dirigirse a través de políticas

específicas y procedimientos administrativos.

- Basadas en administración: En ciertos momentos, será necesario basar las OUs en las necesidades administrativas. No obstante, esto deberá estar bien justificado ya que las OUs están expuestas a los usuarios.

Domain contra OU

La cuestión de si se deben utilizar Dominios o Unidades Organizacionales no siempre es directa. Trataremos de aplicar ciertas reglas y aclaraciones aquí.

Razones para crear dominios:

Seguridad: El requerimiento para mantener las políticas de seguridad separadas será con frecuencia un factor decisivo en la creación de un dominio. Este requerimiento puede existir cuando se cuenta con unidades empresariales autónomas con una estructura IT distribuida. Con menos frecuencia, los ambientes de alta seguridad requerirán que los sobres de seguridad sean distintos, como en el caso de compañías de petróleo y farmacéuticas.

Duplicación: Otra circunstancia común y con frecuencia válida para un ambiente de dominios múltiples es controlar el enfoque de duplicación basado en la región geográfica. Mientras que los sitios proporcionan un mecanismo para realizar una duplicación eficiente, las condiciones de red pueden afectar la duplicación sin necesidad de datos a través de los enlaces de red.

Migración: En una infraestructura Windows NT será necesario establecer desde el principio un mapa de uno a uno entre los dominios Windows NT y Windows 2000. Los detalles de migración se analizan más a fondo posteriormente en este documento.

Razones para no crear dominios:

Para reflejar la estructura organizacional: De ser posible, evite la creación de dominios basados en divisiones, departamentos o grupos. Un diseño adecuado deberá poder resistir a las reorganizaciones de la compañía sin requerir la reestructura de su jerarquía de dominio.

Para reflejar la función de negocios (también denominada políticas): La reorganización de negocios es muy frecuente dentro de las compañías hoy en día. Los dominios se basan en silos políticos que ofrecen muy pocos beneficios funcionales.

Cuándo crear unidades organizacionales:

Para controlar la administración: Las OUs actúan como particiones para la delegación administrativa. Un uso frecuente de OUs proporcionará el enfoque de la administración de recursos.

Para reemplazar los dominios de recurso Windows NT 4.0: En la mayoría de los casos, se pueden reemplazar los dominios de recursos Windows NT 4.0, uno por uno con OUs. Una vez que un dominio de recurso ha sido migrado a Windows 2000, es fácil convertirlo en una OU.

Para enfocar la política administrativa: Las particiones de la delegación política y

administrativa con frecuencia son sinónimos pero no deberán definirse desde un principio en el proceso de planeación. El método más fácil de aplicación de política es mediante una OU, pero una OU creada estrictamente para la política puede ser confusa. Por ejemplo: "OU = Usuarios de terminal Windows" no sería una buena opción para una OU.

Para reflejar la Estructura organizacional: En la medida en que soporten la administración, las OUs deberán proporcionar algunos detalles como la estructura organizacional de la compañía.

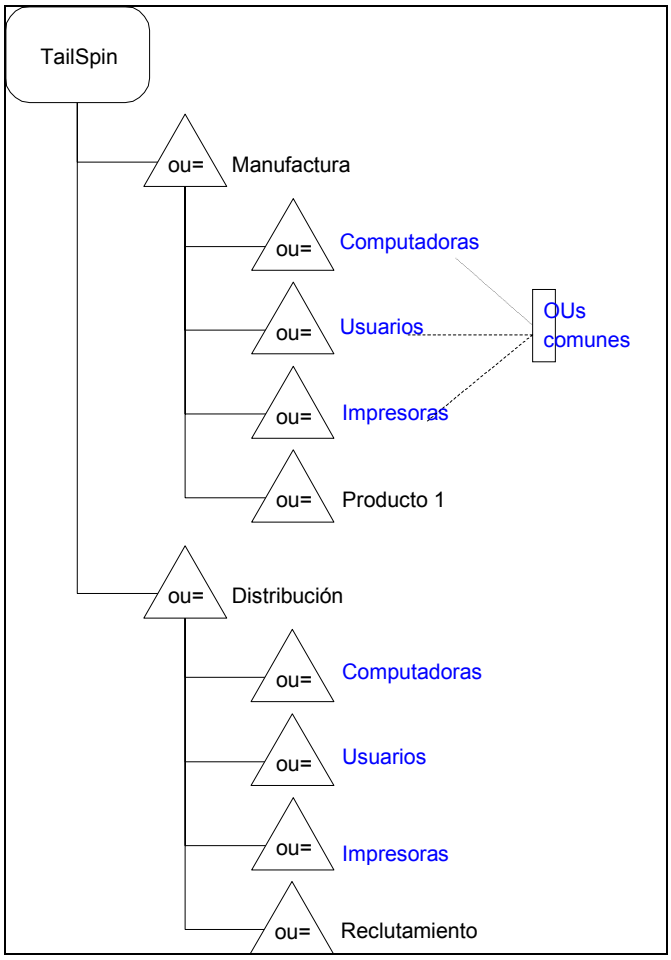
Cuándo no crear Unidades organizacionales:

Para reflejar los silos políticos: Será necesario reflejar los silos políticos, haciéndolo utilizando grupos. Una OU etiquetada "VPs del noreste y amigos" no es un uso adecuado.

Para crear una estructura arbitraria: Las OUs no deberán utilizarse como grupos, y no deberán crearse como colocadores de una estructura apartada. Por ejemplo: Una OU etiquetada como "Unidades de negocios" la cual contiene OUs menores denominadas para cada unidad de negocios debería ser cuestionable a menos de que la delegación de política o administrativa fuera aplicada a la OU denominada "Unidades de negocios".

Consideraciones de diseño OU

Al diseñar las jerarquías de directorio potenciales, identifique aquellos elementos que son comunes para más de una unidad de negocios, unidad de división o administrativa y establezca algunas convenciones para estructura OU a fin de proporcionar consistencia.



■ Figura 3

Es adecuado proporcionar una estructura base para las Unidades organizacionales o inhabilitar por completo la capacidad de crear Unidades organizacionales.

En el ejemplo anterior, tanto la Manufactura como la Distribución comparten algunos requerimientos comunes, uno de los cuales es un lugar para administrar y manejar y controlar a sus usuarios, computadoras e impresoras. Como tal, se implementó una convención para OUs comunes la cual dio como resultado tres OUs (computadoras, usuarios, impresoras) que han sido establecidas bajo cada OU divisional primaria. Al establecer alguna estructura preliminar, los usuarios enfrentan visualizaciones consistentes y se apegan a un nivel de consistencia administrativa.

Mientras no exista una limitación inherente para el número de OUs en nido, las estructuras profundas de OU ocasionarán degradación en el rendimiento. Si se requieren más de 10 niveles de OUs, se deberá considerar la implementación de una estructura diferente.

Arboles y campos

Active Directory utiliza *árboles* y *campos* para proporcionar enlaces lógicos y formaciones que definirán la manera en la que se va a comunicar la extensión de los dominios. Al igual que los

dominios y unidades organizacionales, estos componentes proporcionan la funcionalidad específica y se establecen para cumplir los requerimientos específicos.

Arboles

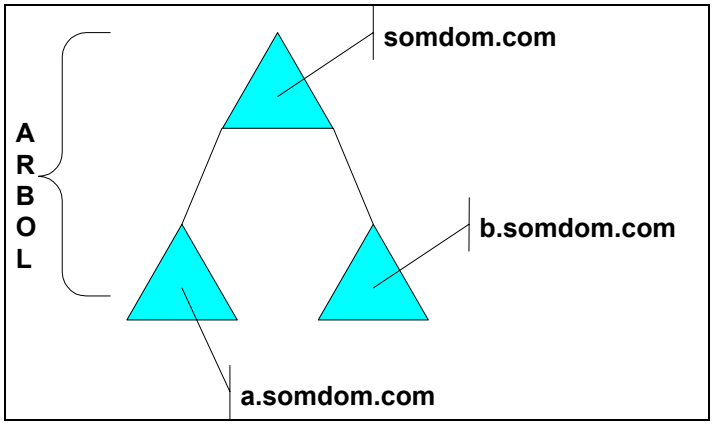
Un árbol es una recopilación jerárquica de los dominios ordenados en un espacio de nombre contiguo.

(Un árbol también puede consistir en un dominio único Windows 2000. Sin embargo, puede crear un espacio de nombre más largo uniendo dominios múltiples en una estructura jerárquica).

Los dominios en un árbol se conjuntan de manera clara a través de dos salidas: relaciones verdaderas transitivas Kerberos. Una realidad transitiva Kerberos significa simplemente que el Dominio A confía en el Dominio B y que el Dominio B confía en el Dominio C, después el Dominio A confía en el Dominio C. Por lo tanto, un dominio que une un árbol tiene de inmediato relaciones verdaderas establecidas con cada dominio en el árbol. Estas relaciones verdaderas hacen que todos los objetos que se encuentran en todos los dominios del árbol estén disponibles para los demás dominios del mismo.

Todos los dominios dentro de un árbol único comparten un espacio de nombre común y una estructura de denominación jerárquica. Siguiendo con los estándares DNS, el nombre del dominio de un dominio menor es el nombre relativo del dominio menor que se adjuntó al nombre del dominio mayor.

Todos los dominios que se encuentran dentro de un árbol único comparten un *esquema* común, el cual contiene definiciones formales de todos los tipos de objetos que se pueden almacenar en una implementación de Active Directory. Además, todos los dominios que se encuentran dentro de un árbol único comparten un *catálogo global* común, el cual es el depósito central de información para los objetos que se encuentran en un árbol o campo.



■ Figura 4

No existe un límite específico de profundidad para un árbol, pero al igual que los dominios, los árboles tienen el procesamiento asociado y las estructuras a fondo afectarán el rendimiento.

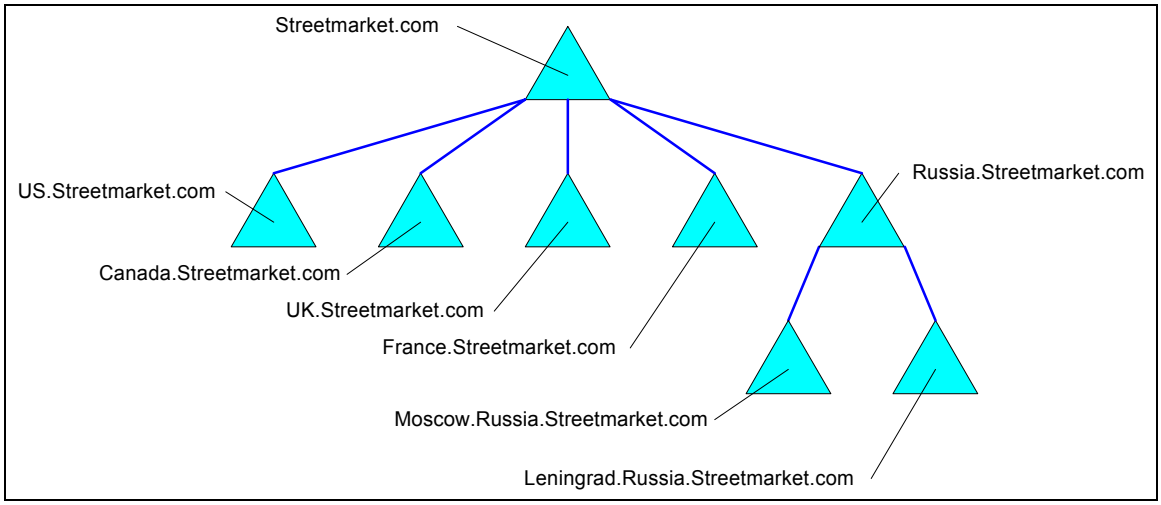
Uso del árbol

Los árboles definen la mayoría de la estructura de Active Directory y hablan para el uso del dominio. Desde una perspectiva de diseño cronológica, la estructura del árbol no deberá preceder las definiciones de dominio. Los dominios deberán definirse de acuerdo con las reglas relacionadas con el uso del mismo. Posteriormente, los dominios deberán ordenarse dentro de una estructura de árbol en forma lógica. Por ejemplo, supongamos que *Streetmarket* ha definido los siguientes dominios:

- EUA
- Canadá
- Reino Unido
- Francia
- Rusia
- Moscú
- Leningrado

Los dominios fueron establecidos para mitigar el impacto de la red relacionado con la duplicación del Dominio NC y en el caso de Moscú y Leningrado, fueron establecidos por la falta de soporte a los servicios de red. Estos dominios se pueden convertir en OUs, las cuales deberán establecer los servicios de red que van a ser implementados.

La estructura de árbol resultante, dará como resultado el árbol siguiente.

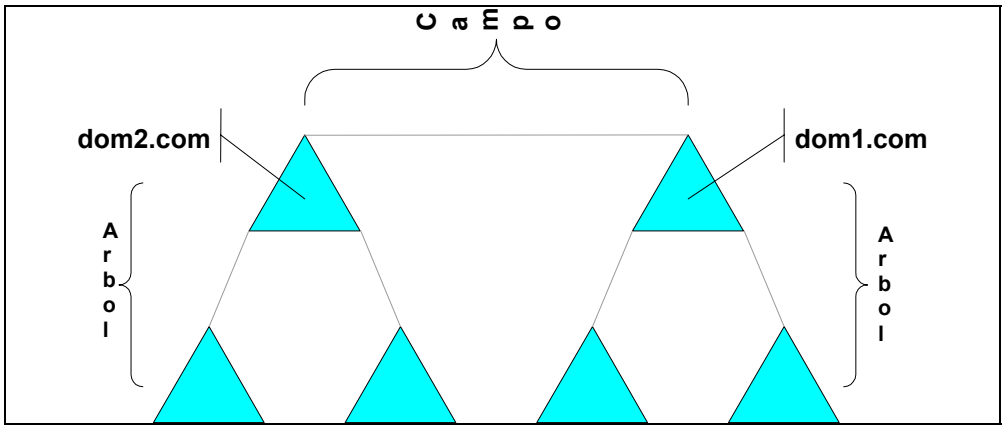


■ Figura 5

En el caso ilustrado anteriormente, los dominios están organizados en un árbol donde el primer nivel de dominios está basado en el país y el segundo nivel de dominio se basa en las ciudades. Sin embargo, los dominios en sí se establecieron sin tener ninguna relación con la estructura resultante del árbol.

Campos

Un *campo* es una agrupación de uno o más árboles, los cuales participarán en un sistema de comunicaciones común.

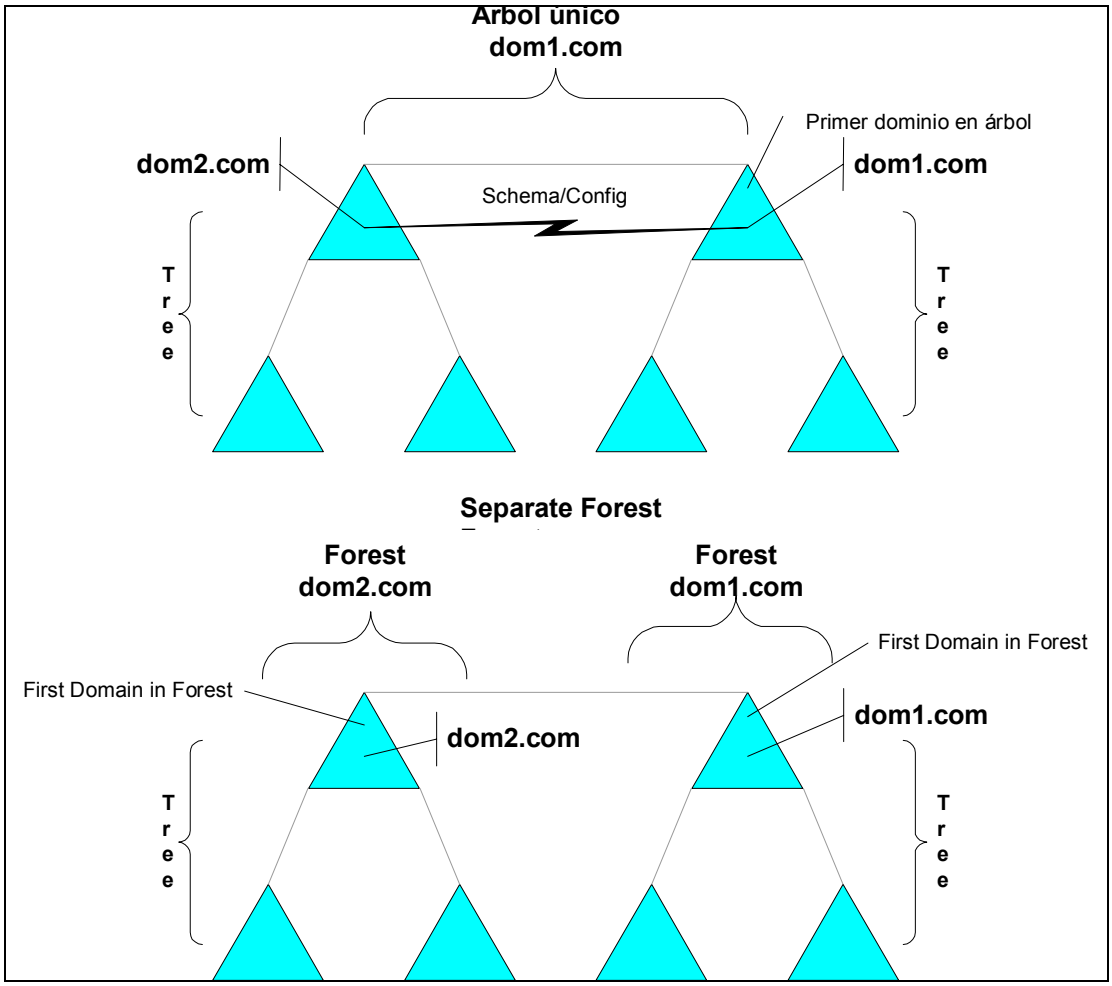


■ Figura 6

Un campo proporciona los vínculos para muchas de las funciones que existen dentro de Active Directory como la seguridad, convenciones y catálogo global.

Dentro de un campo, existe un esquema duplicación único, el cual es controlado a través de un servidor de esquema maestro en un dominio de raíz.

Las confianzas *Kerberos* nunca son transitivas a través de los campos los cuales serán adecuados para las disposiciones de sociedad, donde también la confianza real es limitada.



- Figura 7

Lo diferente entre un campo único y un separado es aquello en los objetos de conexión que duplican el Esquema y los NCs de configuración, así como el Catálogo global. En la figura anterior existen los mismos árboles en ambos casos, pero desplegar dom2.com en un campo separado, tuvo el efecto de desasociar por completo el árbol tres del dom1.com. Una confianza *Kerberos* puede seguir existiendo entre los dos campos, pero compartir el Catálogo global y el Esquema y NCs de configuración ya no es factible. El efecto neto de separar estos árboles de esta manera son dos sistemas de comunicación separados.

Uso del campo

El uso del campo puede originarse de la necesidad de mantener dos esquemas separados, como en el caso de la unidad de negocios, la cual mantiene una aplicación no digna. Asimismo, surgirán diferentes campos para proporcionar la separación entre los recursos DNS internos y externos.

De manera funcional, establecer un campo único o dividir los árboles en campos separados es una decisión que se toma fácilmente durante la instalación de Active

Directory. Esta es una decisión que no deberá ser tomada a la ligera, debido a que el impacto es grande y duradero. Los campos pueden no surgir en este momento y la duplicación entre los mismos no será soportada.

Los aspectos funcionales de este tipo de estructura pueden no ser para lo que fueron planeados en un principio. Al utilizar más de un árbol en un campo único, sólo se utilizará cuando sea necesario. Por ejemplo, si Streetmarket.com es el nombre de dominio estratégico y Sidestreet.com es una estructura heredada soportada o una unidad de negocios autónoma, entonces los dos árboles de nivel superior serían los adecuados.

En otros casos, los árboles secundarios de un campo con frecuencia serán migrados o subpresentados en un árbol homogéneo. Los árboles adicionales no proporcionan beneficios únicos en una estructura de árbol único.

Revisión

Los componentes analizados en esta sección fueron los Dominios, Unidades organizacionales (OUs), Arboles y Campos. Los dominios son particiones de Active Directory que se utilizan principalmente para enfocarse en la autoridad administrativa y para limitar el enfoque de la duplicación. Las OUs son particiones administrativas de Active Directory que habilitan la delegación granular de tareas administrativas y son activos por naturaleza. Los árboles son grupos de dominios que forman un espacio de nombre contiguo y los campos son uno o más grupos de árboles que comparten un esquema común y Catálogo global.

Es importante comprender bien los componentes de Active Directory ya que existen *"bloques de funciones"* de Active Directory. Entender el significado y uso de estos componentes es la clave para crear una estructura de directorio bien diseñada.

Nombre de espacio y jerarquía de OU

Esta sección direcciona las técnicas y metodología de establecer y ordenar los componentes del árbol de información de directorio (DIT). Se tienen que tomar varias decisiones relacionadas con la estructura actual del árbol Active Directory. Esas decisiones se basarán en una combinación de diversos factores como son la estructura organizacional, estructura administrativa y diversidad geográfica. Esta sección proporcionará un entendimiento de acuerdo con las mejores prácticas para el diseño de espacio de nombre.

Diseño de espacio de nombre DNS

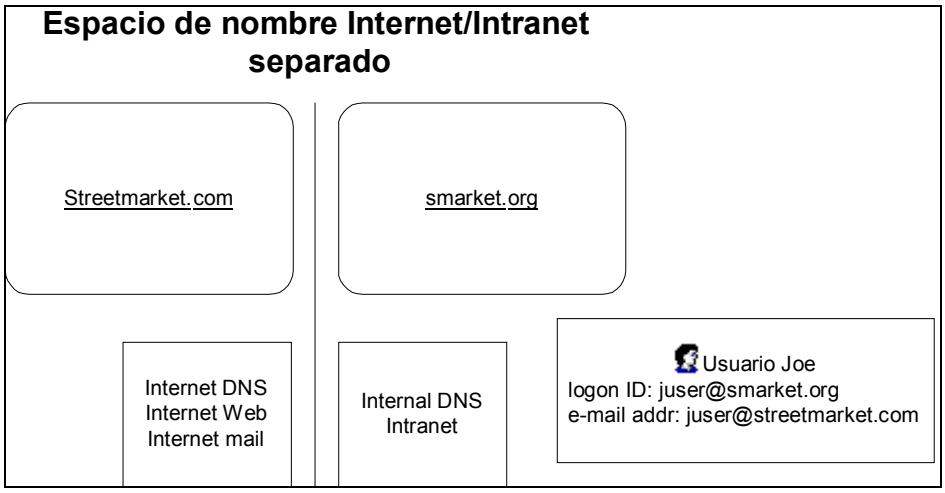
Hoy en día las redes desempeñan dos papeles: Uno es dar servicio a las necesidades de comunicaciones internas y otro es dar servicio a las solicitudes que se originan por Internet. Evidentemente, el DNS desempeña un papel principal al determinar cómo interoperan estos dos reinos. Existirán dos opciones para la infraestructura DNS básica, la cual tendrá un impacto en el diseño de espacio de nombre más adelante.

Una de las primeras decisiones que se deben tomar relacionadas con el diseño de nombre de espacio es la determinación del papel de DNS y cómo será organizado su DNS. ¿Un solo nombre de espacio DNS dará servicio a los servicios internos y de Internet o se separarán los nombres de espacio?

Modelo 1: Espacio de nombre DNS interno/Internet separados

Active Directory presenta la integración de DNS y el directorio corporativo. Los beneficios que se obtienen a partir de este tipo de integración son muchos, pero dichos aspectos no deben relacionarse desde un principio con el proceso de diseño. La principal de estas decisiones es elegir si se tiene que hacer una distinción entre los espacios de nombre de raíz internos y externos. Para infraestructuras DNS maduras, esta opción en su mayoría será dedicada por el ambiente DNS heredado, pero si es adecuada una modificación al sistema DNS, ahora será el tiempo de hacerlo.

La decisión sobre si se tiene que mantener un espacio de nombre DNS interno y externo separado se basa en la lógica convencional, pero las implicaciones se extienden en un ambiente Windows 2000. El espacio de nombre se utiliza de manera interna y afecta directamente a los usuarios finales ya que es parte de su nombre de conexión. Consulte los ejemplos ilustrados en la figura siguiente. Al utilizar espacios de nombre separados, el Usuario Joe debe saber la distinción entre su nombre de acceso: juser@smarket.org y su dirección de correo electrónico en Internet: juser@streetmarket.com. Utilizando un espacio de nombre único, el usuario Joe necesita únicamente conocer y utilizar un solo espacio de dirección: @streetmarket.com.



■ Figura 8: Dominios Internet e internos separados

Evidentemente, la conveniencia de un usuario no es única o necesariamente la consideración más importante. Asimismo, la seguridad y administración también se verán impactadas por esta decisión. En este caso, mantener una separación entre los espacios de nombre internos y externos proporciona una mayor seguridad y simplifica la administración.

Los espacios de nombres separados publican dispositivos en Internet en un nombre de dominio completamente diferente de los dispositivos internos. En esta configuración, únicamente aquellos servicios internos que se requieren específicamente se publican en Internet. Establecer ese tipo de formación es muy sencillo, ya que la administración y los dispositivos en sí se mantienen por separado.

Existen pocos métodos conocidos de configuración de manera que no se comprometan

los registros internos.

- Ya que tanto los nombres de dominio en Internet como intranet deberán registrarse con Internic, las entradas SOA para ambas zonas serán accesibles en Internet. Como tal, el primer paso será crear dos zonas primarias en el servidor DNS Internet. Una para el sistema de dominio Internet, la otra para intranet.
  a) En el servidor DNS basado en Internet, se creó una zona primaria para Streetmarket.com (el dominio en Internet)
  b) En Internet basado en el servidor DNS, se crea una zona primaria para smarket.org (el dominio intranet).

Los problemas de seguridad dictan que los servicios internos no sean publicados en Internet. Para cumplir este requerimiento, el sistema DNS de intranet también debe albergar la zona DNS intranet, como la zona primaria. En este punto, los dos sistemas DNS no tienen conocimiento el uno del otro y responderán a las solicitudes para el nombre de dominio intranet. Existen dos puntos adicionales de configuración que son necesarios para asegurar que la zona en intranet reciba todas las solicitudes adecuadas y también quede protegida de la exposición a Internet.

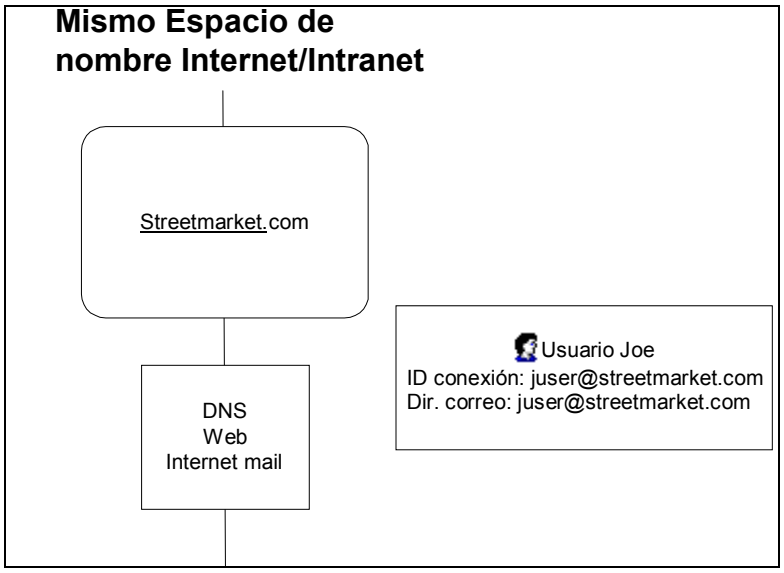
- En el sistema DNS Internet, delegue control de la zona intranet al servidor DNS interno estableciendo un registro tipo NS, indicando el servidor interno.
- En el servidor DNS intranet, cree una zona primaria para smarket.org. Esta será la ubicación que albergue realmente los registros de servicio interno.

Además, establezca el servidor DNS en Internet como el direccionador para el sistema DNS intranet, de manera que el servidor DNS intranet no intente resolver las consultas externas directamente en Internet, sino que pase las solicitudes a través de los servidores DNS de Internet.

Un espacio de nombre único requiere que los servidores *proxy*, *firewalls* y clientes se configuren para distinguirse entre los recursos internos y externos. Mantener una separación del espacio de nombre proporciona esto naturalmente . La seguridad bajo un espacio de nombre separada también es fácil de mantener, ya que de manera predeterminada, no deberán publicarse nombres de recursos internos en Internet.

Modelo 2: Espacio de nombre de dominio de raíz única

La implementación de un dominio DNS único servirá tanto para las consultas de nombre internas como en Internet. En este caso, una zona única abarcará los sistemas DNS Internet e intranet, dando como resultado un espacio de nombre único para la organización.
Los problemas inmediatos surgen relacionados con el uso de un dominio único DNS, tal como el que se utiliza para evitar la publicación de los registros DNS a Internet.



■ Figura 9: Espacio de nombre de raíz DNS única

El requerimiento para asegurar los registros internos aún existe, de tal forma que se deberá utilizar el método de separación de recursos. Nuevamente separar los servidores DNS se utiliza para dar servicio a los servicios de Internet e internos. En este caso la zona primaria para el nombre de dominio se creará tanto en los servidores DNS de Internet como intranet. En este estado, ninguno de los servidores DNS sabe del otro. Esto cumple con los criterios de seguridad deseados para separar los registros por sí mismos.

El servidor DNS intranet nunca deberá quedar expuesto a las solicitudes de Internet o recursión, sino que deberá poder dar servicio a las resoluciones de nombre para las cuales no tiene autoridad. Para cumplir con esto, el servidor DNS de intranet deberá configurarse para utilizar el servidor DNS de Internet como un direccionador.

Los registros en este caso serán administrados como si existieran zonas para dos dominios separados. Los registros de Internet se publican en el sistema de Internet, y los registros internos se publican en el sistema intranet. La configuración resultante establece, de manera efectiva, dos zonas separadas. Incluso aunque compartan el mismo nombre de dominio, ningún servidor tiene conocimiento de que existe otro.

Pros y contras de los dos modelos

Modelo 1:

Mantener una separación entre los dominios internos y de Internet tiene algunas ventajas.

- Existe una distinción clara entre los recursos Internet/intranet desde la perspectiva de administración como desde la del usuario final.
- La estructura es más fácil de administrar ya que no se une el espacio de nombre y se puede mantener separado.
- La configuración del explorador del cliente también es más fácil ya que la lista de excepciones no necesita mantenerse para distinguir entre los recursos de Internet e

intranet.
- La configuración del cliente *proxy* es más simple por la misma razón. Se debe evitar utilizar un servidor *proxy* para los recursos internos. Para llevar a efecto esta configuración, deberá proveerse una lista de excepciones a fin de permitir al cliente distinguir entre los dos reinos.

La desventaja de esta configuración es:

- El nombre de conexión del usuario es diferente al nombre de correo electrónico. Si los usuarios han estado operando bajo un espacio de nombre homogéneo, cambiar los espacios de nombre a separados puede ser una experiencia traumática. Recuerde que mientras no exista un contexto complejo relacionado con los usuarios, aún queda expuesto el contexto DNS (juser@somdom.com) lo cual será diferente a la dirección de correo en Internet.
- <insert table from PPT>

Modelo 2:

El punto principal de esta formación es que los usuarios ven una o dos visualizaciones de Internet e intranet. Es opción del administrador hacer una distribución de respaldo entre las dos redes.

El manejo y la administración son un poco más difíciles en este caso ya que mientras que los sistemas se distinguen de manera técnica, la especificación debe realizarse como dos recursos que existen en la zona primaria. Esto puede conllevar a los problemas de seguridad que resultan de los recursos internos que se están colocando de manera inadvertida al sistema DNS Internet.

<insert table from PPT>

Requerimientos DNS

DNS de Microsoft no se requiere estrictamente para Active Directory, sino que utiliza un sistema DNS de terceros y debe soportar algunos requerimientos.

- El registro de recurso de Ubicación de servicio (SRV RR), RFC 2052
- El protocolo de Actualización dinámica, RFC 2136

Si no existe una infraestructura DNS, la opción lógica se implementa a Microsoft DNS. Sin embargo este caso es poco común, y de ser así, deberá tomarse una determinación para adecuar el sistema DNS heredado.

Además de los requerimientos funcionales básicos de reunir SRV y el soporte de actualización dinámica, se debe considerar otro aspecto. ¿La zona heredada caerá dentro de la zona DNS deseada para su uso con Windows 2000?

Recomendaciones DNS

También hay que tomar en cuenta que aun cuando el sistema heredado cumpla con los requerimientos, tendrá que seguir considerando que las actualizaciones dinámicas serán

duplicacadas entre sus zonas. Esta no es una consideración sin importancia. El DNS dinámico puede dar como resultado miles de entradas existentes en una base de datos DNS. Incluso con transferencias de zonas cada vez mayores, la base de datos del archivo de texto plano es mantenida por el software DNS convencional y queda a salvo de cualquier daño y asume dicho exceso de duplicación.

Sin embargo, Microsoft DNS permite la integración de la base de datos directamente a Active Directory lo que da como resultado un mecanismo de duplicación mucho más sólido para los registros DNS.

Si el sistema DNS heredado no cumple con los requerimientos necesarios para Active Directory, existen tres opciones:

- Actualizar el o los servidor(es) existentes a fin de cumplir con los requerimientos.
- Migrar el o los servidor(es) a Microsoft DNS.
- Seleccionar un nombre nuevo (separar nombres de dominio) y delegar la zona interna para Microsoft DNS.

Con todos los aspectos considerados, la implementación de Active Directory es una buena oportunidad de migrar a Microsoft DNS en su totalidad, en caso posible. Microsoft DNS es realmente madura en este punto y ofrece un excelente rendimiento y soporte para los estándares.

Zonas y dominios DNS adicionales

Hasta aquí, hemos direccionado únicamente la raíz de los dominios DNS/Active Directory. La mayoría de las circunstancias requerirán que muchos otros dominios y zonas existan para dar servicio a subdominios y zonas secundarias.

Subdominios

Aparte de los dominios DNS de raíz, cada dominio menor Windows 2000 en la mayoría de las circunstancias, se clasificará como un subdominio y tendrá un espacio de nombre DNS asociado. Están disponibles diversas opciones para el establecimiento de los servicios DNS para los dominios menores.

El procedimiento recomendado para establecer los servicios DNS para un dominio menor es crear primero un subdominio en la raíz interna y delegar el subdominio a un servidor DNS activo dentro del dominio menor:

- Cree un subdominio DNS para el menor desde el dominio de raíz (por ejemplo, Child.root.com)
- Cree una zona DNS primaria para el menor dentro de su propio dominio (por ejemplo, Child.root.com)
- Desde la raíz, delegue el subdominio para el servidor DNS menor.

Existen otras opciones disponibles que deben ser utilizadas por menos de las circunstancias óptimas. Por ejemplo, no es necesario, establecer un DNS en un dominio menor. El dominio menor se puede crear como un subdominio en un mayor o de raíz para el servicio menor. En este caso, los servicios DNS podrían establecerse en

child.root.com que posteriormente podrían albergar zonas secundarias para el mayor o la raíz.

Zonas secundarias

Las zonas DNS secundarias existirán probablemente en la mayoría de los casos. Una zona secundaria es una copia de sólo lectura de la zona primaria utilizada para distribuir servicios DNS para resolución de consulta. Sin embargo, en Windows 2000, también puede existir una zona secundaria de escritura si DNS es Active Directory integrado. La capacidad de escritura en zonas secundarias proporciona un elemento clave en el ambiente DNS de Windows 2000 con actualización dinámica.

De manera predeterminada, todos los clientes con DHCP Windows 2000 solicitarán DHCP para actualizar de manera automática DNS. Deberían existir zonas secundarias cuando no hay Active Directory integrado, las modificaciones de actualización sólo pueden ser escritas al servidor DNS que actúa como SOA para la zona (primaria). El impacto de esto puede ser muy importante. Dado el gran número de clientes o ambiente distribuido, los registros DNS a la zona primaria y el tráfico de red asociado pueden tener un impacto drástico tanto en el servidor como en el rendimiento de red. Por esta razón, es muy recomendable que todos los controladores de dominio que contengan DNS sean Active Directory integrado.

Revisión

El diseño del espacio de nombre DNS representa una parte integral del diseño de su estructura Active Directory de su empresa. En esta sección analizamos los beneficios y desventajas de tener un espacio de nombre separado sencillo. En breve, el espacio de nombre separado es más flexible, pero requiere un mayor ajuste por parte de los usuarios finales. El diseño de espacio de nombre sencillo es más intuitivo para los usuarios, pero también es más difícil de administrar. Asimismo, esta sección abarca los requerimientos y recomendaciones DNS. Tome en cuenta que su sistema DNS debe soportar registros SRV RR y actualizaciones dinámicas. Microsoft DNS es el sistema de su elección ya que cumple con estos requerimientos y también permite la integración de la base de datos directamente en Active Directory, dando lugar a un mecanismo de duplicación más sólido para los registros DNS.

Introducción a varios métodos de diseño y sus implicaciones

El crecimiento rápido de tecnología durante la última década ha dado como resultado un cambio masivo desde un *host* hasta sistemas distribuidos. Esto también ha dado lugar a un gran incremento en los costos de informática relacionados con la implementación y administración de estos sistemas. Lamentablemente, también existen varias limitantes en los presupuestos de informática para reimplementar una infraestructura distribuida después de un ciclo de vida relativamente corto. Un buen diseño de sistemas distribuido deberá durar muchos años y deberá tener que realizar únicamente una actualización de tecnología como resultado de las actualizaciones para dar soporte al software.

Esto es más fácil de decir que de hacer. Con pocos elementos para el diseño se pueden tener

severas consecuencias originadas ya sea por las reorganizaciones o por las estructuras corporativas que no escalan y que son difíciles de administrar.

Active Directory requiere planeación antes de la implementación pero se obtendrán ganancias valiosas como resultado de una superestructura ampliable para redes distribuidas. La primera etapa de planeación es definir el método básico que se puede utilizar para definir el diseño de espacio de nombre.

Existen tres tipos básicos de diseños de espacio de nombre: Geográfico, Político y Funcional. Además de estos principios básicos, se pueden incluir combinaciones simples para unificar los atributos para el diseño de espacio de nombre. Casi todas las organizaciones adoptarán uno de estos principios de diseño.

Dominio de raíz

Sin importar cuál sea la base para la estructura de directorio, el componente más crítico es el dominio de raíz. Mientras que los cambios para cualquier nivel de estructura del dominio pueden ser difíciles, modificar el espacio de nombre de raíz es particularmente algo poco placentero. Este tema se cubrió parcialmente en la sección DNS, la cual proporcionó los métodos y razones para establecer un dominio de nivel alto.

Además de estas consideraciones, existen atributos específicos del dominio de raíz. El dominio de raíz (nivel alto) es el primer dominio que se instaló en el campo. Este dominio no puede renombrarse ni eliminarse. Asimismo, el dominio de raíz proporciona dos papeles de Operaciones maestras únicas flexibles clave (FSMO) para todo el campo.

La parte más importante del dominio de raíz sugiere que por lo menos deberá ser permanente por naturaleza. Teniendo esto en cuenta, el nombre del dominio de raíz debería ser importante para el nivel alto de la organización, como el nombre de la compañía. Este directorio se correlaciona con el nombre DNS de raíz, el cual será utilizado para servicios internos.

El dominio de raíz por lo regular será activo, lo que significa que será utilizado como cualquier otro dominio y que alojará OUs, usuarios, recursos y otros objetos. De manera alterna, el dominio de raíz deberá ser estático en su naturaleza y existir simplemente como un *placeholder* en el campo para otros dominios menores. El uso de los dominios *placeholder* debe ser adecuado cuando la organización ya ha implementado un espacio de nombre menor para utilizarlo en comunicaciones internas. Por ejemplo, si *Streetmarket* estuviera utilizando inside.Streetmarket.com como una zona intranet antes de la implementación de Windows 2000, establecer un dominio de raíz de Streetmarket.com como *placeholder* sería lo adecuado.

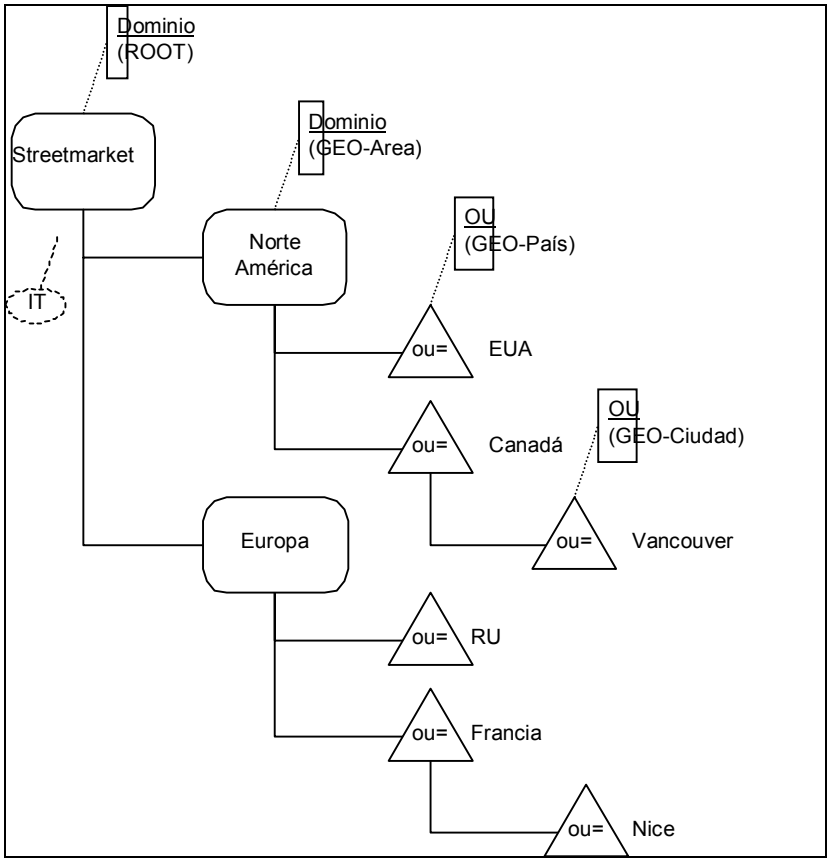
Otro caso en el que el dominio de raíz *placeholder* podría ser utilizado es cuando una compañía desea mantener un solo campo, pero los aspectos de seguridad requieren que los usuarios y recursos para las divisiones no se mezclen dentro del mismo dominio. Normalmente, esto podría dar como resultado un campo de dos árboles. Sin embargo, el uso de un dominio *placeholder* de raíz se puede utilizar como un principal estéril para ambos árboles divisionales.

Geográfico

Es una estructura que se define por ubicaciones físicas y es conocida como recolecciones Geográficas. Esto es un fundamento popular para el diseño de espacio de nombre debido a la impenetrabilidad para una reestructuración organizacional.

Al utilizar la geografía como una base para la estructuración el directorio trabaja particularmente bien de manera directa por debajo del nivel de raíz del directorio, donde las modificaciones hechas a la estructura del directorio tienen el impacto operativo más grande.

El siguiente diagrama muestra una estructura de directorio basada en la geografía para una compañía denominada Streetmarket.



■ Figura 10: Geográfico

La Figura 10 muestra una jerarquía geográfica típica implementada para Streetmarket. El primer nivel de dominio está basado en divisiones continentales y la estructura secundaria está basada en el nivel por país. Un aspecto relevante de esta estructura es su elasticidad en comparación con las reorganizaciones corporativas. Excepto para conflictos civiles o cambios en placas tectónicas, los límites no quedan sujetos a cambio, lo cual proporciona una estabilidad inherente para este diseño.

Para implementar de manera satisfactoria un modelo geográfico, la informática centralizada es obligatoria. A menos que la propia estructura organizacional esté basada en recolecciones Geográficas (lo que haría un modelo político), una entidad única debe

tener autoridad sobre todos los recursos divisionales. En la mayoría de las grandes organizaciones, ésta es una ocurrencia poco frecuente.

Este modelo soporta lo siguiente:

- Organizaciones altamente distribuidas.
- Informática centralizada.

Las opciones sobre cómo definir las recolecciones geográficas actuales para la estructura de directorio varían, pero en su mayoría frecuentemente son manejadas por un requerimiento para duplicación de partición basado en las condiciones de red. El uso de dos dominios de primer nivel en el ejemplo anterior proporciona un buen mapa para los componentes de red primarios que forman parte del curso, y que también están basados en la geografía. Al utilizar los dominios de esta manera, se conserva un tanto del ancho de banda que probablemente sería un enlace trasatlántico costoso. En las grandes organizaciones, esto podría ser una cantidad sustancial de tráfico de red.

Mientras este punto podría ser un asunto de semántica, los dominios no podrían ser creados en este modelo para proporcionar particiones para seguridad. Las particiones de seguridad siempre se basarán en la política y no en los requerimientos geográficos. El hecho de que las leyes internacionales requieran potencialmente dominios distintos entre límites internacionales es el hecho de una política y no de una consideración geográfica.

Como se describe en la sección de variaciones, los dominios deben ser poco profundos o profundos, dependiendo del tamaño de la compañía y de las condiciones de red.

PROS

- La estructura de árbol es inmune a la reorganización corporativa.
- El árbol puede aceptar la expansión. Las recolecciones geográficas adicionales o divisiones se pueden agregar fácilmente.
- Esta estructura origina una distribución adecuada de la informática y soporte a las operaciones de escritorio. Los límites de seguridad permiten el enfoque de que se enlacen dichas operaciones.
- Esta estructura probablemente podría correlacionarse de manera adecuada a todas las fortalezas y debilidades de la red.

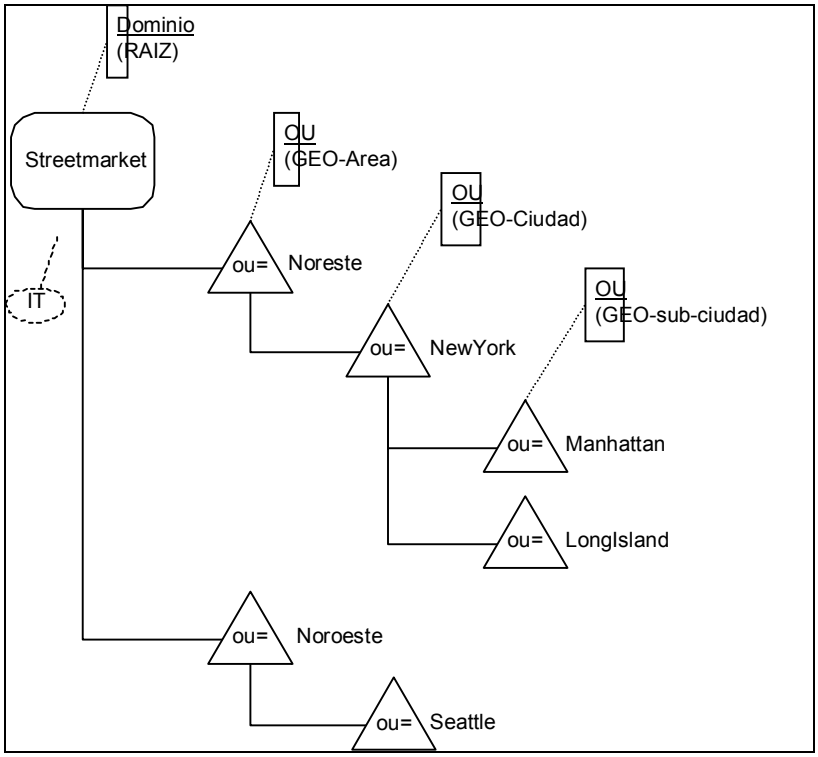
CONS

- La estructura organizacional no es contabilizada por lo que por lo general origina menos a la exploración intuitiva.
- Los límites divisionales pueden ser cruzados lo que haría más fácil obtener la implementación y administración.
- Esta estructura no soporta un traslado a una informática descentralizada basada en el departamento. Las entidades no divisionales deben ser administradas de manera central o colaborativa.

VARIACIONES

Existen muchas variaciones diferentes para el modelo geográfico básico. Estas pueden basarse en unidades de geografía o números de niveles de dominio.

El nivel de la estructura de dominio evidentemente puede reducirse o incrementarse. Al tratar con una distribución geográfica más pequeña, los dominios de primer nivel deben ser eliminados y reemplazados por Unidades organizacionales (OUs). Por ejemplo, tener operaciones Streetmarket únicamente basadas en los EUA, con ubicaciones que fueron bien conectadas, podría terminar con una estructura de directorio como la que aparece a continuación.



■ Figura 11: Geográfico

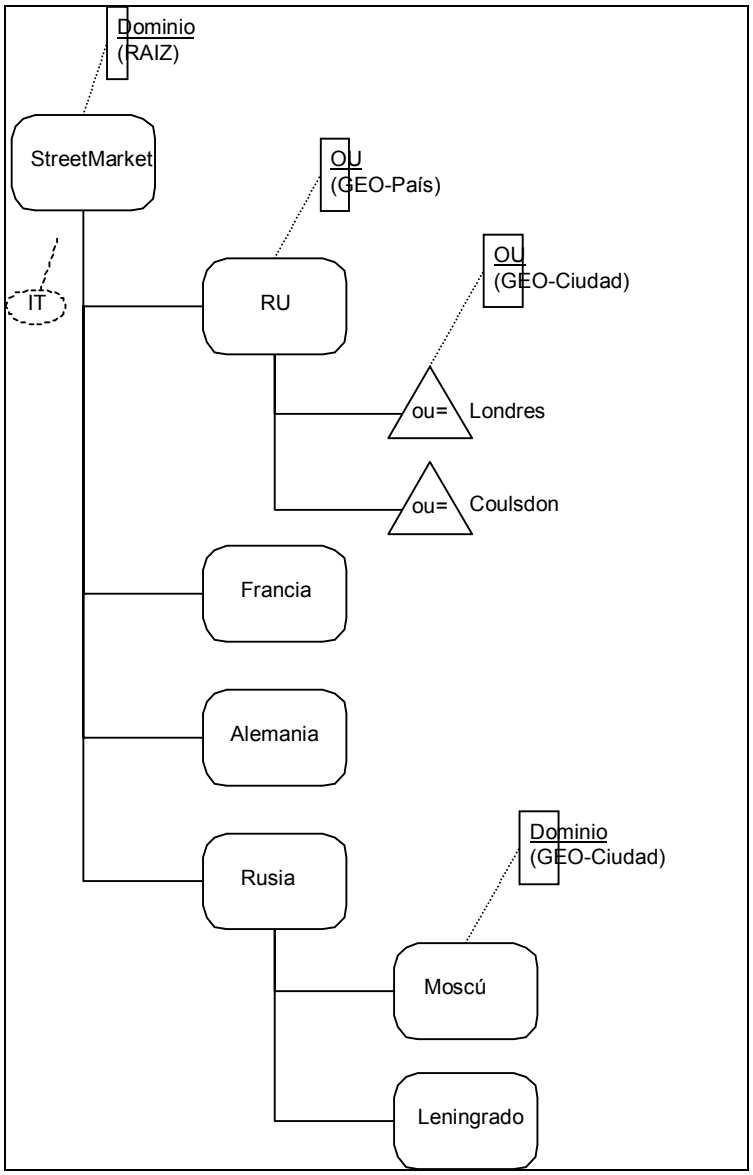
En la Figura 11, eliminamos el dominio de primer nivel todo junto ya que las dos áreas principales (noreste y noroeste) para nuestros fines, tienen una conectividad aceptable WAN. El ancho de banda de red podría haber sido un aspecto, esto podría haber sido establecido como dominios, los cuales podrían:

1. Aislar la duplicación total del Contexto de dominación de dominio (NC).
2. Habilitar las duplicaciones de los dominios para utilizar la compresión, más allá de la reducción de utilización de red.

Las OUs han sido establecidas para representar las áreas geográficas significativas. En una pequeña organización, también podrían caer las OUs basadas en el área y especificar simplemente la ciudad. Incluso en el ejemplo anterior, el país basado en la

estructura de unidad organizacional realmente no proporciona ningún beneficio aparte de su propia estructura.

En las organizaciones globales, es posible que sea necesario establecer más dominios o niveles más profundos de dominios. A partir de este punto, asumimos que Streetmarket tiene diferentes sucursales en diferentes países en Europa. Las conexiones de red entre estos países se basan en una ISDN de marcación en demanda. Las conexiones de red dentro de Rusia también están basadas en ISDN. Ahora nos vemos forzados a reensamblar una estructura como la siguiente.



■ Figura 12: Geográfico con varios dominios

El ejemplo de la Figura 12 muestra los preceptos siguientes.

1. Los países individuales dentro de Europa Occidental cuentan con redes sólidas dentro de los límites del país, permitiendo que multimaestra y duplicación se

presenten sin incurrir en cargos de línea adicionales.

2. La comunicación y duplicación entre los países se enfoca y controla reduciendo los cargos de comunicaciones relacionados con los enlaces ISDN de marcación en demanda.
3. Existe transporte poco confiable entre las oficinas rusas de Streetmarket, lo que hace que se origine otro nivel de dominios, basado en las ciudades. Al mejorar las condiciones de red, estos dominios pueden descargarse en OUs. Por ahora, los dominios separados permiten que la duplicación entre dominios para se lleve a cabo a través del transporte SMTP basado en los mensajes.

El uso de dominios para la duplicación de particiones deberá ser utilizado únicamente junto con funciones proporcionadas por los sitios. En breve, los sitios ofrecen una gran cantidad de control en la manera en la que se presenta la duplicación, mientras que los dominios determinan el enfoque actual de la duplicación. Este tema se analizará en las secciones siguientes.

Conclusión

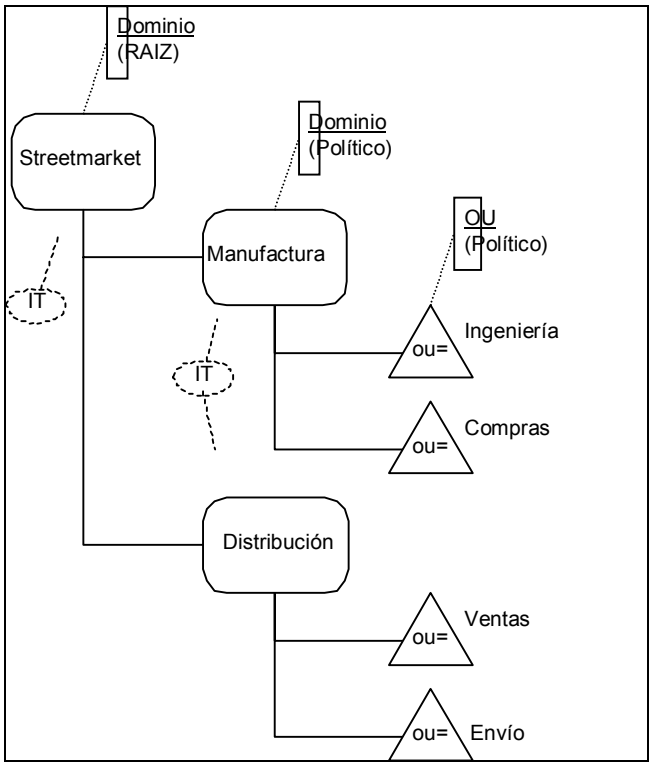
Basarse en la estructura Active Directory en las colecciones geográficas proporciona el tipo más estable de diseño ya que las reorganizaciones corporativas no afectan la estructura del dominio.

El establecimiento de dominio deberá basarse en el requerimiento para minimizar el tráfico de duplicación a través del enfoque y la duplicación comprimida; así como la capacidad de duplicación a través de SMTP.

Política

Hasta hace poco tiempo, basar una estructura de informática en límites políticos era muy popular. La estructura política/organizacional da origen por sí misma a un modelo de negocios, es fácil de diseñar y los aspectos incluyen el cruce de silos divisionales. La razón por la que este modelo cae dentro de la gracia corporativa, se debe a la tendencia relativamente reciente hacia las reorganizaciones corporativas frecuentes. La reestructura de los dominios de primer nivel en un directorio es un proceso difícil y tardado.

La organización de dominios y OUs que siguen el modelo político es estricta, con los dominios que representan divisiones administrativas y las OUs que originan la estructura y recursos departamentales.



■ Figura 13: Estructura de directorio político

Basarse en el dominio de primer nivel en las consideraciones políticas tales como la estructura organizacional da como resultado una estructura de directorio más reflexiva del modelo de negocios. Una base política trabaja adecuadamente en un ambiente de informática distribuido donde las funciones de informática se apegan muy de cerca a los silos divisionales.

En este modelo, se soportan los siguientes atributos:

- Informática centralizada, descentralizada o distribuida
- Red bien conectada
- Silos divisionales sólidos

En este modelo, los dominios deberán cumplir con dos requerimientos:

- Se requieren políticas de seguridad separadas para las divisiones.
- Se requiere separación administrativa distinta debido a la informática política o descentralizada.

Los dominios en este modelo nunca se establecen para enfocarse en la duplicación ya que la geografía no es una base para la estructura.

PROS

- El espacio de nombre interno se alinea con la estructura organizacional de la compañía, lo cual reduce los requerimientos de educación y confusión del usuario

final.

- El diseño de espacio de nombre DNS interno es más fácil de planear e implementar.
- Los silos divisionales son circundados y los límites no son cruzados. Esto incrementa la probabilidad de un registro e implementación exitoso.
- El árbol puede aceptar la expansión ya sea en la división o en la geografía.

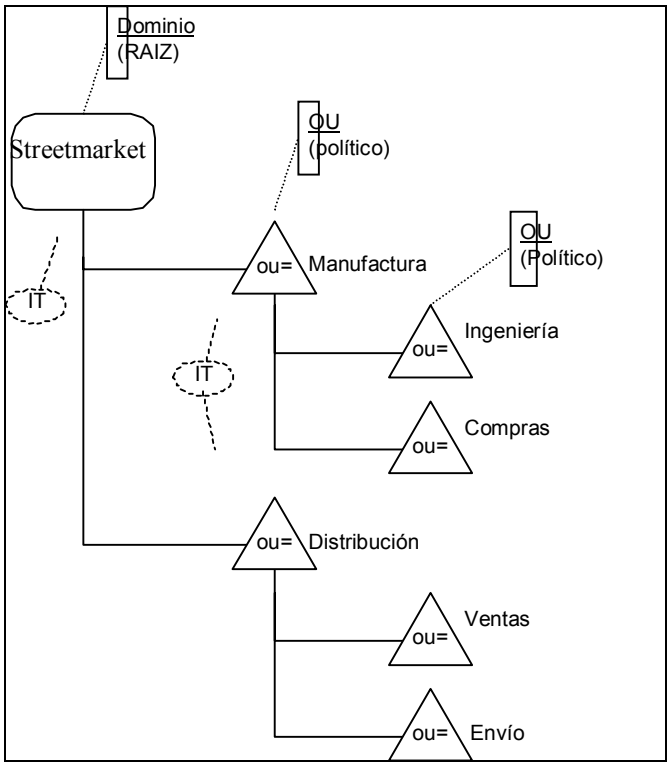
CONTRAS

- En la estructura de dominio no se hace un uso eficaz de la red para el enfoque de duplicación. Ambos dominios existen probablemente en las mismas ubicaciones.
- Una reorganización de las unidades de negocios podrá dar como resultado una iniciativa de informática mayor.

VARIACIONES

Al igual que el modelo geográfico, las variaciones en este diseño se refieren principalmente al número y ubicaciones de dominios. A diferencia del modelo geográfico, la creación de dominios será determinada por los requerimientos de seguridad y administración y no por una necesidad de controlar la duplicación ni de mejorar el rendimiento de la red.

En un ambiente de informática centralizado, la variación evidente es eliminar todo lo de los dominios de primer nivel, reemplazándolos con OUs.



- Figura 14: Estructura de directorio política

Reemplazar los dominios de primer nivel con OUs es posible debido a que existe un departamento de informática de control que puede mantener la raíz, y delegar la administración según sea necesario para los departamentos de informática de unidad de negocios. Esto también puede ser posible para implementar esta variación en un ambiente de informática distribuido así como para los departamentos de informática que no son autónomos.

Esta opción elimina el retroceso relacionado con la red asociado con la duplicación duplicada y proporciona un modelo administrativo eficiente.

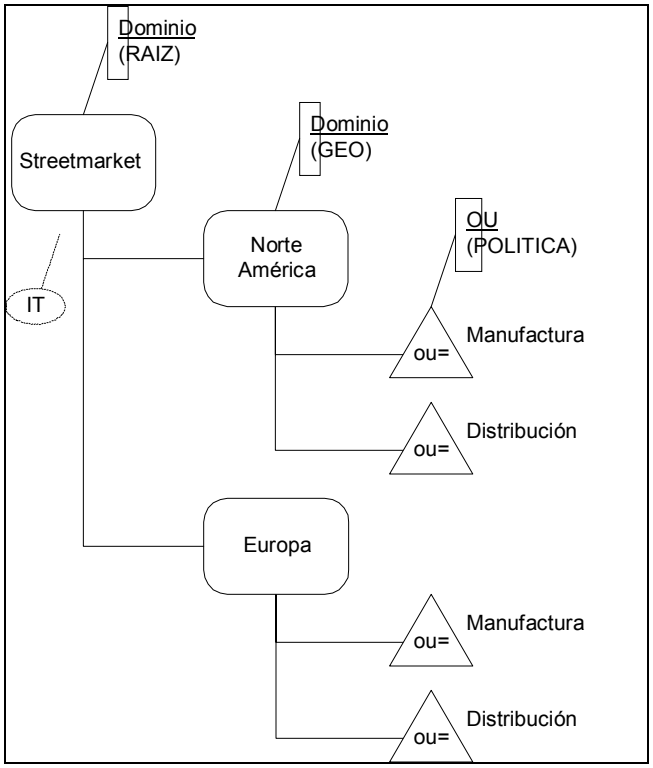
Una ventaja real que se obtiene al eliminar los dominios de segundo nivel es que se mantiene un solo espacio de nombre para la organización. Si el objetivo es la simplicidad de implementación y administración, permanezca con un dominio único, y haga que éste refleje a la empresa.

Es poco frecuente la justificación para crear una estructura de dominio profunda en este modelo, pero puede existir en compañías de retención y otras organizaciones distribuidas donde las compañías de operación autónoma existen dentro de las unidades de negocios. La sobrecarga administrativa en este tipo de modelo puede ser altamente preocupante y deberá evitarse de ser posible.

Geopolítica

El modelo de directorio geopolítico es quizás el más funcional. Como el nombre lo sugiere, el modelo geopolítico combina aspectos de los modelos geográficos y políticos en diversos niveles del directorio. Los niveles particulares en los que cada uno se aplica

podrían variar, pero por lo menos el primer nivel siempre se basa en la geografía, con los niveles subsecuentes basados en los factores políticos.



- Figura 15: Geopolítico

La estructura geopolítica ofrece los mejores atributos para los dos modelos analizados con anterioridad. La elasticidad se obtiene a través de niveles más altos de directorio basando la estructura en la geografía, mientras que la estructura organizacional se puede contabilizar para los niveles más bajos, proporcionando intuitividad y fácil delegación administrativa.

La justificación para este tipo de estructuras es relativamente directa. El impacto potencial más alto para una organización se encuentra en el dominio de primer nivel. Por ejemplo, al dar la estructura que se describe en la base política, surge una fuerza entre los dominios de primer nivel (manufactura y distribución) que podría afectar todos los aspectos de la infraestructura debido a que todos los objetos se encuentran en ella, o sirven para esos dos dominios. Sin embargo, en el caso que se describe en la estructura geopolítica, únicamente los dominios de segundo nivel o las OUs pueden ser afectadas por una reorganización. Entonces, en este punto, el impacto se limita únicamente a los dominios modificados directamente y a sus secundarios.

El objetivo de este principio no es limitar, sino minimizar el riesgo que conllevan las reorganizaciones. Existe un intercambio evidente entre la estabilidad del árbol y la contabilidad para realidades políticas para obtener un *buy-off*.

En este modelo, se soportan los siguientes atributos:

- Informática centralizada o distribuida

- Organización altamente distribuida
- Silos divisionales sólidos

La modelación de dominio se puede hacer con base en dos modelos (Geográfico o Político). Como se acostumbra, es mejor mantener el menor número de dominios.

Utilice dominios para distinguir las áreas geográficas cuando exista un requerimiento para minimizar el tráfico de duplicación a través de los vínculos WAN o si se requiere separación de seguridad entre los países etc.

Utilice los dominios por debajo del nivel geográfico para representar la estructura organizacional únicamente si la compañía se organiza de tal forma que los silos divisionales múltiples se basen en regiones geográficas específicas y dichas divisiones tengan que distinguirse y asegurar una separación entre sí.

PROS

- La estructura de árbol de directorio minimiza el impacto de reorganizaciones corporativas.
- El árbol puede aceptar la ampliación. Se pueden agregar fácilmente las colecciones geográficas o políticas adicionales o divisiones.
- Esta estructura da origen a una distribución de informática y soporta las operaciones de escritorio. Estas limitaciones de seguridad permiten el enfoque para que dichas operaciones se enlacen.
- Esta estructura probablemente correlaciona de manera adecuada las fortalezas y debilidades de la red.

CONTRAS

- No soporta fácilmente un traslado a una informática descentralizada debido al requerimiento de administrar entidades geográficas no unidas.
- La administración departamental puede ampliarse entre dominios múltiples, incrementando el exceso de trabajo administrativo. Observe que si la administración se basa en los factores políticos, las mismas entidades administrativas pueden ampliar los dos dominios.
- Esto puede originar un poco de administración colaborativa dentro de los dominios geográficos.

VARIACIONES

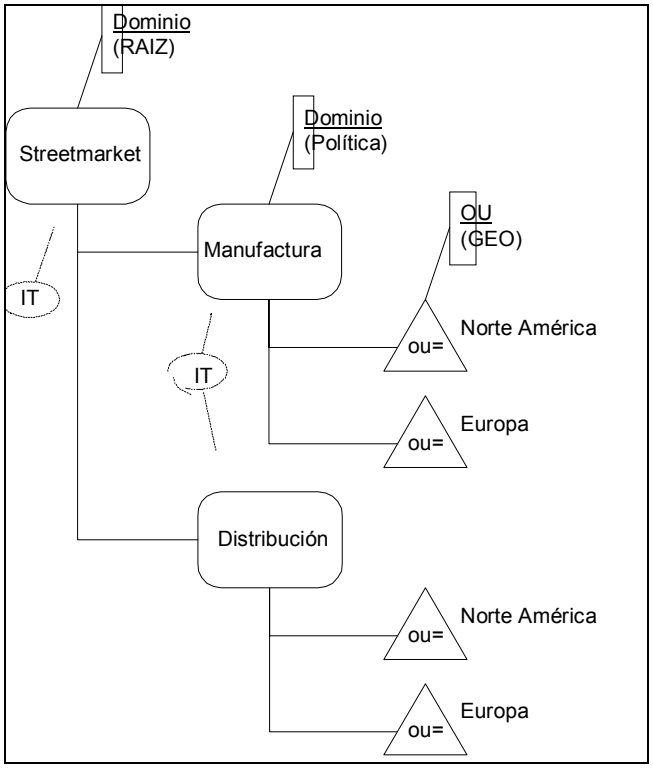
No existen realmente variaciones en este modelo, diferentes a la profundidad de los dominios contra OUs. Incluso en este caso, reemplazar los dominios de primer nivel por OUs podría dar como resultado OUs geográficas que en la mayoría de los casos no serían benéficas, sino que provocarían únicamente una estructura política.

Política geográfica

Asimismo, es posible aplicar una estructura geográfica por debajo de la estructura organizacional en el directorio. El modelo político geográfico contabiliza en primer lugar

la estructura organizacional y después se aplica a la estructura basada en las consideraciones geográficas.

Existen algunas justificaciones para la aplicación de esa estructura particular al directorio. Las grandes corporaciones multinacionales con frecuencia optan por este modelo ya que tienen la capacidad de proporcionar una separación entre las unidades de negocio primarias y dentro de dichas unidades de negocios, contabilizan la distribución geográfica. Frecuentemente, las grandes organizaciones mantienen las unidades de negocios que se encuentran en las grandes corporaciones. Estas subcorporaciones a su vez, son multinacionales y probablemente requerirán dominios para enfocar la duplicación del NC de Dominio.



■ Figura 16: Política geográfica

En caso de que fuera necesario delegar la administración o aplicar una política basada en las unidades organizacionales (OUs geográficas), esa estructura sería la adecuada. Sin embargo, si ese no fuera el caso, el nivel que representa las unidades geográficas podría ser arbitrario e inútil. Las separaciones geográficas dentro de este modelo se basan sólo en eso. Si estas separaciones fueran parte de la estructura organizacional de la compañía, actuarían realmente con base en las consideraciones políticas y no en las geográficas.

En este modelo, se soportan los siguientes atributos:

- Soporta todos los ambientes de informática
- Unidades de negocios distribuidas de manera física
- Silos políticos sólidos

Típico del enlace que representan, los dominios se pueden justificar ya sea para facilitar los requerimientos de seguridad (interdivisionales) o para limitar la duplicación para aceptar limitaciones de red físicas. El uso de este modelo particular con frecuencia combina las dos cosas, lo que da como resultado los dominios de nivel múltiple. También se puede utilizar un dominio único de raíz, asegurado por las OUs políticas y geográficas.

PROS

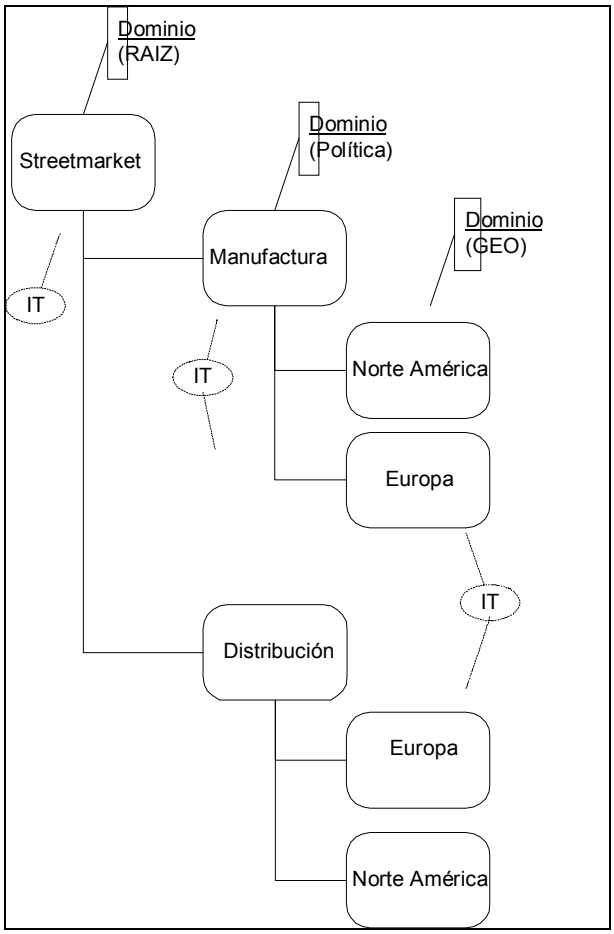
- Soporta organización de negocios de primer nivel.
- Soporta distribución de informática en todos los niveles.
- Proporciona seguridad absoluta entre las unidades de negocios mientras que sigue permitiendo la delegación o duplicación administrativa basada en la ubicación física.

CONTRAS

- La estructura de dominio no hace un uso eficaz de la red para la duplicación. Los dominios múltiples probablemente existen en las mismas ubicaciones, lo que da como resultado una superposición de la información duplicada.
- Una reorganización de las unidades de negocios podría provocar una iniciativa de informática principal.

VARIACIONES

La variación principal de este modelo, como se señala, es el uso de los dominios de nivel múltiple. Con frecuencia, las grandes compañías se ven forzadas a adentrarse en este tipo de ordenamiento debido a la solidez de los silos políticos, combinados con un ambiente distribuido, internacional.



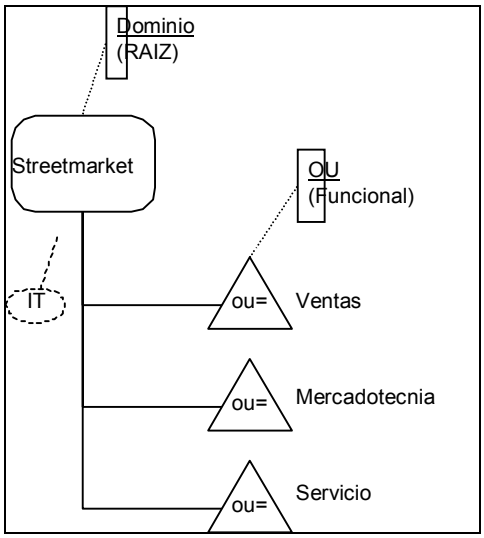
■ Figura 17: Político geográfico

En el ejemplo anterior, se cumplen diversas condiciones preliminares para Streetmarket – "el conglomerado internacional". En primer lugar, Streetmarket tiene unidades de negocios autónomas, lo que requiere una separación de seguridad distinta entre sí. En segundo lugar, Streetmarket puede necesitar ya sea una seguridad distinta entre países o una duplicación optimizada proporcionada por dominios separados.

Funcional

El modelo funcional asume que más allá de las demás consideraciones, el objetivo más importante de las comunicaciones internas es facilitar la colaboración. Un modelo funcional considera únicamente las funciones de negocios de una organización, sin observar las consideraciones políticas o geográficas.

Esto podría funcionar particularmente bien en pequeñas organizaciones, con informática centralizada. Unicamente es necesario un nivel de dominio en este modelo ya que la seguridad entre las unidades no es de consideración. El tema del modelo funcional es aquel de las comunicaciones colaborativas con consideraciones de objetivos de negocios únicamente. Esto requiere una reglamentación a nivel ejecutivo senior, ya que no se soportan los silos divisionales.



■ Figura 18: Funcional

El modelo funcional es completamente inmune a la reorganización corporativa debido a la diversificación para todos los atributos excepto para operaciones de negocios funcionales. Por lo tanto, cualquier aspecto corto de una realineación completa de los negocios principales puede ser absorbido en la estructura. Una organización de consultoría relativamente pequeña podría ser un buen prospecto para este tipo de modelo.

No puede haber más de un nivel de dominio dentro del modelo funcional, ya que no hay bases para su creación. Esto hace que la aplicación de este modelo se limite al enfoque a pequeñas organizaciones, o compañías con distribución geográfica limitada.

PROS

- Proporciona una plataforma para la comunicación corporativa debido a la agrupación de roles similares dentro de las OUs.
- Es intuitiva para los usuarios.

CONTRAS

- Las OUs de segundo o tercer nivel pueden ser necesarias para ubicar la administración de recursos de red.

Revisión

Esta sección le presentó un número de diseños de espacio de nombres diferentes basados en diferentes modelos.

- Político
- Geográfico
- Geopolítico
- Político geográfico

- Funcional

Mientras que cada diseño tiene sus propias fortalezas y debilidades inherentes, el punto es tomar en cuenta que el diseño de espacio de nombre Active Directory se puede basar en la estructura organizacional y reglas de negocios, y como tal, se puede adaptar a diferentes modelos.

Plot Thickens: Consideraciones para sitios

Un *sitio* es una o más subredes IP bien conectadas. Como regla general, un sitio puede ser la causa de que las áreas conectadas utilicen tecnologías LAN. Los sitios consisten únicamente en objetos de servidor y en objetos de configuración que se utilizan para la duplicación.

Lamentablemente, no existe una regla general para determinar el enfoque correcto de los sitios, sino a través del entendimiento sobre la manera en que Active Directory utiliza la información del sitio para que pueda tomar una decisión bien informada sobre cómo implementarlos. Active Directory utiliza los sitios en las siguientes cuatro maneras:

- Cuando un cliente solicita una conexión a un Controlador de dominio (por ejemplo para conexión), el sitio habilita al cliente para conectarse a un Controlador de dominio dentro del mismo sitio siempre que sea posible. Esto reduce la latencia y conserva el ancho de banda de red.
- Los sitios definen la topología de duplicación para los controladores de dominio que forman parte de ese sitio. El Verificador de consistencia de conocimiento (KCC) también utiliza la información contenida dentro del sitio para agregarla de manera automática a servidores adicionales a la topología de duplicación.
- Los mensajes de duplicación entre los DCs en un sitio no están comprimidos, por lo que utilizan menos ciclos CPU en los DCs. Los mensajes de duplicación entre DCs en diferentes sitios están comprimidos, de manera que utilizan menos ancho de banda de red.
- La duplicación entre los DCs en un sitio se origina por la llegada de actualizaciones, reducción de la latencia de duplicación dentro de un sitio. La duplicación entre los DCs en diferentes sitios se realiza en un programa, conservando el ancho de banda de red. La compresión en estos casos puede ser tan grande como de 10 a 1.

Los sitios no están vinculados de ninguna manera al espacio de nombre de Active Directory. El nombre de un objeto de directorio no refleja el sitio o sitios en los que se almacena el objeto. Un sitio puede contener DCs desde diversos dominios y los DCs de un dominio pueden representar varios sitios. (En los sitios de Exchange Directory Service están vinculados con el espacio de nombre).

Ubicación del controlador de dominio

Cuando un usuario se conecte, la estación de trabajo tratará de ubicar un controlador de dominio en su sitio local. Cuando no estén disponibles los controladores de dominio en el sitio, la estación de trabajo utilizará otro controlador de dominio en la red.

La proximidad de los controladores de dominio para los clientes en la red tendrá un impacto evidente durante la autenticación.

Determinación sobre dónde colocar los controladores de dominio y catálogos globales

Al planear la ubicación del controlador de dominio para los dominios, hay que tomar en cuenta tener por lo menos un controlador de dominio por sitio. Esta teoría se basa en un

modelo “consulta del 99 por ciento y actualización de 1 por ciento”. Esto significa que el 99 por ciento de su tráfico de red Active Directory estará relacionado con la consulta como usuarios, administradores e información de solicitud de aplicaciones sobre otros objetos en la red y autenticación. Las actualizaciones al directorio, las cuales utilizan el tráfico de duplicación de directorio, se presentarán con menor frecuencia.

Al colocar un controlador de dominio en cada sitio, todos los usuarios tendrán una computadora local que puede dar servicio a las solicitudes de consulta sin requerir tráfico de enlace lento. Puede configurar los controladores de dominio en sitios más pequeños a fin de recibir las actualizaciones de duplicación de directorio únicamente en horas fuera de trabajo, a fin de optimizar el flujo de tráfico.

Considere las siguientes directrices para colocar los controladores de dominio en su empresa:

- Un controlador de dominio debe poder responder a las solicitudes del cliente a tiempo.
- El mejor rendimiento de consultas se presenta cuando se coloca un controlador de dominio (en un sitio pequeño) con un servidor de catálogo global, permitiendo que el servidor llene por completo las consultas sobre los objetos en todos los dominios de la red).

Los servidores de Catálogo global son controladores de dominio que también mantienen información que se utiliza con frecuencia desde otros dominios. Esta función puede parecer trivial, pero cada usuario que se conecta es procesado por un servidor de Catálogo global para la membresía de Grupo universal. Considere estos lineamientos para colocar los servidores del Catálogo global en su empresa:

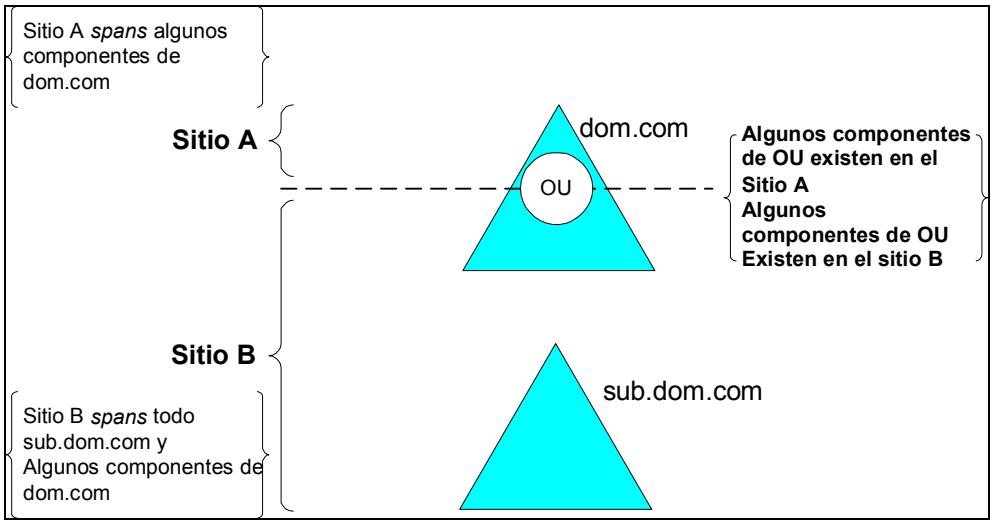
- Un servidor de Catálogo global debe tener la capacidad de mantener todos los objetos desde todos los dominios en el campo.
- Un servidor de Catálogo global debe poder responder a las consultas de cliente y a las solicitudes de autenticación de manera oportuna.

La disponibilidad es la clave para ubicar los Controladores de dominio y servidores de Catálogo global. Mientras se puede ubicar el servidor de Catálogo global en la empresa, se da servicio a varios sitios, por lo menos un controlador de dominio deberá colocarse en cada ubicación de sitio. El número de servidores de Catálogo global también tendrá un impacto en la cantidad de información duplicada a través del directorio.

Limitantes de sitio

Existen dos conceptos importantes relacionados con estos sitios los cuales son:

- Un sitio puede ampliarse más que un dominio. Ya que un sitio es simplemente una recolección de objetos que existen en ubicaciones físicas, la distribución lógica de objetos puede incluir tantos como dominios parciales sean posibles para estar presentes dentro de la definición de sitio.
- Asimismo, múltiples sitios pueden ampliar dominios e incluso unidades organizacionales. Esto es particularmente interesante al considerar la manera en que la política de grupo afectará los objetos dentro de un dominio particular. Un beneficio es que el sitio no puede ampliar una computadora actual.



■ Figura 19

En la figura anterior, el Sitio A se define de manera tal que contiene únicamente la mitad de los componentes del dominio dom.com. Sin embargo, el Sitio B, contiene todos los componentes de sub.dom.com así como algunos objetos dentro del dominio dom.com. Una observación interesante es que algunos objetos dentro de la OU también se dividen entre los sitios.

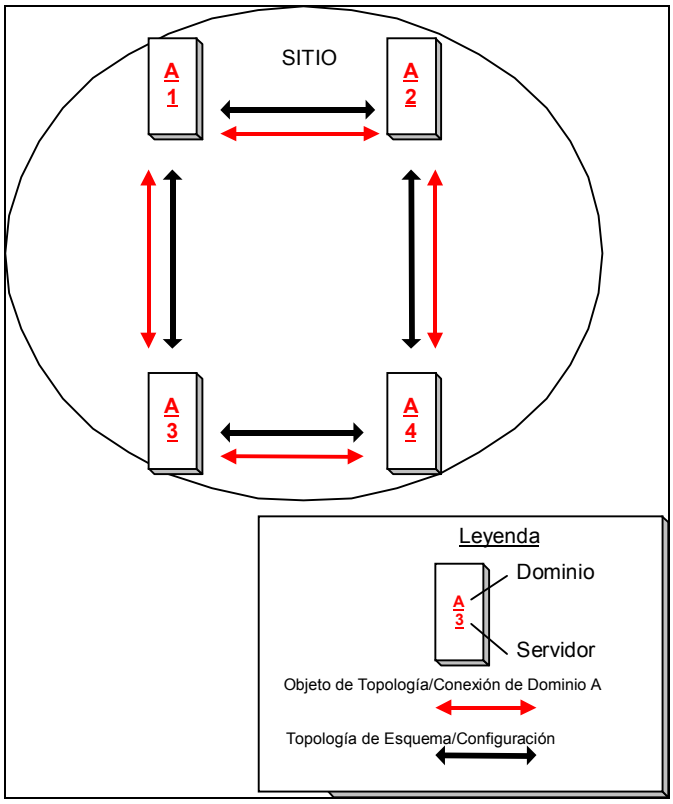
Duplicación de sitio

Para tener una comprensión clara de la duplicación entre sitios, también se debe entender que dichas partes del directorio son duplicadas. Esos tres elementos se duplican dentro de un sitio:

- Contexto de denominación de dominio
- Contexto de denominación de configuración
- Contexto de denominación de esquema

Los contextos de denominación de Configuración y Esquema comparten la misma topología de duplicación dentro de un sitio, mientras que el contexto de denominación de Dominio mantiene una topología separada para cada dominio dentro de un sitio.

Esto podría ser confuso pero en realidad es muy simple. Cada servidor que se une a un sitio se inserta automáticamente dentro de las topologías de duplicación de Configuración/Esquema y Dominio. Al trabajar con los servidores en el mismo dominio, las topologías de duplicación son idénticas.

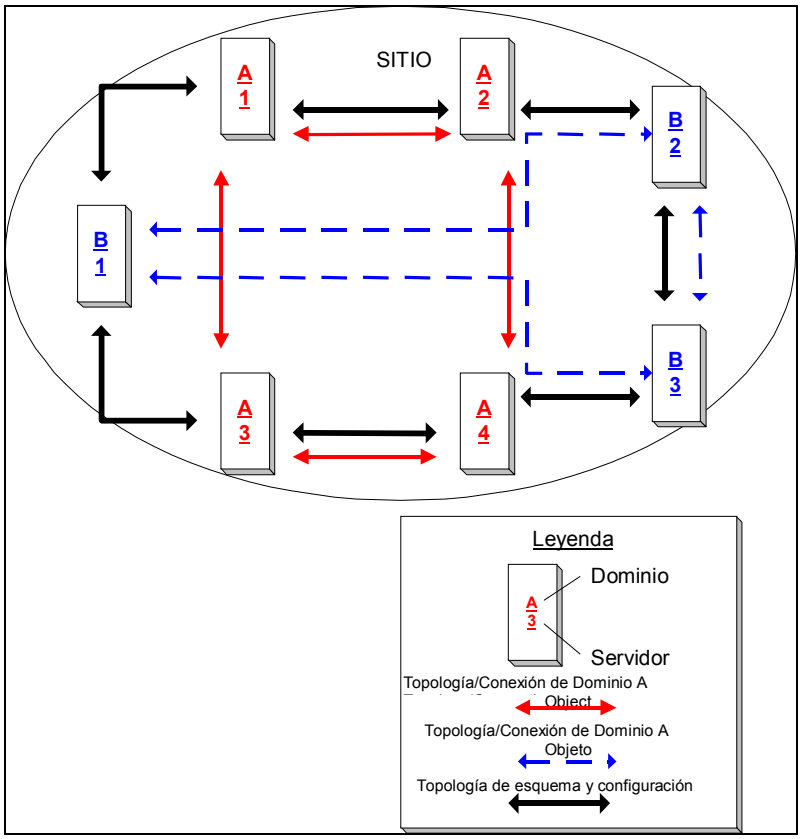


■ Figura 20: Duplicación de sitio de dominio único

A medida que cada controlador de dominio adicional se agrega al sitio, la topología cambiará para albergar al nuevo miembro de sitio.

Los controladores de dominio desde dominios separados también se insertarán dentro de las topologías de duplicación, únicamente de dos maneras. La inserción dentro de la topología de Esquema/Configuración se presentará en un modo normal. El servidor también se insertará dentro de la topología de contexto de denominación de Dominio del sitio.

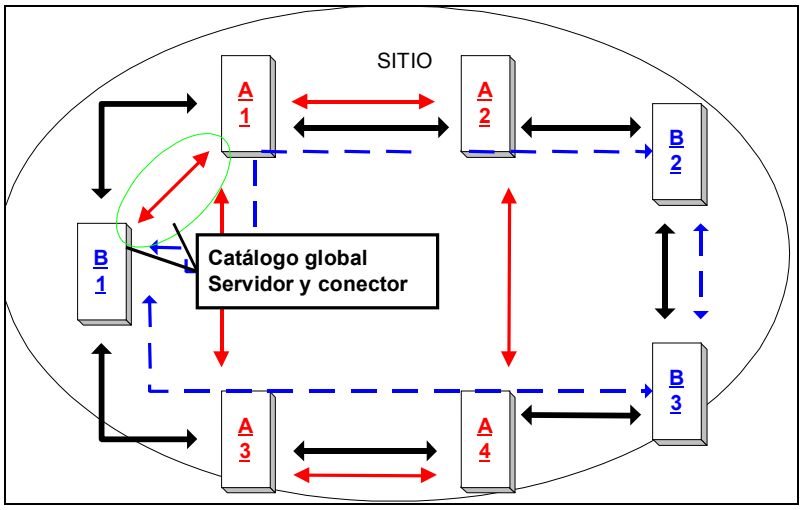
La figura siguiente muestra un sitio con dos dominios: A y B. Observe que a medida que los DCs se agregan a la topología de sitio, se forman dos topologías distintas, una para la Configuración/Esquema y otra para el contexto de denominación de Dominio.



■ Figura 21: Duplicación de sitio – Dominios múltiples

El Esquema/Configuración (común para un campo) se duplica sin considerar la membresía de dominio, mientras que cada uno de los dominios mantiene una topología distinta.

Entonces surge la duda sobre la manera en que los dominios se dan cuenta del contexto de denominación de Dominio. Esto se puede llevar a cabo a través de los Controladores de dominio que sirven como servidores de Catálogo global – un GC desde cada dominio, que duplicación con un DC desde otro dominio. Unicamente necesita un conector de duplicación de contexto de denominación de Dominio ya que se duplica globalmente el Esquema/Configuración.



■ Figura 22: Duplicación de Catálogo global

En este caso, el dominio B ha introducido un GC en el sitio. Además de sus deberes de duplicación normales, el GC (B1) ha creado un objeto de conexión con el controlador de dominio A1 del dominio A. El GC surgirá como una duplicación parcial del NC del Dominio A que se incluirá en el Catálogo global.

A medida que se creen sitios adicionales, ajustarán constantemente la topología de duplicación para albergar nuevos controladores de dominio. La duplicación entre los sitios se hace utilizando los conectores de sitio, los cuales se analizan en la sección siguiente.

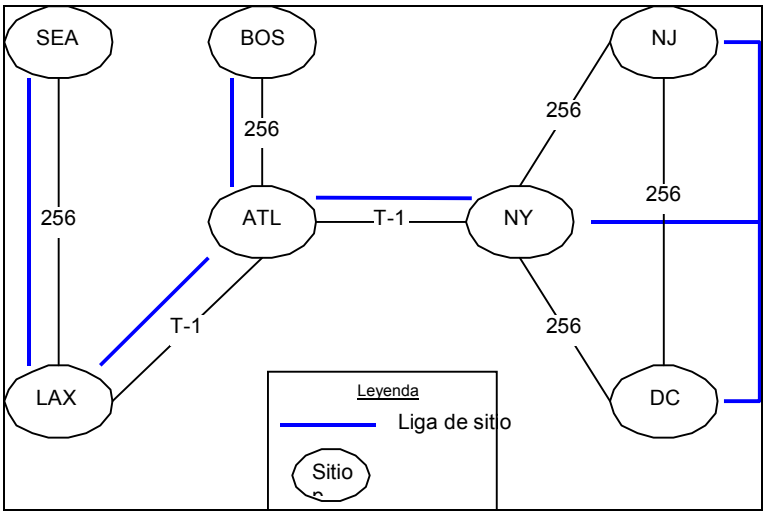
El proceso de duplicación entre sitios es totalmente automático y siempre utiliza DS-RPC para pasar los cambios de directorio. Sigue siendo de utilidad comprender claramente la duplicación entre sitios en caso de que sean necesarios ajustes manuales a la topología.

Duplicación entre sitios

Los sitios no afectan lo que duplicará la información, sino cómo se duplica la información. La duplicación entre sitios se lleva a cabo normalmente utilizando DS-RPC en un conector lógico definido por un *enlace de sitio*. De manera opcional, la duplicación entre sitios puede utilizar mensajes SMTP mientras que dichos sitios no se encuentren en el mismo dominio.

Para que ocurra la duplicación Active Directory, las rutas de duplicación entre los sitios necesitan vincularse manualmente mediante la definición de los vínculos de sitio. Un vínculo de sitio define una conexión lógica entre dos o más sitios. Una vez definida, los objetos de conexión se configuran de manera automática.

Los enlaces de sitio pueden representar una recopilación de conexiones de red similares o un enlace WAN único. Un enlace de sitio puede contener varios sitios.



■ Figura 23: Red, Sitios y Vínculos de sitio

En el ejemplo anterior, los sitios NY, NJ y DC se conectan a través de una malla de vínculos WAN de 256k. Todos han sido incluidos bajo un vínculo de sitio único, lo que significa que la comunicación entre los tres se hace con base en *peer*. Los sitios restantes han sido conectados, siguiendo la correlación de red y utilizando vínculos de sitios separados para cada conexión.

Vínculos de sitio

Un *objeto de vínculo de sitio* representa un grupo de sitios que se comunican a un costo uniforme a través de un transporte entre sitios. Para el transporte IP, un vínculo de sitio típico conecta justamente dos sitios y corresponde a un vínculo WAN real. Un sitio IP enlaza la conexión a más de dos sitios que debe corresponder a la parte principal ATM que conecta dos *clusters* de estructuras en un gran campus, o diversas oficinas en una gran área metropolitana conectada a través de líneas rentadas y enrutadores IP.

Se puede crear un objeto de vínculo de sitio para un transporte entre sitios específico (típicamente transporte IP) especificando:

- El costo para la ruta
- Dos o más sitios
- Un programa

El programa determina los períodos durante los cuales está disponible el vínculo. Esto puede ser de utilidad para la conexión de sitios que utilizan conexiones de alto costo, como son las conexiones de marcación.

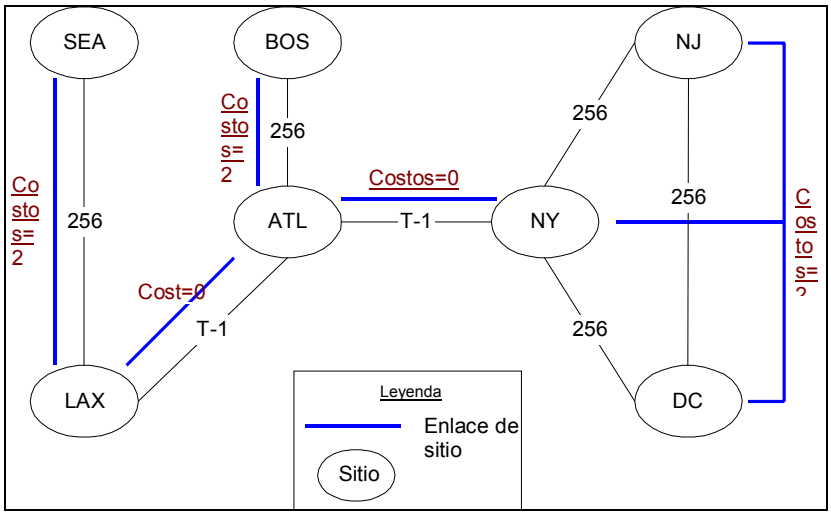
Un sitio se puede conectar a otros sitios a través de cualquier número de objetos de enlace de sitios. Cada sitio en un directorio de sitios múltiples se puede conectar por lo menos a un solo enlace. De otra manera, no podría duplicarse con los DCs en cualquier otro sitio, por lo que se desconectaría el directorio. Por lo tanto, se debe configurar por lo menos un vínculo en un directorio de sitios múltiples.

Factor de costos

Los enlaces de sitio tienen varios costos asociados, los cuales afectan el enrutamiento de

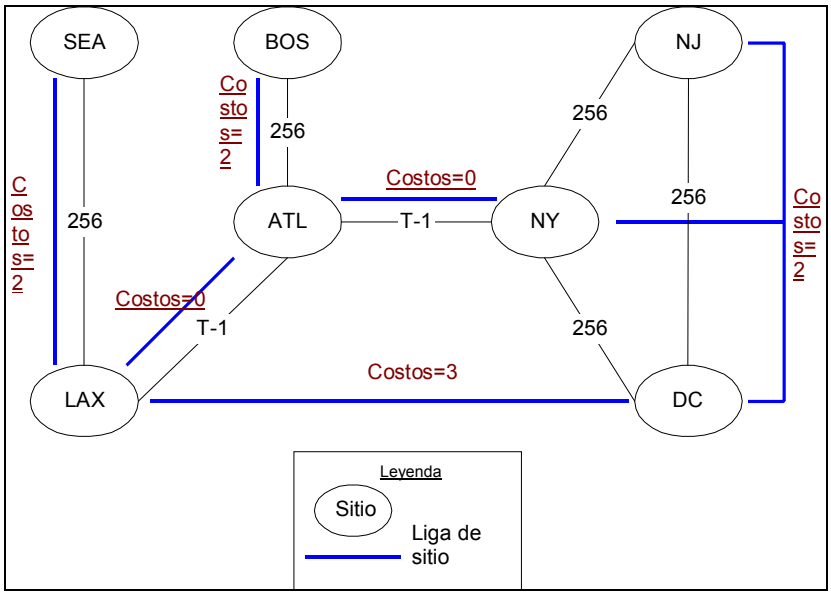
mensajes entre sitios. Los costos se asignan automáticamente, pero se pueden cambiar de manera manual a fin de reflejar los atributos de las rutas de red que siguen. Por lo regular, los costos para los vínculos de sitio se relacionarán con las velocidades del vínculo WAN. Los números de costos más altos representan rutas de mensaje más costosas.

Por ejemplo, si se establece NY-NJ-DC de objeto de vínculo de sitio que conecta los tres sitios — Nueva York, New Jersey y Washington, DC — con costo 20, se estará diciendo que un mensaje de duplicación se puede enviar entre todos los pares de sitios (NY a NJ, NY a DC, NJ a NY, NJ a DC, DC a NY, DC a NJ) con costo 20.



■ Figura 24: Enlaces de sitio

Los costos de enlace de sitios tienen un impacto en el enrutamiento de mensajes entre los sitios. Por ejemplo, en la Figura 16 siguiente, se envía un mensaje desde un sitio LAX a DC lo que podría ser una ruta menos costosa, en este caso LAX-ATL-NY-DC las cuales tienen un costo de dos, incluso aunque el sitio DC esté únicamente a un paso.



■ Figura 25: Enrutamiento de vínculo de sitio

Como se muestra en la figura anterior, los costos de vínculo de sitio pueden tener mayor impacto en las rutas de duplicación. Un buen método para establecer los costos de sitio, es relacionar un costo con un vínculo o condición de red. Por ejemplo, T-1 puede tener un costo de 15, mientras que un enlace de 512k puede tener un costo asociado de 25 etc. Establecer los estándares para los costos de vínculo de sitio implicará cierto trabajo de investigación sobre el diseño de la topología del sitio.

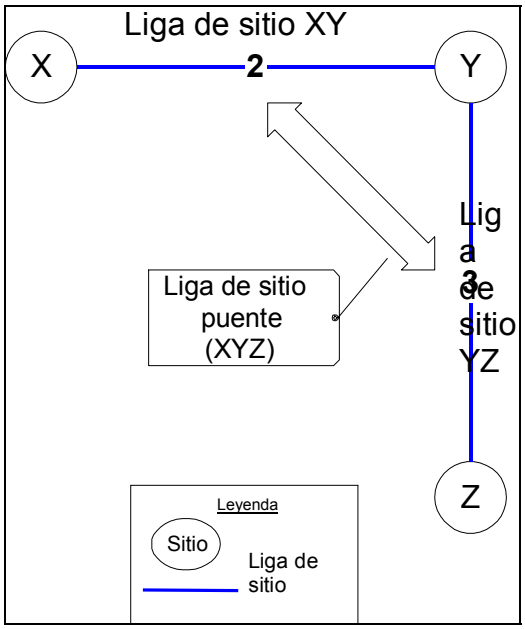
Puentes de vínculos de sitio

Un objeto de *puente de vínculo de sitio* representa un grupo de vínculos de sitio, mediante los cuales los sitios se pueden comunicar a través de algún transporte. Por lo regular, un puente de vínculo de sitio corresponde a un enrutador (o a un grupo de enrutadores) en una red IP.

Los puentes de enlace de sitio proporcionan transitividad entre los vínculos de sitio y representan el objeto de conexión real. Se puede crear un objeto de puente de vínculo de sitio para un transporte entre sitios especificando:

- Dos o más vínculos de sitio para el transporte entre sitios especificado.
- Para entender lo que significa un puente de vínculo de sitio, considere este ejemplo:
- El vínculo XY de sitio se conecta a los sitios X e Y a través de IP con costo 3
- El vínculo YZ de sitio se conecta a los sitios Y y Z a través de IP con costo 4
- El puente de vínculo de sitio XYZ conecta XY e YZ.

El puente de vínculo de sitio XYZ implica que un mensaje IP se puede enviar desde un sitio X a un sitio Z con costos de 3+4 = 7. Esto es todo lo que el puente hace en este ejemplo simple.

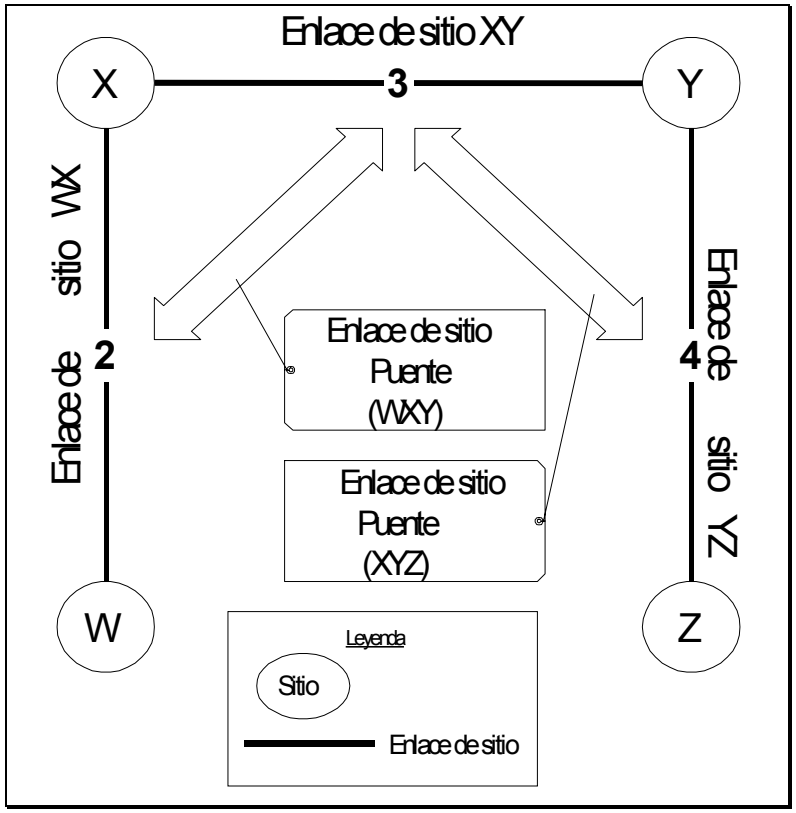


■ Figura 26: Puente de vínculo de sitio

Cada vínculo de sitio en un puente deberá tener un sitio en común con otro vínculo de sitio en el puente. De otra manera el puente no podría calcular los costos de los sitios en el vínculo L para los sitios en otros vínculos del puente.

Los puentes de vínculo de sitio separados, incluso para el mismo transporte, son independientes. Agregue los siguientes objetos para el ejemplo anterior:

- Vínculo de sitio WX que conecta los sitios W y X a través de IP con costo 2
- Puente de vínculo de sitio WXY que conecta WX y XY.



- Figura 27: Puentes de vínculo de sitio múltiples

La presencia de este puente adicional significa que un mensaje IP se puede enviar desde W hasta Y con costos de 2+3 = 5. Pero esto *no* implica que un mensaje IP se puede enviar desde un sitio W a un sitio Z con costos de 2+3+4 = 9. En casi todos los casos se tendrá que utilizar un puente de vínculo de sitio único para todo el modelo de red IP.

Cualquier red que se pueda describir mediante la combinación de vínculos de sitio y puentes de vínculos de sitio, también puede describirse únicamente por los vínculos de sitio. Al utilizar los puentes, su descripción de red es mucho más pequeña y más fácil de mantener, ya que no necesita un vínculo de sitio para describir cada ruta posible entre pares de sitios.

Creación de topología

Dependiendo del nivel de control que se requiera, las topologías de sitio son completamente configurables desde las que son totalmente automáticas hasta las que son totalmente manuales.

Si no se ha realizado un trabajo adecuado sobre el cálculo de costos para sus vínculos de sitio, simplemente puede seleccionar un puente para todos los sitios desde las configuraciones NTDS del nivel de sitio, y permitir que KCC determine la mejor ruta para el enrutamiento del mensaje.

De manera alterna, se puede tener control total sobre el proceso apagando la generación KCC y estableciendo de manera manual cada puente de vínculo de sitio. Aunque en este caso, el administrador es el responsable absoluto de establecer y mantener los puentes

de vínculo de sitio que, para grandes organizaciones, puede ser una tarea monumental.

También se puede utilizar una combinación de configuraciones automáticas y manuales. Esto permite que un administrador tenga influencia en la duplicación sin tener que configurar de manera manual toda la topología. Este método permite que KCC genere de manera automática todos los puentes de vínculo de sitio que se puedan modificar manualmente según sea necesario.

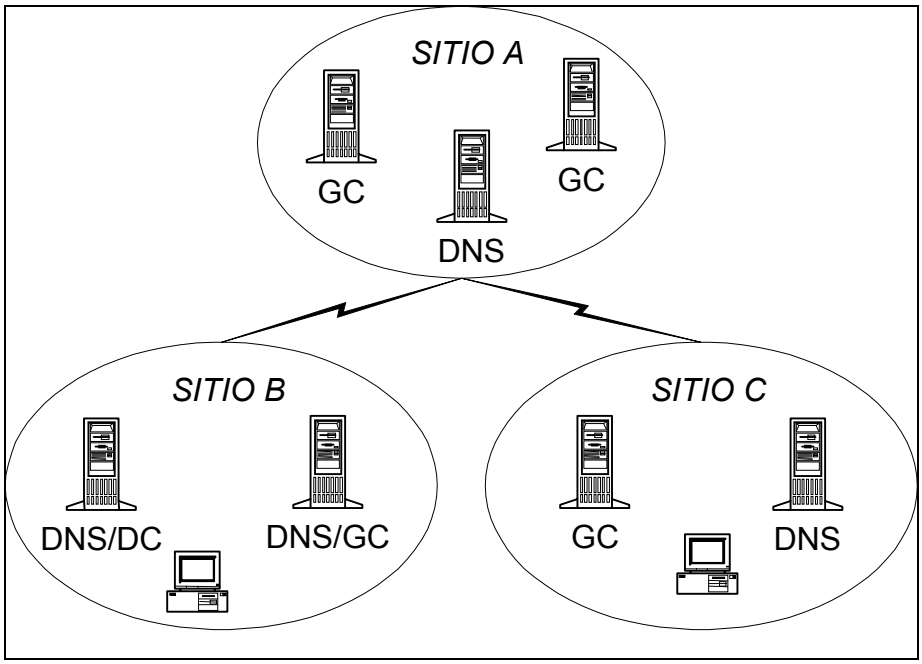
Ubicación de servicios

El servidor de Catálogo global mantiene una duplicación parcial de sólo lectura de la información que se accesa con frecuencia desde cada dominio en el campo. También mantiene una duplicación de lectura/escritura de esta información para su propio dominio. Lo que es más importante, cada autenticación de objeto para Active Directory debe referirse al servidor de Catálogo global (GC). Esto significa que cada usuario que se conecta, y cada computadora que se inicia, deberá hacer referencia al GC para membresía en grupos universales.

Esto no significa necesariamente que cada Controlador de dominio deberá etiquetarse como un GC. Mientras que es verdad que GC desempeña un rol importante en el proceso de autenticación, también es verdad que mucho menos tráfico y procesamiento de red se relaciona con el GC más que con un Controlador de dominio. Esto significa que menos GCs pueden servir a más clientes. Es realmente el DC de autenticación (no el cliente) el que contacta un GC para una membresía de Grupo universal.

Como un lineamiento, cada sitio debe tener por lo menos un servidor de Catálogo global. Sin embargo, si se conectan bien varios sitios mediante vínculos de red confiables, los servidores de Catálogo global pueden dar servicio a más de un sitio.

Como ya se analizó anteriormente, es totalmente posible combinar los roles de servidor y colocación a fin de lograr el resultado deseado de proporcionar servicios específicos del sitio confiables y disponibles.



- Figura 28

Sitio A: Se configura con dos servidores de Catálogo global y un servidor DNS único. El Sitio A proporciona excelente disponibilidad del GC. En este caso cuando el servidor DNS único no está disponible, un servidor DNS puede ser un sitio B o un sitio C que puede ser utilizado.

Sitio B: Mantiene dos servidores para proporcionar ambos servicios DNS Asimismo, uno de los controladores de dominio actúa como un servidor de Catálogo global para el sitio. Una vez más, los servidores de Catálogo global están disponibles en otros sitios si no están disponible el GC local.

Sitio C: Contiene un GC único y un DC único. En caso de no estar disponibles uno o el otro, los clientes podrían utilizar los servicios del sitio A.

Un caso considerado menos que óptimo podría ser el uso de un servidor único que proporcione servicios GC y DNS. Ese servidor podría no estar disponible, y todos los servicios podrían no tener que ser proporcionados más allá de los límites del sitio.

En cualquier caso, es importante que el servidor DNS y el servidor de Catálogo global estén disponibles para los clientes de un sitio. En caso de que no esté disponible el servidor de Catálogo global, el cliente no podrá conectarse a la red y no podrá acceder a muchos servicios.

Enfoques de sitio

Los tamaños reales de los sitios variarán en gran medida dependiendo de:

- El tamaño de la organización
- El número de clientes y su distribución física
- La cantidad de datos que van a ser duplicados

En las grandes organizaciones con varios cientos de ubicaciones, puede no ser factible establecer un sitio para cada segmento de red o red de campus. En estos casos, será necesario enfocar los sitios lo más grande que sea posible para reducir la cantidad de administración y manejo que se requiere. En este ejemplo, los sitios pueden ampliarse a diversas ubicaciones físicas conectadas a través de vínculos WAN rápidos y confiables (T-1).

Los sitios se pueden utilizar para incrementar el rendimiento de conexión del cliente. Si el cliente se conecta y se tarda demasiado debido al gran número de clientes de un sitio, o la autenticación de clientes es muy lenta, entonces la mejor opción sería reducir el tamaño del sitio o agregar otro.

Determinar el enfoque de los sitios no siempre es un procedimiento directo. Los sitios se definen simplemente como una recolección de subredes IP que están bien conectadas. Sin embargo, ya que se definirán tanto las subredes IP como las subredes que serán incluidas en un sitio, las opciones pueden variar.

En pequeñas organizaciones, las definiciones de sitio serán fáciles y estarán basadas en la conectividad de velocidad LAN. En casos directos, la definición de topología de duplicación también es simple y puede ser realizada por el KCC.

En grandes organizaciones con muchas ubicaciones, definir los límites de sitios será más difícil debido a la variación de las condiciones de ancho de banda de los vínculos de red, además de tratar de minimizar la sobrecarga administrativa relacionada con la configuración y administración de conexiones entre los sitios.

En una situación donde pueden existir varios sitios, también se deberá tener una buena idea sobre la manera en que se verá la topología de duplicación entre los sitios. La duplicación de directorio se presenta dentro de un sitio y entre sitios.

Active Directory ya cuenta con algunas funciones integradas las cuales ayudan a disminuir el tráfico de duplicación:

- Duplicación diferencial: Active Directory duplica únicamente cambios a un objeto, en lugar de hacerlo con el objeto mismo. Por ejemplo, si se modifica el número telefónico de un usuario, únicamente se duplica el número telefónico en vez de la información del usuario.
- Duplicación programada: La duplicación, tanto dentro de un sitio, como entre sitios se puede programar y configurar. De esta manera, la duplicación puede programarse durante horas de red no pico.
- Compresión: La duplicación RPC entre sitios utilizará la compresión. (Esto es aplicable únicamente entre dominios diferentes).
- Enfoque de duplicación: La cantidad de información que se duplica entre los dominios es menor a la cantidad de información que se duplica dentro de un dominio.
- Topologías configurables: El orden en que los servidores y sitios se duplican es completamente configurable, al igual que las veces que lo hacen, permitiendo que la duplicación (entre sitios) sea programada y la duplicación dentro de un sitio sea regida.

En diversas circunstancias, los límites de sitio se pueden basar en los límites de vínculos

de red de 10 megabits o más. Esto no quiere decir que los límites de sitio no pueden ampliar los vínculos más lentos. El número de variables como el ancho de banda disponible, topología de red, latencia de red y tráfico de cliente y duplicación prohiben el establecimiento de cualquier tramo de red máximo para los sitios. Ya que la topología de sitio se duplica por sí misma, y que los sitios están, en su mayoría, interrelacionados entre sí, planee su topología de sitio de manera adecuada y establezca el plan basándose en cálculos de tráfico futuros y no actuales.

Revisión

En esta sección, analizamos los sitios y duplicación. De manera específica, definimos los sitios y enlaces de sitio y puentes de vínculos de sitio y se analizó la duplicación dentro y entre sitios. Más allá de entender esas definiciones, es necesario comprender la manera en que Active Directory utiliza la información de sitios. De esta manera se pueden tomar buenas decisiones sobre cómo implementar sitios en su empresa.

Un sitio es una o más subredes IP bien conectadas. Los vínculos de sitio proporcionan vínculos entre los sitios y habilitan los costos y programación. Los puentes de vínculo de sitio proporcionan vínculos transitivos entre los vínculos de sitio. La duplicación es el proceso mediante el cual se propaga la información Active Directory a través de la empresa. Definir un sitio como un grupo de subredes permite configurar rápida y fácilmente el acceso y topología de duplicación de Active Directory para aprovechar al máximo la red física.

Seguridad

Implementación de seguridad, ya sea para una empresa, dominio o una sola computadora, significa buscar un balance entre las fuerzas de oposición fundamentales, dando a conocer la información de la manera más fácil posible al mayor número de usuarios y protegiendo la información importante del acceso no autorizado.

Encontrar el balance adecuado requiere planeación:

- Evaluar el riesgo y determinar el nivel adecuado de seguridad para su organización.
- Identificar la información valiosa.
- Definir las políticas de seguridad que utilizan el riesgo de los criterios de administración y protegen la información identificada.
- Determinar la manera en que las políticas se pueden implementar de mejor manera dentro de la organización existente.
- Asegurar que se lleven a cabo los requerimientos de administración y tecnología.
- Proporcionar a todos los usuarios un acceso eficaz a los recursos correspondientes, según sus necesidades.

Windows 2000 ofrece funciones de seguridad extraordinarias que podrían proporcionar flexibilidad para cumplir con la mayoría de los requerimientos de seguridad demandantes. Cuando se planea la seguridad de Active Directory, los fundamentos de la solución de seguridad se crearán con base en:

- Autenticación
- Políticas de seguridad
- Control de acceso (derechos y permisos)

- Auditoría
- Privacidad e integridad de datos

El marco de trabajo de seguridad Windows 2000 está diseñado para completar los requerimientos de seguridad más estrictos. Sin embargo, el software por sí solo puede convertirse rápidamente en ineficiente sin la planeación y evaluación cuidadosa, lineamientos de seguridad eficaces y educación para el usuario.

Roles del servidor

Asimismo, las consideraciones de seguridad están influenciadas por el rol que desempeñará un servidor en particular dentro de una organización (como el controlador de dominio, servidor Web, servidor de archivo, servidor de base de datos).

Las implementaciones de seguridad se deberán aplicar en una manera adecuada, definiendo los roles de un servidor en particular que pueden facilitar hacer esto. A continuación se presentan los roles principales de un servidor:

- Controlador de dominio
- Servidor de archivo
- Servidor de aplicación
- Servidor de base de datos
- Autoridad de certificación
- Servidor Web
- Firewall
- Servidor de enrutamiento y servicio de acceso remoto

Controlador de dominio

Los controladores de dominio administran todos los aspectos de las interacciones de dominio del usuario. Active Directory se localiza en cada controlador de dominio y almacena las credenciales de seguridad para todas las cuentas de dominio así como para las políticas de seguridad basadas en el dominio y configuraciones. Debido a la información más importante almacenada, y al rol crítico que desempeñan dentro de la empresa, los servidores actúan como controladores de dominio que deberán ser asociados con medidas de seguridad estrictas.

Servidor de archivo

Los servidores de archivo almacenan archivos para acceso de grupos y usuarios. La finalidad principal de la seguridad para los servidores de archivo es garantizar la integridad de los archivos y disponibilidad de los mismos para los grupos y usuarios adecuados.

Definir el nivel de seguridad que se deberá asociar con los servidores de archivo se relaciona de manera directa con los datos que están siendo almacenados. Los propietarios de datos o política departamental por lo regular dictarán las medidas y estándares que deberá aplicarse al almacenamiento de datos.

Servidor de aplicación y base de datos

Los servidores de aplicación y base de datos ejecutan programas para la red que utilizan múltiples grupos y usuarios. La finalidad principal de la seguridad para los servidores de aplicación es garantizar la disponibilidad de los programas para los grupos de usuarios adecuados, la integración del programa o los programas y la integridad de los datos de registro.

Asigne los derechos y permisos correspondientes para los grupos que acceden al servidor. Esto normalmente será especificado por la persona que administra la aplicación en particular.

Por lo general, los grupos no necesitan modificar datos en servidores de aplicación y leer los permisos sería suficiente en la mayoría de los casos. Sin embargo, si a los usuarios se les permite modificar los archivos de configuración específica de programa durante una sesión, tendrán que tener permiso de Escritura para estos archivos.

Autoridad de certificación

Utilizar el software para establecer una autoridad de certificación (CA), como Microsoft Certificate Server, puede designar a un servidor para que funcione como una CA para su organización, emitiendo certificados digitales para la identificación y autenticación del usuario, para la firma de código o para fines de personalización.

Los servidores de certificado serán reservados frecuentemente a la más alta seguridad disponible en la empresa ya que comprometen la autoridad certificada en casi todos los objetos de seguridad de datos.

Servidor Web

El software de servidor Web, como es Microsoft Internet Information Services (IIS), habilita una computadora que esté ejecutando el Servidor Windows 2000 para albergar datos para intranet, extranet y acceso general a Internet.

La seguridad para los servidores Web se aplica junto con los datos particulares a los que se da servicio. Por lo menos, un servidor Web también puede ser un servidor de aplicación, pero en ocasiones, los servidores Web también proporcionan acceso a redes tanto internas como de Internet.

Firewall

Un *firewall* (como Proxy Server) actúa como una central internacional segura entre un sitio (red interna) y redes externas (Intranets, extranets o Internet), restringiendo tanto la dirección como los tipos de solicitudes. Los *firewalls* más eficaces actúan como *proxies* para servicios específicos. Esto significa que, un programa en *firewall* sirve como un intermediario entre el sitio y los servicios que existen para soportar las operaciones en la red externa (como la exploración Web). Los programas *proxy* están diseñados para utilizarse con protocolos de comunicación particulares, y pueden aplicar restricciones sofisticadas a los datos. Además, los *firewalls* pueden ocultar sus direcciones de red internas de la red externa y rechazar conexiones de direcciones de red externas.

Enrutamiento y servidor de acceso Remoto

Un servidor de acceso remoto proporciona acceso remoto a recursos de la empresa. El Enrutamiento y Acceso remoto de Windows 2000 (RRAS) soporta los siguientes roles de servidor:

- Servidor de marcación
- Servidor de red privada virtual (VPN)
- Servidor de enrutamiento

Un servidor único puede llevar a cabo todos estos roles, o roles particulares que se pueden distribuir entre los servidores.

Políticas de seguridad Active Directory

La política de seguridad se puede aplicar a los Sitios, Dominios y OUs (en ese orden). Ya que estamos hablando de la seguridad de Active Directory, se aplica de manera predeterminada la herencia; derechos aplicados al dominio que también se aplican a los OUs menores del dominio.

El enfoque de una política de seguridad se relaciona de manera directa con el espacio de nombre Active Directory, la jerarquía del árbol estructurado del sitio, dominios, OUs y usuarios/computadoras. En muchos casos, esto dará como resultado una amplia política de seguridad la cual existirá para un sitio o dominio. Cada una de sus OUs menores (o dominios menores) tendrán sus políticas de seguridad las cuales son un subgrupo de aquéllas que se aplican a su principal, con políticas adicionales asignadas que son específicas para sus fines organizacionales y funcionales.

Una política de seguridad está contenida en un objeto de Política de grupo. Puede aplicar políticas de seguridad asignando un objeto de Política de grupo para cada dominio y OU. Unicamente se puede asignar un objeto de Política de grupo por dominio o una OU a la vez.

Derechos y permisos

Los accesos a los recursos y/u objetos se controlan a través de permisos y derechos de acceso. Los derechos aplican a los grupos y cuentas de usuarios (y a los procesos que actúan en nombre de los grupos o usuarios) y autorizan al grupo o usuario a realizar ciertas operaciones, tales como respaldo de archivos y directorios, conexión de manera interactiva o el apagar una computadora. Los derechos definen las capacidades ya sea a nivel de dominio o a nivel local y son los mejores administrados con base en un grupo; un usuario que se conecta como miembro de un grupo hereda los derechos asociados con el mismo.

Los permisos son atributos de seguridad de objetos, los objetos incluyen objetos de sistema de archivo NTFS (archivos, carpetas o volúmenes), objetos de sistema como procesos y objetos Active Directory o locales (como Usuario, Grupo o de Impresora).

Los permisos especifican cuáles usuarios o grupos pueden acceder el objeto así como qué acciones pueden realizar en él. Los tipos de permisos que se pueden otorgar varían según el objeto del tema. Los objetos del sistema de archivo contienen atributos de

permisos como son Lectura, Escritura y Ejecución para una carpeta, mientras que la puesta en cola de impresión tiene permisos relacionados con otorgar la capacidad de imprimir y administrar la impresora y la puesta en cola de trabajo. Los permisos asignados a un objeto permanecen con el objeto, incluso cuando se mueve a otro contenedor o dominio en Active directory.

Los derechos se aplican de manera independiente para cualquier otro objeto lo cual significa que un derecho puede en ocasiones anular un permiso. Por ejemplo, un usuario que es miembro de un grupo de Operadores de respaldo tiene derecho a realizar operaciones de respaldo para todos los servidores dentro de un dominio. Ya que este derecho requiere la capacidad de leer todos los archivos en dichos servidores, el usuario podrá acceder los datos que de otra manera tenían acceso prohibido a través de permisos en el objeto. En este caso, el derecho de realizar un respaldo, sienta precedentes sobre los permisos de directorio y archivo.

Los permisos son acumulativos: un permiso de nivel más alto incluye todos los permisos de nivel más bajo, con excepción del permiso de No acceso, el cual anula a los demás. Por ejemplo, si un usuario A es miembro de dos grupos con permisos para un archivo particular, el Grupo 1 que tiene permiso de Lectura y el Grupo 2 que tiene permiso de Cambios, los derechos eficaces para el usuario A en este archivo podría ser Cambiar. Sin embargo, si un usuario A se agrega al Grupo 3 que tiene el permiso etiquetado de No acceso, el usuario A no tendrá acceso al archivo a pesar de los permisos otorgados por los miembros de otro grupo.

Windows 2000 Server utiliza un grupo de permisos estándar para los directorios NTFS y archivos. Los permisos estándar pueden ser combinaciones de permisos individuales específicos. Los permisos individuales son:

- Control total
- Modificar
- Lectura y ejecutar
- Lista de contenido de carpeta (sólo para carpetas)
- Lectura
- Escritura
-

Herencia

De manera predeterminada, cada objeto menor hereda permisos de objeto mayor. La herencia propaga los permisos asignados a un objeto y sus propiedades a todos los menores del objeto. La herencia se puede restringir para un objeto de contenedor.

Al aplicar la herencia a la asignación de derechos y permisos, se puede distribuir a través de la administración de la empresa, la administración de cuentas, políticas y recursos. El componente administrativo de su política de seguridad puede ser paralela efectivamente a un diagrama organizacional, un árbol de administradores con un enfoque de autoridad limitado exitosamente.

De manera predeterminada, un objeto hereda autorizaciones de su principal cuando se crea. Esto hace que sea más fácil crear y administrar jerarquías lógicas. Sin embargo,

los permisos asignados o modificados al objeto en sí siempre sentarán precedentes sobre los permisos heredados. Por ejemplo, si agrega un archivo a una carpeta que tiene permiso de Cambio de grupo de informática y permiso de Lectura para el grupo Financiero, dichos permisos aplicarán al archivo. Podría cambiar los permisos del archivo seleccionándolos y modificando los permisos de grupo Financiero a No acceso. Al inhabilitar la opción para heredar permisos para el principal, los permisos del archivo no se verán afectados por ningún cambio subsecuente a los permisos asignados a la carpeta principal.

Control de acceso

El acceso a los recursos y u objetos se controla a través del permiso y derechos de acceso. El control de acceso se puede aplicar a cualquier objeto en Active Directory. Los derechos y permisos que asigne al nivel de dominio son distribuidos a través del dominio por Active Directory.

Derechos y permisos

Los derechos aplican a los grupos y cuentas de usuarios (y a los procesos que actúan en nombre de los grupos o usuarios) y autorizan al grupo o usuario a realizar ciertas operaciones, tales como respaldo de archivos y directorios, conexión de manera interactiva o el apagar una computadora. Los derechos definen las capacidades ya sea a nivel de dominio o a nivel local y son los mejores administrados con base en un grupo; un usuario que se conecta como miembro de un grupo hereda los derechos asociados con el mismo.

Los derechos se aplican de manera independiente para cualquier otro objeto lo cual significa que un derecho puede en ocasiones ser más fuerte que el permiso. Por ejemplo, un usuario que es miembro de un grupo de Operadores de respaldo tiene derecho de realizar operaciones de respaldo para todos los servidores dentro de un dominio. Ya que este derecho requiere la capacidad de leer todos los archivos en dichos servidores, el usuario podrá acceder los datos que de otra manera tenían acceso prohibido a través de permisos en el objeto. En este caso, el derecho de realizar un respaldo, sienta precedentes sobre los permisos de directorio y archivo.

Los permisos son atributos de seguridad de objetos, los objetos incluyen objetos de sistema de archivo NTFS (archivos, carpetas o volúmenes), objetos de sistema como procesos y objetos Active Directory o locales (como Usuario, Grupo o de Impresora).

Los permisos especifican cuáles usuarios o grupos pueden acceder el objeto así como qué acciones pueden realizar en él. Los tipos de permisos que se pueden otorgar varían según el objeto del tema. Los objetos del sistema de archivo contienen atributos de permisos como son Lectura, Escritura y Ejecutar para una carpeta, mientras que la puesta en cola de impresión tiene permisos relacionados con otorgar la capacidad de imprimir y administrar la impresora y la puesta en cola de trabajo. Los permisos asignados a un objeto permanecen con el objeto, incluso cuando se mueve a otro contenedor o dominio en Active directory.

Se pueden asignar permisos a objetos como un todo o para cualquier atributo del objeto. Esto da como resultado la capacidad de aplicar control de acceso *fine-grain* dentro de

Active Directory. Esto también puede dar como resultado un esquema administrativo complejo que es imposible de administrar. Al planear el control de acceso, se asegura que los derechos se apliquen en una manera lógica.

Los permisos asignados permiten o niegan acciones particulares para un objeto particular, o sus propiedades. Para los contenedores (como OUs), estos permisos se pueden aplicar a objetos menores. Esto permite un rango de opciones al ejercer el control de acceso. Se puede controlar no únicamente lo que se puede ver en un objeto, sino que también se pueden ver propiedades particulares del objeto. Los permisos para una sola propiedad son el nivel más fino de granularidad que se puede establecer.

Active Directory proporciona una gran cantidad de flexibilidad sobre cómo aplicar los permisos. Los permisos que se asignan a un contenedor se pueden aplicar a (Dominio/OU):

- El objeto actual
- El objeto y sus objetos menores
- Unicamente sus objetos menores
- Unicamente sus objetos específicos menores

Herencia

Los permisos son acumulativos: un permiso de nivel más alto incluye todos los permisos de nivel más bajo, con excepción del permiso de No acceso, el cual es más fuerte que los demás. Por ejemplo, si un usuario A es miembro de dos grupos con permisos para un archivo particular, el Grupo 1 que tiene permiso de Lectura, y el Grupo 2 que tiene permiso de Cambios, los derechos eficaces para el usuario A en este archivo podría ser Cambiar. Sin embargo, si un usuario A se agrega al Grupo 3 que tiene el permiso etiquetado de No acceso, el usuario A no tendrá acceso al archivo a pesar de los permisos otorgados por los miembros de otro grupo.

De manera predeterminada, cada objeto menor hereda permisos de objeto mayor. La herencia propaga los permisos asignados a un objeto y sus propiedades a todos los menores del objeto. La herencia se puede restringir para un objeto de contenedor.

Al aplicar la herencia a la asignación de derechos y permisos, se puede distribuir a través de la administración de la empresa, la administración de cuentas, políticas y recursos.

De manera predeterminada, un objeto hereda autorizaciones de su principal cuando se crea. Esto hace que sea más fácil crear y administrar jerarquías lógicas. Sin embargo, los permisos asignados o modificados al objeto en sí siempre sentarán precedentes sobre los permisos heredados. Por ejemplo, si agrega un archivo a una carpeta que tiene permiso de Cambio de grupo de informática y permiso de Lectura para el grupo Financiero, dichos permisos aplicarán al archivo. Podría cambiar los permisos del archivo seleccionándolos y modificando los permisos de grupo Financiero a No acceso. Al inhabilitar la opción para heredar permisos para el principal, los permisos del archivo no se verán afectados por ningún cambio subsecuente a los permisos asignados a la carpeta principal.

Administración delegada

La capacidad de delegar la administración es una de las funciones clave de Active Directory, y una que ha sido esperada ansiosamente por los administradores. La administración delegada proporciona la capacidad de ofrecer control administrativo limitado sobre partes y tareas dentro de Active Directory. Esto elimina la necesidad de que múltiples administradores tengan autoridad total sobre un dominio o sitio. Un administrador que tenga los derechos adecuados puede, a su vez, delegar la administración de un subconjunto de sus cuentas y recursos. La manera más sencilla de utilizar la delegación es reflejar la responsabilidades administrativas de su organización en sus políticas de seguridad. Por ejemplo, al especificar el departamento de contabilidad como un contenedor, se pueden asignar al administrador del departamento derechos que estén relacionados con la creación y administración de estos recursos de contabilidad, grupos y usuarios.

La delegación puede ser para un contenedor individual, o un árbol de contenedores. Estos derechos asignados son eficaces únicamente para el contenedor o contenedores designados y puede permitir al usuario autorizado:

- Asignar propiedades para un contenedor particular.
- Crear y eliminar tipos específicos de objetos menores del contenedor.
- Asignar propiedades específicas en tipos específicos del contenedor de objetos menores.

Las opciones para accesar la delegación se pueden sobrellevar debido al número completo de opciones disponibles.

El administrador puede:

- Delegar el control de todo el contenedor o 14 tipos diferentes de objetos delegables.

Dentro del contenedor de objetos delegables seleccionados, existen:

a) 16 tipos de permisos Generales.
b) 54 permisos de propiedad individual.
c) 88 permisos individuales relacionados con los permisos de creación/eliminación de subobjetos.

Por lo tanto, existen 158 opciones de permisos individuales, los cuales dan como resultado millones de combinaciones. Mientras que esta es una buena idea para conocer los tipos de permisos delegables disponibles, se pueden mantener permisos a un alto nivel suficiente para hacerlos administrables.

- Delegue todos los contenedores cuando:

a) El enfoque de la administración para el grupo delegado sea para todos los objetos dentro del contenedor.
b) Cuando pase la autoridad de un subárbol en un ambiente de informática descentralizada.

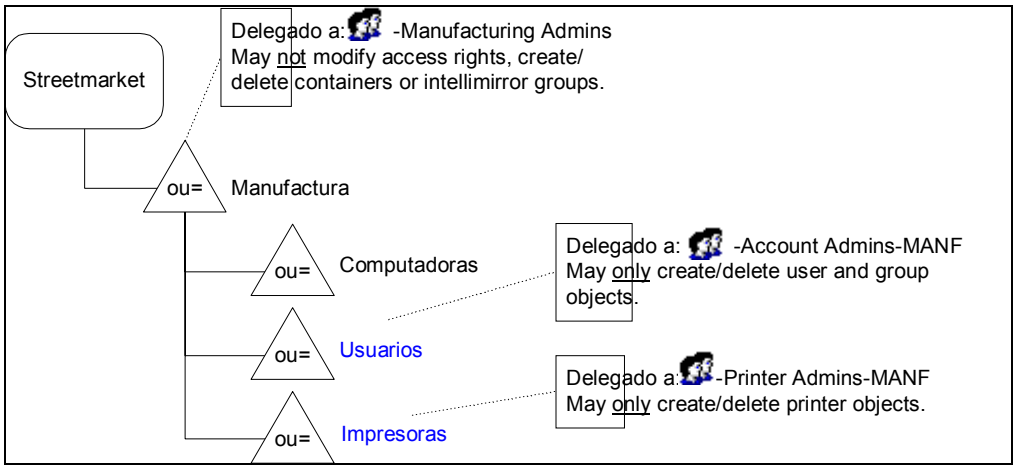
Este tipo de delegación es adecuado para la delegación de OU departamental.

- Delegar objetos de contenedor parciales cuando:

c) Se asigne una autoridad administrativa basada en la tarea, como cuando se crean Administradores de impresión o Administradores de usuario, etcétera.

La delegación parcial de contenedor es adecuada para la administración basada en tareas.

La Figura X siguiente muestra la delegación básica para los dos propósitos. El grupo "Administración de manufactura" ha sido delegado a la OU de manufactura y proporcionó todos los accesos excepto aquéllos que están reservados para los administradores de nivel de raíz. Las OUs de Usuarios e Impresoras únicamente delegaron el control de sus objetos respectivos (usuarios e impresoras).



■ Figura 29: Delegación simple

Observe que a la entidad Administrativa para OU se le proporcionó acceso completo, excepto para aquellos permisos reservados para los administradores de la empresa, mientras que a los administradores basados en las tareas (Usuarios, Impresoras) únicamente se les proporcionaron los permisos necesarios para llevar a cabo las tareas asignadas. A menos de que se sienta completamente cómodo con los impactos de delegación de permisos, sería de utilidad confiar en ciertos conceptos básicos durante la planeación:

1) Cualquier permiso que pueda tener un impacto adverso en unidades adyacentes, o contenedores superiores en la jerarquía que deberán ser restringidos a la autoridad administrativa más alta.
2) Nunca delegar una autoridad completa de un contenedor (por ejemplo, Modificar permisos y control de accesos), a menos de que exista una autoridad administrativa más elevada.
3) Al delegar tareas, únicamente se delegan aquellos objetos del contenedor y permisos que se requieran para realizar el trabajo.

La manera en que se delegan los permisos también variará de acuerdo con el modelo de informática administrativo que se utilice:

Tipo de informática	*Método recomendado para la delegación de OU*
Centralizado	La delegación siempre se basa en las tareas.
Descentralizado	Todos los permisos se delegan.
Informática distribuida	La delegación de permisos y creación de contenedor se restringe.

Impacto en el diseño de directorio

La capacidad para realizar delegaciones administrativas lógicas basadas en los contenedores es suficiente para justificar un impacto en la estructura de la OU para

contabilizar los contenedores delegables. Aunque hay que tener cuidado, no hay que basarse estrictamente en la estructura de directorio de acuerdo con la necesidad administrativa.

Desde la perspectiva de las consideraciones de diseño de prioritización, el peso ubicado en la facilidad de administración se ajustará después de que se cumplan ciertos objetivos.

Es evidente que la estructura del directorio debe poder administrarse, y hasta este punto administración sienta precedentes. Sin embargo, una vez que se ha cumplido el objetivo, la administración deberá tomar un respaldo para otros objetivos de diseño como son la seguridad, optimización de red, flexibilidad y escalabilidad.

Infraestructura de clave pública

Las redes ya no son sistemas cerrados en los que la sola presencia del usuario en la red puede servir como prueba de identidad. Las redes empresariales pueden consistir en intranets, sitios en Internet y extranets, muchas de las cuales pueden ir más allá de la red inmediata.

Existen varias razones para preocuparse sobre el acceso a los datos. Muchas transacciones de negocios se llevan a cabo a través de la red. Y, varios empleados no son permanentes. O, su compañía puede trabajar con socios en proyectos de enfoque limitado y duración, con empleados que usted no conoce.

Para explicar esto en otras palabras, verificar la identidad del usuario se ha convertido en algo más difícil en años recientes, ya que las relaciones de negocio (tanto entre compañías y entre compañías y sus empleados) se han convertido en algo más transitorio. Una infraestructura de clave pública puede proporcionar los mecanismos para resolver estos problemas al presentar certificados verdaderos que puedan verificar la autenticidad.

Dependiendo de las necesidades de su organización, una infraestructura de clave pública deberá incluir:

- Una política completa que establezca cómo se pueden utilizar los certificados y clave.
- Que los certificados se puedan utilizar por programas de clientes únicamente en intranets por todos los empleados o empleados específicos. Pueden utilizarse para cuentas relacionadas con compañías socias en extranets, o para cuentas de acceso limitado sobre Internet. Y los certificados deben utilizarse para los procedimientos de conexión con tarjetas inteligentes.
- Las políticas de administración verdaderas para cada autoridad de certificación (CA).
- Su organización puede requerir una CA para emitir certificados para autenticación de cuenta estándar o seguridad de correo electrónico. En este caso, únicamente puede necesitar seleccionar una CA verdadera para este fin. Sin embargo, si su organización cuenta con múltiples funciones de certificado, con firma, autenticación, correo electrónico y acceso extranet/Internet, deberá considerar la asignación de una CA verdadera para cada función.

- Emitir las reglas y la regla de validación para cada CA.
- Emitir las reglas y reglas de validación que especifiquen a quién y bajo qué circunstancias se puede emitir un certificado. Una sola CA que emita certificados de autenticación o correo electrónico puede utilizar certificados para todos o para empleados específicos. Las CA múltiples podrían emitir certificados únicamente para usuarios que tengan validez de acuerdo con la base funcional de las CAs, como son el miembro de grupo de Desarrollo para una CA de firma de código.
- Disponibilidad de las CAs en una cadena de certificados CA.
- Cuando un certificado CA es validado por otros CA, los certificados para ambos deben estar disponibles para el cliente. Cuando son muy largas las cadenas con CA, se asegura que la disponibilidad de todos los certificados CA puede ser difícil. Su infraestructura de clave pública debe dirigir dichas circunstancias posibles.
- Políticas de revocación de certificado.
- Las políticas se deben establecer revocando un certificado que ya no aplique o que haya entrado en desuso. Por ejemplo, puede necesitar revocar un certificado que haya sido emitido a un empleado que ya no trabaje en la organización.
- Políticas de renovación de certificado.
- Al expirar, en lugar de requerir un nuevo certificado, podría ser más efectivo renovar el certificado existente. La política debe cubrir si puede ocurrir esto, así como cuándo y cómo.

Microsoft Windows 2000 introduce una Infraestructura de clave pública (PKI) completa para la plataforma Windows. Esto aumenta y amplía los servicios criptográficos de clave pública (PK) de Windows, introducidos durante los años recientes, proporcionando un grupo integrado de servicios y herramientas administrativas para la creación, implementación y administración de aplicaciones basadas en PK. Esto permite a los desarrolladores de aplicaciones aprovechar al máximo los mecanismos de seguridad secretos convertidos de Windows 2000 Server o el mecanismo de seguridad basado en PK según corresponda. Al mismo tiempo, las empresas aprovechan el poder administrar el ambiente y las aplicaciones basadas en herramientas consistentes y mecanismos de política.

Propiedades de seguridad

Las propiedades de seguridad describen los atributos proporcionados a través de la clave pública como de los protocolos de seguridad IP. Estos incluyen elementos como la autenticación, integridad de datos y confidencialidad.

Windows 2000 incluye un sistema de administración clave funcional completo que se entrega a través del servidor Microsoft Certificate. Los certificados en Windows 2000 se integran con Active Directory a fin de permitir la publicación automática y procesamiento de solicitudes de certificado.

La seguridad PKI e IP protege sus datos privados en un ambiente público. Los administradores del sistema y usuarios necesitan sus datos para estar seguros de la intercepción, modificación o accesos de partes no autorizadas y que la entrega de los certificados sea segura.

Autenticación: Determina la identidad genuina para otro *host*. Sin una autenticación

sólida, cualquier dato y *host* que se envíen serán sospechosos. Puede seleccionar qué método de autenticación será utilizado para la comunicación.

Integridad: Protege los datos de modificación no autorizada en tránsito, con lo que se asegura que los datos se reciben exactamente como fueron enviados. Puede seleccionar qué algoritmo va a ser utilizado para los servicios de integridad.

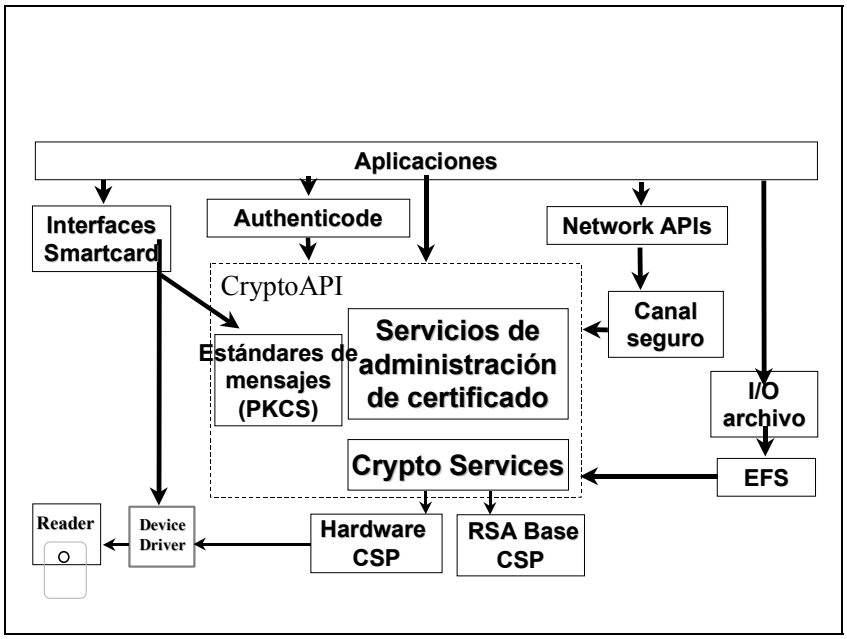
Confidencialidad: Asegura que los datos únicamente llegan a los depósitos objetivo encriptando los datos antes de la transmisión. Esta propiedad se puede configurar para cumplir con las restricciones de exportación, las cuales tienen límites en las longitudes clave.

Antireproducción o prevención de reproducción: Asegura que cada paquete IP es diferente. Esto protege contra los ataques durante un intento por interceptar un mensaje para ser reutilizado posteriormente y recursos de acceso de manera ilegal.

Sin repudio: Protege los datos de ser interceptados por la fuente. En otras palabras, el remitente no puede negar que fue la fuente de los datos que resultó ser una fuente de datos dudosa.

Componentes de seguridad de clave pública

El soporte para la creación, implementación y administración de aplicaciones basadas en PK se proporciona de manera uniforme en estaciones de trabajo y servidores de aplicación Windows NT y 2000 así como en estaciones de trabajo Windows 95 y 98. El gráfico que se muestra da una descripción general de estos servicios de aplicación. Microsoft CryptoAPI es la parte principal para estos servicios. Proporciona una interfaz estándar para funcionalidad criptográfica proporcionada a través de los Proveedores de servicios criptográficos instalables (CSPs). Estos CSPs pueden estar basados en software y/o aprovechar los dispositivos de hardware criptográficos, y soportar una variedad de algoritmos y fuerzas clave. Como se muestra en la figura, un CSP posible basado en hardware soporta tarjetas inteligentes.



- Figura 30

La estratificación de servicios criptográficos es un grupo de servicios de administración de certificados. Estos soportan los certificados estándar X.509v3 que proporcionan almacenamiento persistente, servicios de enumeración y soporte de codificación. Por último, existen servicios para tratar con los formatos de mensaje estándar en la industria.

Otros servicios aprovechan CryptoAPI para proporcionar funcionalidad adicional para los desarrolladores de aplicación. El Canal seguro (schannel) soporta la autenticación de red y la encriptación utilizando los protocolos TLS y SSL estándar en la industria. Estos se pueden acceder utilizando la interfaz Winlnet de Microsoft para utilizarse con el protocolo HTTP (HTTPS) y utilizarse con otros protocolos a través de la interfaz SSPI. Authenticode soporta la firma de objetos y verificación. Esto ha sido utilizado principalmente para determinar el origen e integridad de los componentes descargados a través de Internet, aunque puede ser utilizado en otros ambientes. Por último, se soportan interfaces de tarjeta inteligente de fines múltiples. Estas han sido utilizadas para integrar tarjetas inteligentes criptográficas en una aplicación de manera independiente y son la base del soporte de conexión de tarjeta inteligente integrada con Windows 2000.

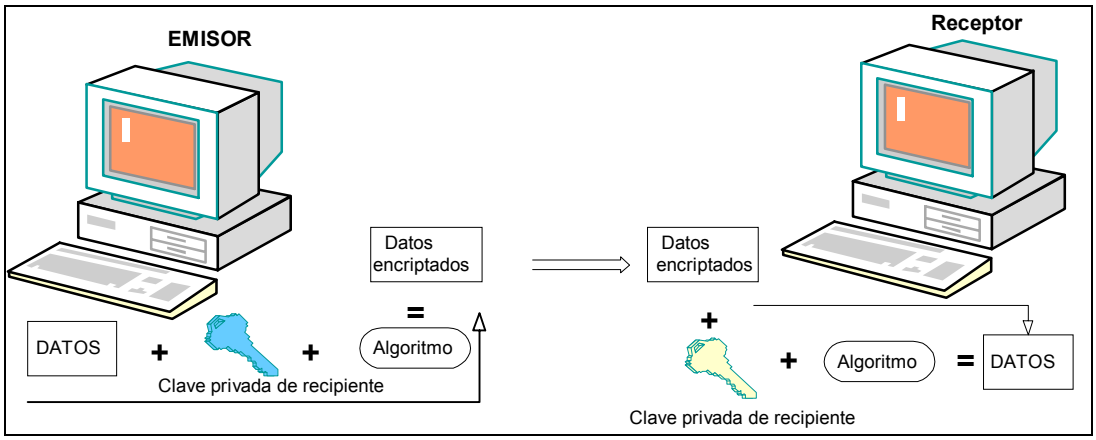
Criptografía y claves públicas

La criptografía es la ciencia de protección de datos. Los algoritmos criptográficos combinan matemáticamente la entrada de datos en texto plano y una clave de encriptación para generar datos encriptados denominados *ciphertext*.

En la criptografía clave secreta tradicional, las claves de encriptación y decriptación son idénticas a aquéllas que comparten datos sensibles. Las partes que deseen comunicarse con la criptografía de clave secreta deberán intercambiar de manera segura sus claves

de encriptación y decriptación antes de que puedan intercambiar los datos encriptados.

Por el contrario, la propiedad fundamental de la criptografía PK consiste en que las claves de encriptación y decriptación son diferentes. La encriptación con una clave de encriptación de clave pública es una función “de una vía”; el texto plano se vuelve a su vez *ciphertext* de manera fácil pero la clave de encriptación es irrelevante para el proceso de decriptación. Una clave de decriptación diferente (relacionada pero no idéntica a la clave de encriptación) es necesaria para regresar el *ciphertext* a texto plano. Por lo mismo, para la criptografía PK cada usuario tiene un par de claves que consisten en una clave pública y una clave privada. Al dar a conocer la clave pública, es posible que otros envíen datos encriptados al propietario de la clave que puede decriptar únicamente el mensaje utilizando la clave privada. De igual forma, un usuario puede transformar los datos utilizando su clave privada de igual manera que aquéllos pueden verificar que se originó con el propietario de la clave privada. Esta capacidad es la base para las firmas digitales que se analizan subsecuentemente.

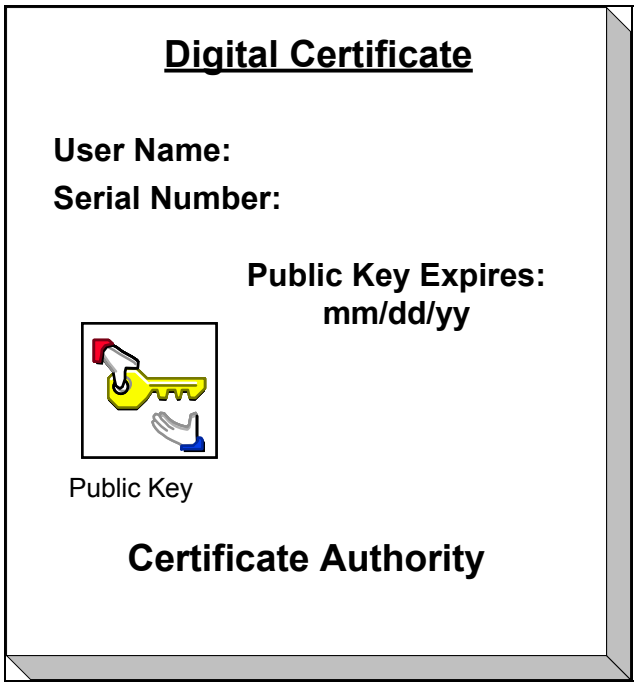


- Figura 31

La figura anterior muestra el flujo básico de datos utilizando la Criptografía de clave pública. Si el remitente en este caso desea enviar datos a la computadora receptora utilizando una clave secreta por ejemplo, tanto el remitente como el receptor podrían generar la mitad de la clave secreta. El remitente podrá obtener una clave pública de receptor para encriptar la mitad de la clave secreta y enviarla al receptor. El remitente y el receptor combinan las mitades de la clave secreta para generar la clave secreta compartida que va a ser utilizada para encriptar los datos que van a ser enviados. Esta negociación de clave secreta y el uso de la clave secreta para encriptar los datos proporciona autenticidad, integridad y confidencialidad.

Certificados

Los certificados proporcionan un mecanismo para obtener confidencialidad en la relación que existe entre una clave pública y la entidad apropiándose de la clave privada correspondiente. Un certificado es un tipo particular de un estado firmado de manera digital; el tema del certificado es una clave pública de tema particular y el certificado es firmado por el emisor (manteniendo otro par de claves privada y públicas).



- Figura 32

Por lo regular, los certificados también pueden contener otra información relacionada con la clave pública del tema, como es la información de entidad sobre la entidad que tiene acceso a la clave privada correspondiente. Por lo tanto, al emitir un certificado el emisor trata de validar la unión entre la clave pública del tema y la información de identidad del tema.

Servicios de certificado

Microsoft Certificate Server, incluido en Windows 2000, proporciona servicios personalizables para la emisión y administración de certificados para aplicaciones que utilizan la criptografía de clave pública. Certificate Server puede desempeñar un rol central en la administración de dicho sistema a fin de proporcionar comunicaciones seguras a través de Internet, intranets corporativas y otras redes no seguras. Microsoft Certificate Server se puede personalizar a fin de soportar los requerimientos de la aplicación de organizaciones diferentes.

El rol de Servicios de certificados es crear Autoridad de certificación (CA) con el fin de recibir una solicitud de certificado en formato PKCS #10, verificando la información en la solicitud y emitiendo un certificado X.509 correspondiente en formato PKCS #7. EL módulo de política para el Servidor de certificado utiliza la autenticación de red de solicitudes de certificado para emitir certificados a los usuarios con cuentas de dominio 2000. El módulo de política puede ser personalizado a fin de cumplir las necesidades de emisión de la organización. El Servidor de certificado genera certificados en formato X.509 estándar.

El Servidor de certificado recibe solicitudes para nuevos certificados sobre transportes como RPC, HTTP o correo electrónico. Cada solicitud se verifica comparándola con las

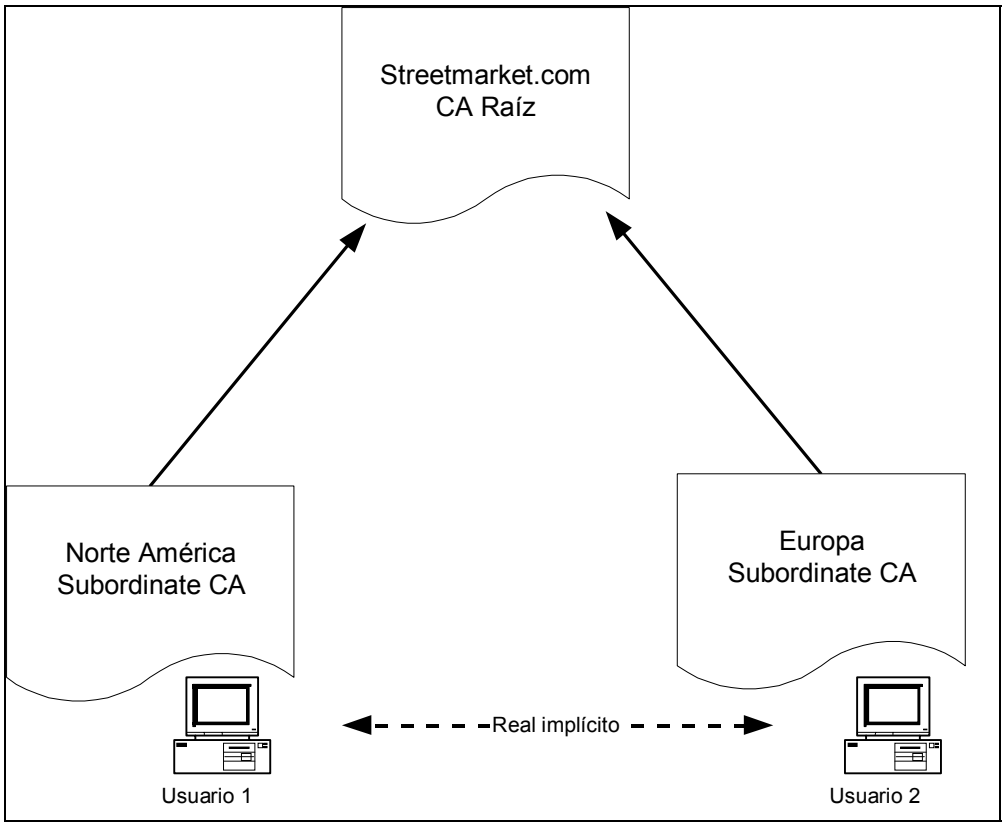
políticas personalizadas o específicas del sitio, grupos de propiedades opcionales del certificado que va a ser emitido y emisiones del certificado. Asimismo, permite que los administradores agreguen elementos a la lista de revocación de certificado (CRL), y publiquen una CRL firmada regularmente. Para solicitar un certificado, un usuario puede utilizar el *snap-in* de Administrador de certificado o el Explorador de Internet. Un Proveedor de servicio criptográfico (CSP) localizado en su computadora genera un par de claves públicas/privadas para el usuario. La clave pública del usuario se envía con su información de identificación necesaria al CA. Si la información de identificación del usuario cumple con los criterios de CA para otorgar una solicitud, el CA genera el certificado , el cual es recuperado por la aplicación del cliente (Administrador de certificado o Explorador de Internet) y se almacena de manera local.

Los Servicios de certificado soportan extensiones de correo en Internet con fines múltiples/seguros (S/MIME), pago seguro como las Extensiones electrónicas seguras (SET) y firmas digitales. Su organización puede elegir emitir todos los certificados desde una CA única o utilizar varias CAs que están encadenadas en una jerarquía *CA*.

Planeación de autoridades de certificado

Una Autoridad de certificado (CA) es simplemente una entidad o servicio que emite certificados. Una CA actúa como garantía de un enlace entre la clave pública del tema y la información de identidad del tema contenida en los certificados que emite. Las diferentes CAs se pueden enlazar para formar una confianza jerárquica de autoridades referidas como jerarquía CA.

Una implementación típica dentro de Windows 2000 es establecer una jerarquía de certificados Enterprise para distribuir la administración y carga. Esto no tiene nada que ver con la jerarquía de dominio aunque las CAs por lo regular coinciden con las confianzas *kerberos*. Una jerarquía de autoridad de certificado establece una confianza transitiva de certificados emitidos.



- Figura 33

Por ejemplo, debido a que Norteamérica y Europa confían en la CA Streetmarket, también confían en los certificados de cada uno.

Dentro de las grandes organizaciones que están compuestas de pequeñas y múltiples unidades, la necesidad de cada unidad para administrar sus propios recursos en la intranet corporativa es muy común. Cada unidad debe reforzar sus políticas bajo las cuales se garantice a los solicitantes tener acceso a sus recursos intranet.

Se pueden proporcionar estas unidades con la capacidad de establecer políticas y emitir certificados mismos permitiéndoles instalar Servicios de certificado y establecer su propia autoridad de certificación (CA). Se deberá monitorear cuidadosamente la proliferación de CAs múltiples dentro de una intranet de manera que no haya desuso de autoridad.

En las grandes organizaciones, pueden existir múltiples niveles de CAs, por lo que la jerarquía se puede implementar a través de todas las unidades en la organización principal. El uso de una jerarquía CA proporciona a las grandes organizaciones la flexibilidad necesaria para administrar políticas y otorgar certificados a través de un sistema de certificación compuesto de múltiples autoridades certificadas y puede ser administrado por un solo punto de control.

IPSec

Microsoft Windows 2000 Server incluye una implementación de seguridad de Protocolo de Internet (IPSec), basada en los estándares IETF para IPSec. La implementación de la

Seguridad IP en Windows 2000 está diseñada para proteger comunicaciones de extremo a extremo entre los *hosts*. Se supone que lo que está entre ellos, los medios en los que se transmiten los datos, no son seguros.

Los datos de aplicación desde el *host* que inician una comunicación se encriptan de manera clara antes de ser enviados a través de la red. En el *host* de destino, los datos se decriptan de manera transparente antes de que pasen a la aplicación que los recibe. Al encriptar todo el tráfico de red IP se asegura de que ninguna comunicación que utilice TCP/IP esté a salvo de *eavesdropping*. Debido a que los datos pasan y se encriptan en el nivel de protocolo IP, no se requieren paquetes de seguridad separados para cada protocolo en la versión TCP/IP.

Un nivel alto de seguridad con frecuencia incrementa la administración. Windows 2000 proporciona una interfaz administrativa, Administración de política de seguridad IP, para administrar de manera central la política, equilibrar la facilidad de uso y seguridad. Las políticas IPSec pueden configurarse fácilmente a fin de cumplir los requerimientos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global. Las políticas se basan en las metodologías de filtración IP críticas que permiten el acceso o bloqueo a las comunicaciones de alto nivel (todas las subredes), o a un nivel granular (protocolos específicos en puertos específicos), según sea necesario.

IPSec puede proporcionar alto nivel de protección debido a su implementación en el nivel de transporte IP (red Nivel 3). La seguridad Nivel 3 proporciona protección para todos los protocolos de nivel IP y mayores en el paquete de protocolos TCP/IP (TCP, UDP, ICMP, Raw (protocolo 255) y protocolos personalizados). Las aplicaciones que utilizan TCP/IP pasan los datos al nivel de protocolo IP, donde están asegurados por IPSec.

Los mecanismos de seguridad, los cuales operan por encima del Nivel 3, por ejemplo el Nivel de *sockets* de seguridad (SSL), únicamente protegen las aplicaciones que utilizan SSL como los exploradores Web. Los mecanismos de seguridad que operan por debajo del Nivel 3, por ejemplo la encriptación del nivel de enlace, no son portátiles para Internet o comunicación intranet enrutada.

Al operar en el Nivel 3, IPSec es claro para los usuarios y las aplicaciones. No se tienen que separar los paquetes de seguridad para cada protocolo en el paquete TCP/IP. Una vez que se configura la política y los usuarios no requieren realizar más acciones para asegurar los datos.

Política de seguridad IP

La Seguridad IP se implementa a través de la política Windows 2000. Varias políticas de seguridad pueden existir para un dominio dado, pero los componentes de la política son constantes.

Políticas de negociación: Las políticas de negociación determinan los servicios de seguridad que se utilizan durante una comunicación. Se puede seleccionar entre los servicios que incluyen la confidencialidad (ESP) o que no proporcionan confidencialidad (AH), o se puede especificar el algoritmo de seguridad IP. También se proporciona la capacidad para establecer múltiples métodos de seguridad para cada política de negociación. Si no es aceptable el primer método para la asociación de seguridad, el

servicio ISAKMP/Oakley continuará con la lista hasta que encuentre uno que pueda establecer la asociación.

Políticas de seguridad: Cada configuración de los atributos de seguridad IP se denomina Política de seguridad. Las Políticas de seguridad están compuestas por las políticas de negociación asociadas y filtros IP. Las Políticas de seguridad están relacionadas con las políticas del controlador de dominio. Una Política de seguridad IP se puede asignar a una Política de dominio predeterminada, la Política local predeterminada o Política de dominio personalizada que haya creado. Una computadora que se conecta al dominio seleccionará de manera automática las propiedades del Dominio predeterminado y las políticas locales predeterminadas, incluyendo la Política de seguridad IP asignada a la política de dominio.

Filtros IP: Los filtros IP determinan las diferentes acciones que se deben realizar basándose en dónde va un paquete IP, qué protocolo IP se está utilizando (por ejemplo TCP o UDP) y los puertos relacionados que van a ser utilizados por el protocolo. El filtro en sí se utiliza como un patrón para los paquetes que corresponden. cada paquete IP se verifica comparándolo con el filtro IP y si se encuentra coincidencia, se utilizan las propiedades de la Política de seguridad asociada para enviar la comunicación.

Opciones de seguridad IP

Parte de la política de negociación IPSec determina qué papel va a desempeñar una computadora durante la comunicación. Se pueden asignar tres modos básicos de operación a una computadora:

- Contestador: Un contestador se comunicará a través de IPSec cuando así se solicite. Esto puede resultar desde un contestador que inicie a una sesión de comunicación a una computadora que opera en el iniciador o de bloquear el modo o de ser solicitado por un iniciador.
- Iniciador: De manera predeterminada, un iniciador se comunicará a través de IPSec. Si la computadora de destino no soporta comunicaciones seguras, un iniciador responderá y comunicará todo en el borrado.
- Bloqueo: Una computadora entrará en el modo de bloqueo y sólo se comunicará a través de IPSec.

Las políticas básicas pueden mejorarse con filtros para proporcionar aplicación granular de la política. Por ejemplo, las computadoras desde un departamento particular pueden tener políticas de negociación múltiples dependiendo de la dirección IP de una computadora con la que establecen comunicaciones.

Los usuarios expertos pueden decidir qué algoritmo HMAC utilizarán para proporcionar integridad. HMAC-MD5 y HMAC-SHA proporcionan el mismo nivel de protección, con la diferencia de la longitud de clave que se utiliza para asegurar la información: MD5 utiliza una clave de 128-bits y SHA una clave de 160-bits. Longitudes más largas de clave proporcionan mayor seguridad.

Asimismo, los usuarios expertos pueden decidir qué algoritmo utilizarán para los servicios de confidencialidad. La confidencialidad se proporciona utilizando el Estándar de encriptación digital (DES). 40DES se proporciona para asegurar el cumplimiento con las

regulaciones de exportación, las cuales limitan las longitudes clave. 3DES, también denominado DES triple, proporciona la longitud de clave estándar de 56 bits que se ejecuta a través del proceso de encriptación tres veces. Cada vez que utilice una clave única nueva, con el resultado final siendo una encriptación triple de la información. Cipher Block Chaining (CBC) con DES (DES-CBC) también proporciona una longitud de clave de 56 bits y una prevención de reproducción adicional.

Protocolos de seguridad
Los Protocolos de seguridad proporcionan datos y servicios de protección de identidad (direccionamiento). Los usuarios expertos pueden seleccionar qué protocolo utilizarán para la comunicación:

Encabezado de autenticación (AH) proporciona la protección de identidad, con autenticación, integridad y servicios antireproducción. La protección de identidad significa que únicamente la información direccionada se encripta y no los datos. Sin embargo, ya que se proporciona la integridad, los datos no pueden ser modificados, sólo pueden ser leídos (AH no proporciona confidencialidad). El Encabezado de autenticación IP (AH) no puede proporcionar repudiación si se utiliza con ciertos algoritmos de autenticación.

Protocolo de seguridad encapsulada (ESP) ESP es un mecanismo para proporcionar integridad y confidencialidad a los datagramas IP. También puede proporcionar autenticación, dependiendo de qué algoritmo o modo de algoritmo se utilice. La no repudiación y protección del análisis de tráfico no es proporcionada por ESP. El Encabezado de autenticación IP (AH) no puede proporcionar repudiación si se utiliza con ciertos algoritmos de autenticación.
El Encabezado de autenticación IP puede utilizarse junto con ESP para proporcionar autenticación.

Planeación de políticas PKI e IPSec

La administración y manejo IPSec se integra a la interfaz de administración básica de Active Directory.

En los dominios Windows 2000, se puede llevar a cabo la autenticación mediante el protocolo Kerberos integrado. Por lo tanto, las infraestructuras de certificado no tienen que implementarse para asegurar a los clientes, servidores de archivo u OUs de seguridad (un grupo de computadoras agrupadas con una unidad organizacional Active Directory (OU) para fines de seguridad comunes).

En las situaciones acceso/VPN/enrutador a enrutador, se deben utilizar certificados de clave pública para la autenticación (o claves predistribuidas en el caso enrutador a enrutador

Por lo general, las comunicaciones intranet requieren niveles menores de seguridad que las comunicaciones de red pública: sin confidencialidad; sin conexión en túnel, permiso de comunicaciones no seguras. Esto acelerará la conexión de comunicaciones intranet, al tiempo que permite un cierto nivel de seguridad: integridad y autenticación.

Las comunicaciones IPSec pueden activarse, aceptarse o forzarse entre cualquier grupo de computadoras o de manera individual. Si los datos son muy sensibles, es fácil forzar a una computadora para aceptar únicamente comunicaciones IPSec.

Por lo general, ya que la conexión por túnel es adecuada para los niveles altos de seguridad, las reglas IPSec que especifican la conexión por túnel también deberán tener un nivel alto de seguridad en la política de negociación. En realidad los datos viajarán a través de la red pública, de manera que la confidencialidad (ESP) por lo general es garantizada. Debido a que se encapsulan los paquetes conectados por túnel, los cuales protegen el encabezado original, combinan ESP con AH para obtener protección de direccionamiento (encabezado) que no es necesario.

Definición de los niveles de seguridad

Implementar IPSec requiere un equilibrio entre hacer que la información esté disponible para un mayor número de usuarios y proteger la información importante de modificación e interpretación no autorizada. Tanto la seguridad IP como el marco de trabajo de seguridad Windows 2000 deben considerarse durante la planeación:

- Evaluando los niveles de riesgo para determinar el nivel adecuado de seguridad requerido.
- Determinar qué información debe ser encriptada y qué información debe ser protegida de la modificación.
- Definir las políticas de acuerdo con los criterios de riesgo y proteger la información categorizada.

Asimismo, las consideraciones de política también se ven influenciadas por la función de las computadoras en la que se aplican: se utilizará seguridad diferente para los controladores de dominio, servidores Web, servidores de acceso remoto, servidores de archivo, servidores de base de datos, clientes intranet y clientes remotos. IPSec puede volverse rápidamente inservible si no se tiene cuidado al planear y evaluar los lineamientos de seguridad, así como el diseño y asimilación de política sensible.

Antes de crear la política IPSec, defina:

- lo que es seguro
- cómo asegurarlo
- dónde asegurarlo
- quién administrará la política
- si los requerimientos de exportación son un problema

Se recomiendan los niveles de seguridad siguientes como lineamientos en la implementación del marco estructurado de seguridad general de Windows 2000. De manera más clara, los niveles de seguridad IPSec deberán coincidir con esta lista.

- Seguridad mínima
- Seguridad estándar
- Seguridad alta

Niveles de seguridad mínimos: IPSec no está habilitado de manera predeterminada. Si el plan de seguridad no solicita protección en ciertas situaciones, entonces no se requerirá ninguna acción administrativa.

Niveles de seguridad estándar: No existe una definición exacta de los niveles de seguridad estándar. Estos pueden variar en gran medida, dependiendo de las políticas e infraestructura de la organización. IPSec trata de cumplir con estos requerimientos ambiguos con:

- Políticas y reglas predeterminadas
- Los servicios de confidencialidad que se proporcionan como una opción, de manera que los servicios de protección son automáticos a un nivel estándar.
- Las configuraciones ISAKMP, algoritmos de autenticación e integridad, conexión por túneles y la regeneración clave son, por predeterminación, establecidos a un nivel estándar.

Las comunicaciones intranet por lo general requieren niveles más bajos de seguridad que Internet, WAN o comunicaciones entre redes externas: sin confidencialidad; sin conexión por túnel, con lo que se permiten comunicaciones más seguras. Esto acelerará la conexión de comunicaciones intranet, mientras se sigue permitiendo el mismo nivel de seguridad: integridad y autenticación.

Niveles de alta seguridad: Un nivel alto es adecuado para las situaciones de marcación remota, comunicaciones WAN o cualquier comunicación entre redes externa. Las comunicaciones de red privada no deberán excluirse de manera automática; en algunos casos la alta seguridad se puede garantizar para la intranet.

Nuevamente, no existe una definición exacta por las mismas razones, e IPSec cumple con estos requerimientos con:

- Servicios de confidencialidad para encriptar datos
- Perfect Forward Secrecy, lifetimes de clave configurable, Límite de modo rápido, Grupos Diffie-Hellman configurables y algoritmos extremadamente sólidos (3DES y SHA).
- Conexión por túnel para cualquier tipo de conexión de red.
- La capacidad de combinar ESP y AH para proporcionar el nivel máximo de protección: integridad de paquete además de la privacidad de datos.

Es importante recordar que no todos los ataques vienen de fuera de una red corporativa. Si se garantiza extremadamente alta seguridad para una intranet, se deberá utilizar la conexión por túnel, además de la política de negociación de alta seguridad.

Cuando los datos son extremadamente sensibles, se permiten comunicaciones no seguras con un *host* no IPSec que indica que no deberá ser habilitado, incluso si los *hosts* se encuentran dentro de la misma red, ya que esto no asegura que los datos estén a salvo. Las asociaciones de software también deberán ser prevenidas en este caso.

Por lo general, ya que la conexión por túneles es adecuada para niveles altos de seguridad, las reglas IPSec que especifican la conexión por túnel también deberán tener un nivel alto de seguridad en la política de negociación. Los datos viajarán, en realidad, a través de Internet, de manera que los servicios de confidencialidad (ESP) están garantizados generalmente.

Kerberos

En esta versión de Windows 2000, Kerberos versión 5 es el protocolo de seguridad primario. Kerberos verifica tanto la identidad del usuario como la integridad de los datos de sesión.

Los servicios Kerberos están instalados en cada controlador de dominio, y un cliente Kerberos se instala en cada estación de trabajo y servidor Windows 2000. Una autenticación Kerberos inicial de usuario proporciona al usuario una sola conexión a los recursos de la empresa.

Además de la seguridad mejorada, Kerberos permite:

- Relaciones verdaderas transitivas para la autenticación entre dominios
- Credenciales de autenticación emitidas por un servicio Kerberos son aceptadas por todos los servicios Kerberos dentro del árbol de dominio. También, credenciales emitidas por un servicio Kerberos en un campo de árboles de dominio son aceptadas por todos los servicios Kerberos dentro del campo.
- Autenticación mutua de cliente y servidor
- Se autentifican el cliente y servidor en la sesión de Kerberos.
- Procesos de autenticación eficaz
- Windows 2000 Server puede verificar las credenciales del cliente sin consultar el servicio Kerberos en el controlador de dominio.
- La implementación Kerberos en Windows 2000 es compatible con cualquier otra implementación Kerberos versión 5 que cumpla con IETF RFCs 1510 y 1964. Los clientes y servidores Windows 2000 pueden autenticar y comunicarse con una variedad de plataformas distintas para implementar el paquete de autenticación Kerberos.

Autenticación delegada para transacciones cliente/servidor multinivel

En algunas arquitecturas de aplicación, una transacción de cliente necesita transitar servidores múltiples. En este caso, el servidor actual puede autenticar el servidor solicitado en nombre del cliente.

Términos Kerberos

Servidor de autenticación, servidor de otorgación de boleta, centro de distribución de clave:

La documentación Kerberos (RFC 1510) se refiere al Servidor de autenticación (AS), un Servidor de otorgación de boletas (TGS) y un Centro de distribución clave (KDC).

El KDC es un servicio de red que suministra boletas y claves de sesión temporales. El KDC da servicio a ambos, la boleta inicial y las solicitudes de otorgación de boletas. La parte de boleta inicial en ocasiones se conoce como AS. La parte de otorgación de boletas en ocasiones se conoce como TGS. Por lo tanto KDC es tanto AS como TGS según RFC 1510.

Certificado de atributos privilegiados (PAC):

PAC es una estructura que contiene la SID del usuario y las GIDs universales, globales y locales de las que forma parte el usuario.

Boleta de otorgación de boleta, boleta:

En un intercambio Kerberos básico, el cliente envía primero una solicitud a AS para solicitar una otorgación de boleta que será utilizada para pedir una boleta a TGS para el servidor de destino.

Una boleta es un registro que ayuda al cliente a autentificarse para un servidor. Contiene la identidad del cliente, PAC, una clave de sesión, un sello y otra información, todo encriptado utilizando la clave secreta del servidor. De esta forma únicamente el servidor que conoce esta clave secreta puede decodificar la boleta. La boleta se obtiene de un KDC y se pasa al servidor de destino para su autenticación.

Una otorgación de boleta (TGT) por lo regular se obtiene durante el inicio de una sesión de conexión (en el intercambio AS). TGT incluye la información PAC para el usuario y será utilizada para obtener credenciales para otros servidores (por ejemplo, servidores de archivo) sin requerir mayor uso de la clave secreta del cliente.
TGT se encripta en la clave secreta KDC y no puede ser decriptado por el cliente a fin de evitar que el cliente cambie la información de membresía de grupo contenida en PAC.

Kerberos y hora

Dada la naturaleza sensible del tiempo de protocolo Kerberos, es de utilidad tener los relojes del sistema sincronizados. Tanto los clientes como los controladores de dominio realizarán de manera automática la sincronización de tiempo utilizando SNTP (Protocolo de tiempo de red seguros).

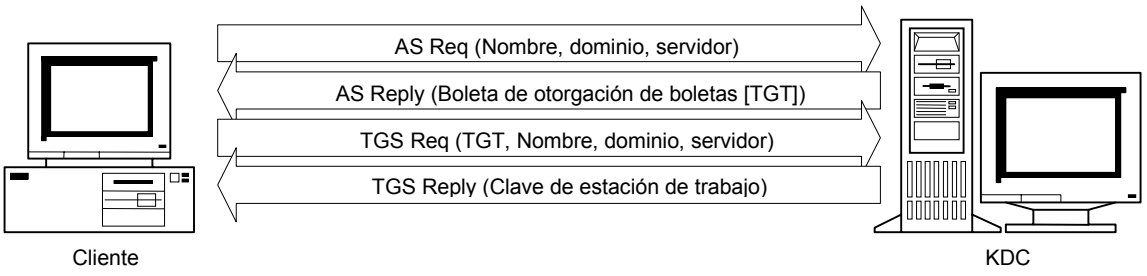
Un cliente Windows 2000 obtendrá el tiempo del sistema desde un controlador de dominio durante la conexión y las renovaciones de boletas subsecuentes. De igual forma, los controladores de dominio sincronizan el tiempo de manera jerárquica dentro de Active Directory. La raíz de la estructura SNTP será de manera predeterminada el Dominio de denominación maestro del campo. Windows 2000 incluirá una UI para la configuración adicional de los parámetros y maestro de tiempo SNTP.

Autenticación Kerberos: Conexión de dominio

KDC se ejecuta en todos los controladores de dominio Windows 2000 y consiste en un AS (Servicio de autorización) y un TGS (Servicio de otorgación de boletas). Estos dos servicios actúan en conjunto para proporcionar TGT (Boletas de otorgación de boletas) y Boletas de sesión para autenticación.

Cuando un cliente se conecta por primera vez al dominio Windows 2000, se incluirán dos pasos básicos.

- El cliente solicitará y recibirá una boleta de otorgación de boletas del KDC.
- El cliente presentará TGT a KDC y recibirá subsecuentemente una boleta de sesión para la autenticación al LSA local.



- Figura 34

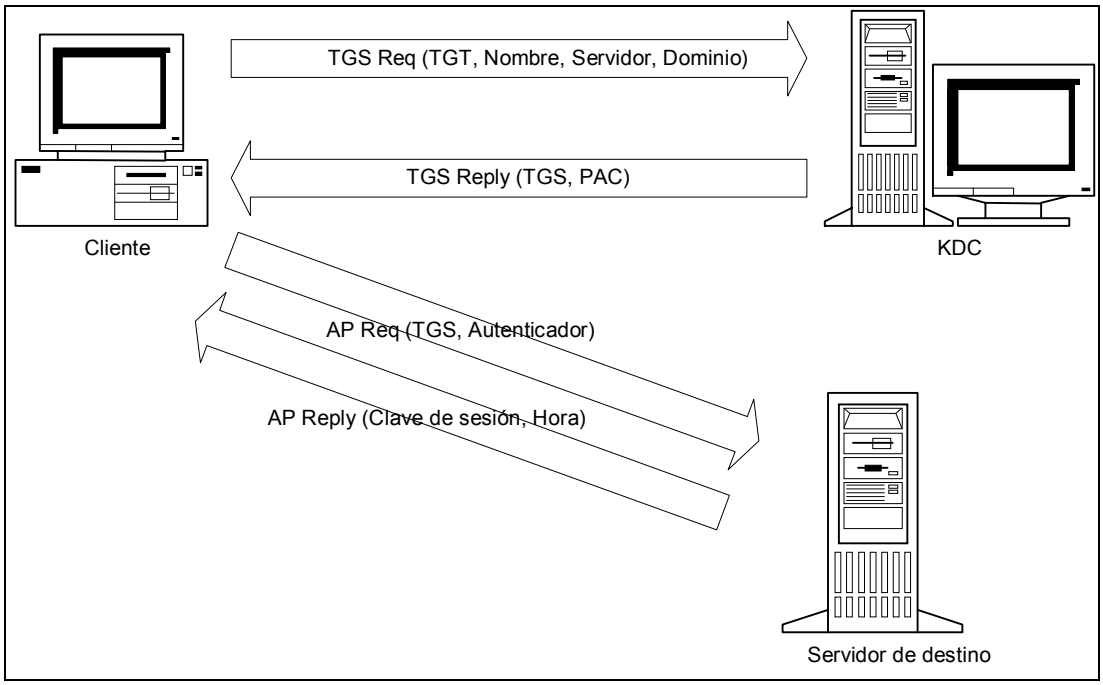
Todos los Controladores de dominio Windows 2000 se ejecutan como KDCs de Kerberos. Antes de conectar al sistema del cliente primero se tendrá que ubicar el controlador de dominio antes de continuar. Ya que la estación de trabajo forma parte de un dominio, esto por lo general ocurre cuando se crea el canal seguro y ya se conoce el DC.

Intercambios AS y TGS con KDC son enviados en el puerto 88 UDP. Los intercambios entre el cliente y el servidor de destino dependen del protocolo *pear* utilizado por dichos componentes.

- El cliente envía una solicitud AS inicial a KDC, proporcionando el nombre de usuario de nombre de dominio. Esta es una solicitud de autenticación y un TGT.
- KDC genera una respuesta AS que contiene TGT encriptado con la clave secreta KDC y una clave de sesión para intercambios TGS encriptados en la clave secreta del cliente. PAC está contenida en la parte de Datos de autorización de TGT. KDC encripta TGT con su propia clave privada a fin de evitar que el cliente cambie la información de membresía de grupo.
  Esta respuesta es enviada nuevamente al cliente.
- Para autenticar una conexión de usuario en el sistema local, el TGT obtenido en el intercambio AS se utiliza en el intercambio TGS a fin de obtener credenciales para el sistema local, esto significa que la conexión del usuario debe tener derechos para trabajar en el sistema local.
  El cliente genera y envía una solicitud TGS que contiene el nombre principal del cliente (= nombre de usuario) y realm, el TGT (desde intercambio AS) para identificar al cliente, y el nombre de estación de trabajo local servidor de destino. También incluye un Autenticador. De esta manera el usuario solicita el acceso a la máquina local.
- KDC genera y envía una contestación TGS que contiene una boleta para la estación de trabajo encriptada en la clave privada de cliente, y otra información (por ejemplo un Sello) encriptado utilizando la clave de sesión desde TGT. Asimismo, se incluye una parte Datos de autorización de la boleta que es el PAC que fue copiado por KDC desde el TGT original. Desde la información incluida en PAC el LSA del lado del cliente creará un token de acceso para el usuario.

Autenticación Kerberos: Acceso a recursos

Antes de que un cliente pueda acceder a un recurso en un servidor de destino, el cliente debe solicitar una boleta válida para el servidor de destino desde KDC.



- Figura 35

Solicitud TGS:

Para solicitar una boleta válida para el servidor de destino el cliente envía una solicitud TGS a KDC que incluye el TGT obtenido durante la conexión inicial, el nombre del cliente (=usuario) y el nombre de servidor de destino.

Respuesta TGS:

El KDC contesta con una boleta de servidor de destino y una clave de sesión para que sea utilizada entre el servidor de cliente y de destino.
El PAC se incluye en los Datos de Autenticación de la boleta. Tanto la clave de sesión como la boleta están encriptadas.

Solicitud AP:

Después de obtener una boleta válida para el servidor de destino, el cliente envía una Solicitud de aplicación (AP) al servidor de destino . La solicitud AP contiene la boleta de servidor y un autenticador para que sea utilizado entre el cliente y el servidor de destino. Entonces el servidor de destino decripta a la boleta y al autentificador y verifica que el mensaje no haya sido contestado.

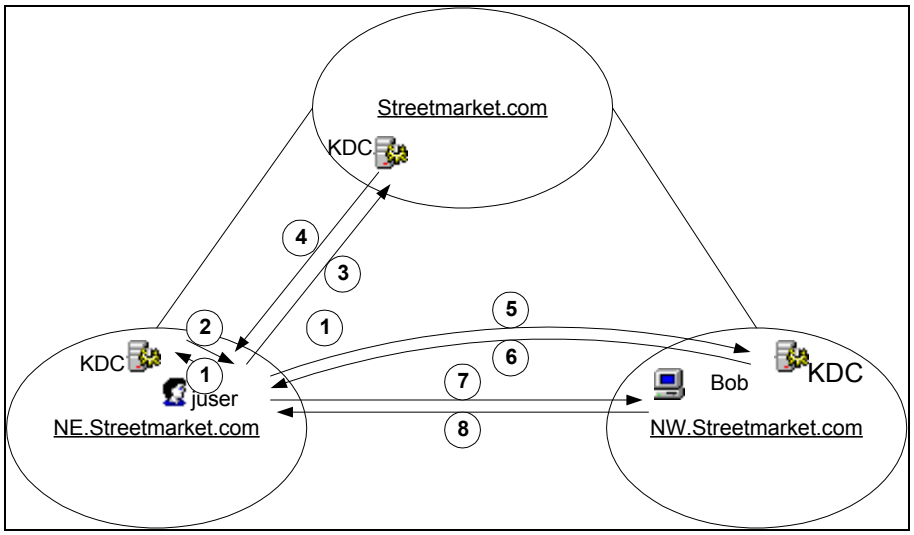
Contestación AP:

La contestación AP únicamente contiene el tiempo actual encriptado con la sesión clave, para informar al cliente que ha sido validado en el servidor de destino.

Autenticación Kerberos – *Cross-realm*

Los enlaces de *Realm* Kerberos son idénticos a los del dominio Windows 2000.

Entonces, la autenticación *Cross-Realm*, se puede establecer como el acceso a los recursos en otros dominios. El proceso de acceso *cross-realm* es muy similar al acceso *in-realm* excepto que los cliente KDC comenzarán a referir al cliente a KDCs en otros *realms*, que le siguen al establecimiento explícito verdadero del *realm* de destino.



■ Figura 36

Por ejemplo, el juser desea acceder BOB en el realm NW (dominio). El proceso para tener acceso es:

- 1) juser envía TGS_REQ a NE KDC
- 2) NE KDC contesta con la clave de sesión para Streetmarket
- 3) juser envía TGS_REQ a Streetmarket KDC con información de destino g
- 4) Streetmarket KDC replies with session key for NW.
- 5) juser envía TGS_REQ a NW KDC con información de destino
- 6) NW KDC contesta con TGT y datos de autorización para Bob
- 7) juser envía a AP_REQ a Bob con TGT y datos de autorización
- 8) Bob contesta con autentificador (opcional)

*Se utiliza la misma boleta de sesión para acceder a Bob

Las confianzas Kerberos en Windows 2000 son transitivas dentro del enfoque de un campo. Sin embargo, estas confianzas no establecen necesariamente una relación directa entre todos los dominios. Por el contrario, los clientes recibirán TGTs para realms mayores que a su vez proporcionan una ruta al destino. En el caso que aquí se muestra, se pueden justificar una gran cantidad de acceso entre NE.Streetmarket.com y NW.Streetmerket.com que explica la creación de un confianza Kerberos entre los dos dominios. Una vez que se ha obtenido la boleta para acceder al recurso, el cliente puede utilizar la boleta hasta su expiración (normalmente 10 horas).

Interoperabilidad Kerberos

Existen dos formas en que Windows 2000 puede interoperar con KDCs basados en MIT Kerberos.

1. Primero, Windows 2000 Workstation se puede configurar para utilizar un KDC de Unix. Los usuarios se pueden conectar a Windows 2000 utilizando una cuenta definida en KDC Unix. Esto es semejante al soporte de la estación de trabajo Unix para la conexión Kerberos. Cualquier aplicación Windows 2000 o Unix que requiera únicamente la autenticación basada en el nombre puede utilizar KDC Unix al igual que el servidor Kerberos.

2. La segunda manera en que Windows 2000 interopera con MIT Kerberos es a través de *cross-realm trust* entre Unix y dominio Windows 2000. *Cross-realm trust* es la mejor manera de soportar los servicios Windows 2000 que utilizan la impersonalización y el control de acceso.

Sin embargo, los clientes Windows 2000 no pueden utilizar un KDC Unix para autenticación en Active Directory. El modelo de seguridad distribuido Windows 2000 depende más que la lista de SIDs para autorización de datos en las boletas Kerberos, y estos protocolos se acoplan con los servicios de autenticación proporcionados por el servidor MIT Kerberos.

Planeación Kerberos

El uso Kerberos natural dentro de Windows 2000 requiere poca planeación a diferencia de la implementación de las extensiones de cliente en Windows 95 y Windows 98. Sin embargo, si alguna forma de interoperabilidad Kerberos requeriría *realms* externos, esto podría planearse con anticipación a la implementación . Posteriormente, una integración de PKI en el esquema de autenticación será permitida. También se planea pasar al Puerto 88 a través de cualquier *firewalls* a fin de permitir la duplicación verdadera entre los *realms*.

Revisión

La seguridad en Active Directory necesita crear un balance entre la realización de datos fácilmente accesibles, y al mismo tiempo, protegerlos. Esta sección analizó los conceptos de seguridad de Windows 2000 como son el control de acceso y versiones anteriores. También explicó los diversos mecanismos de seguridad proporcionados con Windows 2000, y presentó una discusión sobre cómo planear su infraestructura de seguridad.

Grupos

El mejor método de aplicación de la política de seguridades es a través de la administración de cuenta efectiva. Los grupos de seguridad en Windows 2000 representan el tercer principio de seguridad y representan un monto relevante de la relación que existe entre los usuarios y la seguridad.

La manera más eficaz de administrar la seguridad es asignar derechos y permisos para grupos de Seguridad en lugar de hacerlo para usuarios individuales o computadoras. Por los general, un usuario o computadora necesita acceder a varios recursos. Si el usuario o la computadora es miembro de un grupo con acceso a los recursos, se puede controlar

el acceso agregando o eliminando al usuario o computadora del grupo, en lugar de cambiar los permisos en el recurso. La configuración de los permisos para un usuario individual o computadora no excede los permisos otorgados al usuario o a la computadora a través de grupos a los que pertenece el usuario.

Basarse en las políticas de seguridad y en la administración de cuenta en grupos en lugar de hacerlo en usuarios o computadoras, reduce sus costos de propiedad. La administración de la cuenta o nivel de recurso se puede limitar según casos excepcionales.

Estructura de seguridad

Los grupos proporcionan un mecanismo sólido para establecer las estructuras de seguridad de Windows 2000, mientras que las estructuras de seguridad son una jerarquía administrativa que se utiliza para reducir el número de elementos que se van a administrar de manera individual.

Las estructuras de seguridad se pueden utilizar para combinar a los usuarios en grupos, y que dichos grupos se combinen con otros que son administrados más adelante por agrupaciones administrativas. Por ejemplo, un grupo particular de usuarios puede estar contenido dentro de otro grupo denominado usuarios de Office. El grupo puede utilizarse para asignar un ambiente de escritorio específico a través de la política. Otro grupo denominado Todos los usuarios puede incluir el grupo de usuarios Office así como otros para facilitar la colocación de configuraciones globales en los usuarios. El grupo Todos los usuarios es el principal de la estructura de seguridad particular, pero también debe ser administrado por otra estructura de seguridad que consiste de grupos tipo administrador.

El monto de las estructuras de seguridad es clasificar y agrupar los principios de seguridad de la misma manera en que deben ser administrados.

Uso de grupos

Un grupo puede tener miembros de otros grupos. Se puede utilizar esto para crear un rango adecuado de contextos de grupos para la asignación de derechos. Por ejemplo, puede tener un grupo de Producción que incluya manufactura, empaquetamiento y responsabilidades de envío. Podría crear grupos de manufactura, envío de producción, asignar derechos a cada uno y hacer que todos estos miembros de grupo sean parte del grupo Producción. Los derechos que asigna el grupo de Producción se asignan a todos sus grupos de miembros.

Para implementar una estrategia basada en el grupo:

- Establezca grupos de seguridad completos.
- Asigne derechos a los grupos antes de crear cuentas de usuario o computadora.
- Delegue la administración de grupos a la administradora adecuado o líder de grupo.

El tipo de grupo que utiliza para administrar las cuentas y recursos determina en parte cómo se aplican las políticas de seguridad . Windows 2000 Server presenta grupos nuevos y más funcionales, cada uno tiene una funcionalidad y enfoque diferente. Existen

tres grupos de seguridad dentro de Active Directory:

Grupos globales: Los grupos globales pueden contener usuarios únicamente desde el dominio local, pero pueden utilizarse en cualquier parte. Por lo tanto si los miembros de un grupo son limitados para un dominio único, se requiere el acceso a recursos globales, y el uso de grupos globales.

Grupos locales de dominio: Los grupos locales de dominio pueden contener miembros de cualquier dominio, pero también pueden ser utilizados en el dominio en el que fueron creados. Los grupos de dominio local se arreglan para el acceso de recursos de dominio local que requieren membresia global.

Grupos universales: Los grupos universales pueden contener miembros de cualquier dominio y se utilizan para asignar derechos de acceso a recursos.

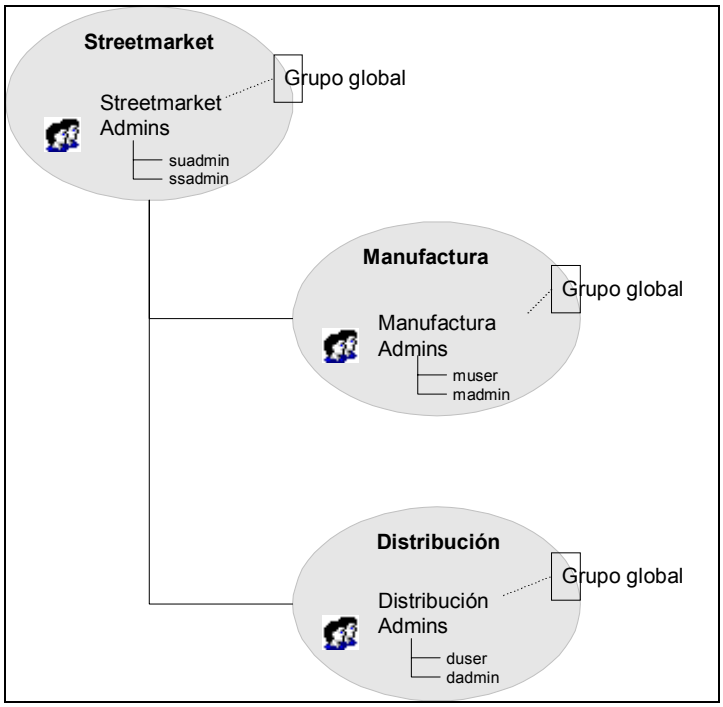
Las siguientes secciones proporcionan diferencias entre los tipos de grupos – refuerzos y limitaciones – así como recomendaciones sobre el uso.

Grupos globales

Los grupos globales son los miembros más versátiles de la familia de grupo y tienen los siguientes atributos:

- Pueden contener miembros únicamente desde el dominio en el que fueron creados.
- Los miembros pueden incluir cuentas de usuarios u otros grupos globales desde el mismo dominio.
- Varios miembros de grupos locales, universales y de dominio.

Estos atributos proporcionan un uso claro para los grupos globales. Dado que la membresia es limitada, los grupos globales pueden utilizarse para definir grupos, cuya membresia siempre estará restringida a sus propios dominios.

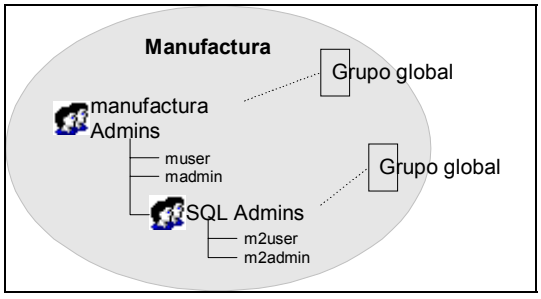


■ Figura 37: Global Group Membership

Por ejemplo, estos grupos Globales fueron creados en los dominios Streetmarket, de Manufactura y Distribución con la intención especial de permitir únicamente la membresia de las respectivas cuentas de dominio.

La membresia limitada reduce el número de aspectos de seguridad que podrían surgir normalmente en ese tipo de situación, cuando cuentas de dominio extranjeras no autorizadas intencionalmente o inadvertidamente se agregan a los grupos globales.

Los grupos globales están bien situados para la creación de estructuras de seguridad dentro de un dominio ya que pueden estar anidados, pero únicamente dentro del dominio en el que fueron creados. La creación del ejemplo anterior, el grupo Global “Manufacturación de administraciones” pueden contener otros grupos globales desde algún dominio de Manufactura como SQL Admins. Utilizar los grupos globales de esta manera proporciona una base para el control de acceso muy granular y asignación de permisos.



■ Figura 38: Grupos globales anidados

Utilizar grupos globales de esta manera proporciona una base para un control de acceso

muy granular y asignación de permisos.

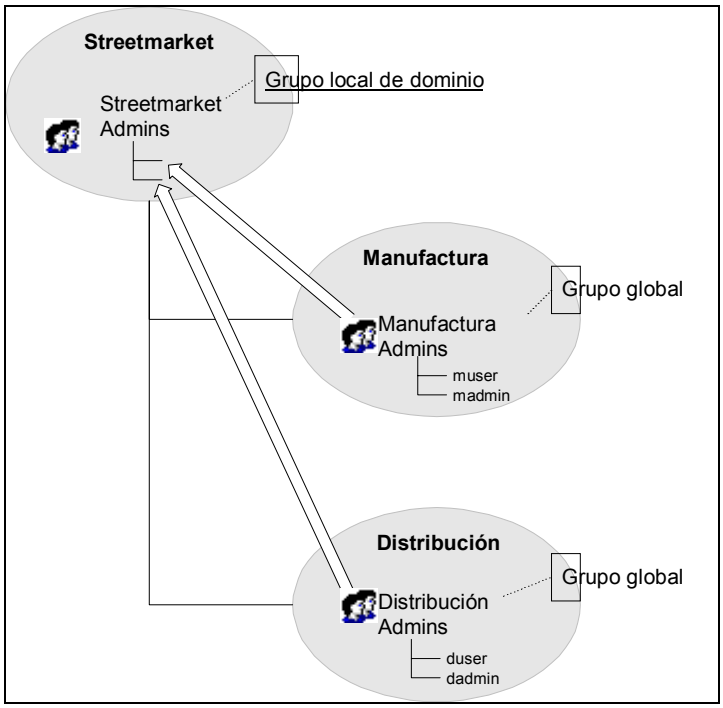
El aspecto global de los grupos Globales entra en su uso actual. Un grupo global puede ser miembro de cualquier otro tipo de grupo de seguridad, con lo que se crea el concepto de estructuras de seguridad. Esto significa que pueden ser utilizados para dirigir la asignación de permisos a los recursos fuera de sus dominios así como ser incluidos en los grupos Universales o Locales en cualquier dominio.

Grupos locales de dominio

Los grupos locales de dominio son antítesis de los grupos Globales, ya que pueden contener miembros de cualquier otro tipo, y desde cualquier dominio, pero únicamente se pueden dirigir de manera local. Al igual que los grupos Globales, los grupos locales de dominio pueden contener otros grupos locales de dominio, pero únicamente desde su propio dominio.

Estos atributos hacen que los grupos locales de dominio sean adecuados para limitar el enfoque de su uso, mientras permiten la membresia desde cualquier dominio.

La creación en las estructuras de seguridad en el concepto de las estructuras de seguridad presentado en el uso de grupo Global, un uso adecuado de los grupos locales de dominio podría servir como la base de la estructura de seguridad .



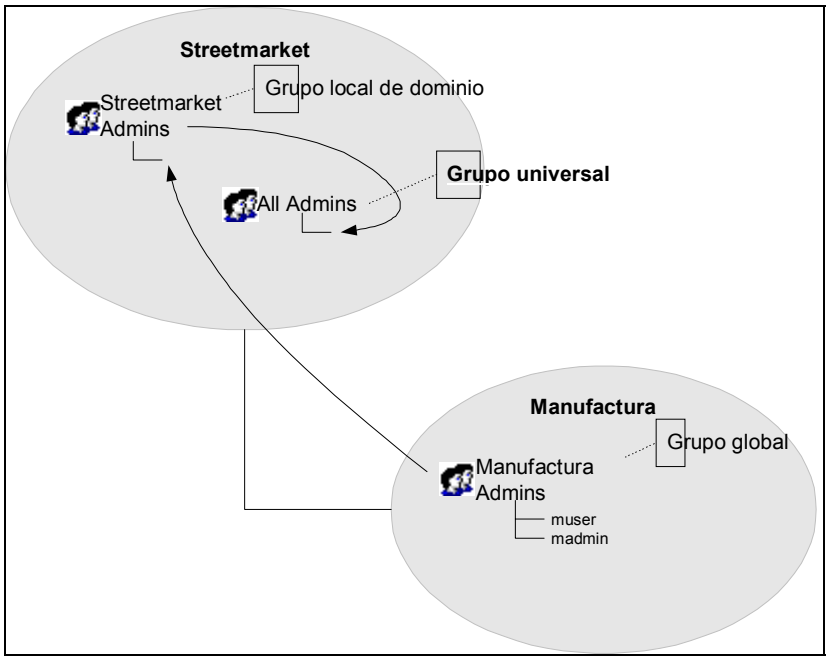
- Figura 39: Uso de grupo local de dominio

En la figura anterior, el grupo “Streetmarket Admins” se creó con la intención de tener una membresia global y permisos asignados a los recursos dentro del dominio de Streetmarket. Es efectivamente un grupo agregado que contiene grupos Globales desde los dominio menores. El grupo local de dominio “Streetmarket Admins” en este caso, puede accederse únicamente desde el dominio Streetmarket.

Grupos universales

Los grupos universales son muy similares a los grupos locales de dominio en el hecho de que pueden contener cuentas de usuarios, grupos universales y globales desde cualquier otro dominio. Sin embargo, los grupos universales también se pueden acceder desde cualquier dominio, haciéndolos muy flexibles.

Nuevamente, para utilizar los ejemplos anteriores, los grupos Universales podrían ser utilizados nuevamente para crear la estructura, pero ahora la estructura puede basarse en cualquier nivel, incluso dentro de su propio dominio.



■ Figura 40: Uso de grupo universal

En el ejemplo anterior, el grupo Universal contiene tanto los grupos locales globales como de dominio, pero se pueden acceder desde cualquier dominio. Además, es posible para el grupo universal “All Admins” estar contenido por otro grupo Universal ya creado en cualquiera de los dominios.

De igual forma, los grupos universales por si mismos pueden actuar como miembros de cualquier otro tipo de grupo, el cual proporciona un mecanismo para estructuras de grupo muy complejas.

Consideraciones de diseño

Los grupos de seguridad también pueden utilizarse como base para una administración de cuenta de usuario y seguridad distribuida. La planeación adecuada e implementación de grupos tendrá un papel en la disminución de los costos totales de administración de un sistema distribuido.

Mientras se enfoca en lo que ha sido el uso de grupos para asistir la administración de

recursos, los grupos también proporcionan un gran mecanismo para la administración de los mismos usuarios. La agrupación como la de los usuarios en clasificaciones para administración permitirá tareas pesadas como las distribución de software y aplicación de políticas para ser aplicadas en un orden rápido. Este aspecto de grupos se analizará más a fondo posteriormente en esta sección en planeación de política de grupo.

La siguiente información deberá ser útil en la planeación de grupos y políticas para grupos.

Un controlador de dominio requiere conocimiento global de sus membresias de grupo a fin de calcular todos los grupos (de manera directa o indirecta) contenidos en ellos. Con los grupos universales el DC utiliza el catálogo global para realizar este cálculo de membresia.

Debió a que DC utiliza GC para calcular sus membresías de grupo universales, el GC debe contener todas las membresias de grupos universales. Pero si todos los grupos son grupos universales, las membresias de grupo universal cambiarán con frecuencia, produciendo un alto nivel de tráfico de duplicación GC. Una sucursal mediana quizás no esté disponible para afrontar el ancho de banda de red que se requiere para mantener un GC actualizado.

Cuando usted se conecta un servidor de recurso con un controlador de dominio en su dominio de cuenta, calcula el conjunto de todos los grupos a que pertenecen que deben ser utilizados para controlar su acceso a su servidor de recurso. Esto incluye todos los grupos universales a los que pertenece. Típicamente, sólo una fracción de los grupos a los que pertenece será utilizada para acceder el control en cualquier servidor de recurso.

Local de dominio: Mientras hay divisiones, los grupos locales de dominio no se duplican como parte del NC de dominio, y por ende producen menos sobrecarga de duplicación.

Atributo	**Global**	**Local de dominio**	**Universal**
Membresia	Limitado	Abierto	Abierto
Puede contener	Usuario /Global	Usuario,Univ,Global	Usuario,Univ,Global
Asignación de permiso	Abierto	Limitado	Abierto
Anidación	Limitado	Limitado	Abierto
Puede actualizar	A universal	A universal	Ninguno

* **Membresia:** El enfoque de membresia (limitado = únicamente dominio local de objeto. Abierto = objetos desde cualquier dominio). **Puede contener :** Tipos de objetos que pueden ser miembros de este grupo. **Asignación de permisos:** El enfoque al que se puede acceder el dominio. (limitado = puede utilizarse únicamente en el dominio creado). **Anidación:** La capacidad del grupo para contener su propio tipo de grupos. (limitado = dentro de su dominio únicamente). **Puede actualizar:** la capacidad de un grupo para cambiar (actualizar) a un grupo diferente.

Restricciones de modo combinado

Mientras se opera en modo combinado, existen algunas restricciones relacionadas con la funcionalidad de grupo. Dichas restricciones por lo general se relacionan con el proveer compatibilidad de respaldo a Windows NT 4.0 y están asociadas con la anidación. En el modo combinado:

- Los grupos universales no existen como un grupo de seguridad.

- Los grupos globales pueden contener sólo cuentas y no pueden ser anidados.
- Los grupos Locales de dominio pueden contener cuentas y grupos globales, pero no pueden ser anidados.

Estas restricciones se eliminan tan pronto como el Dominio se convierte en modo natural.

Revisión

Entender las propiedades e implicaciones de los diversos tipos de grupos en Windows 2000 es esencial al planear su jerarquía administrativa y roles. Para la revisión, los grupos son unidades administrativas, y pueden ser Globales, Locales de dominio o Universales.

Los grupos locales pueden contener usuarios únicamente desde el dominio local, pero se pueden utilizar en cualquier parte. Asimismo, los grupos locales de dominio pueden contener miembros desde cualquier dominio, pero únicamente pueden utilizarse en el dominio en el que están creados. Los grupos universales pueden contener miembros desde cualquier dominio y utilizarse para asignar derechos de acceso a los recursos.

Debido a que utiliza grupos para administrar y reforzar sus políticas de seguridad de la organización, es necesario comprender por completo los grupos y asegurarse de que sus grupos estén bien planeados.