INTRODUCCIÓN AL WINDOWS NT

Windows NT 4 es uno de los componentes de Microsoft Back Office, un grupo de aplicaciones orientadas a la administración de negocios. Algunos de los componentes de Back Office son:

- Windows NT4 Server/Work station
- Servidor Proxy
- Base de datos SQL Server 7
- Internet explorer 5
- Office 2000
- Service Pack 4 ó 5

El sistema operativo Windows NT4 viene a competir directamente con UNIX, que hasta hoy es la mejor y mas estable solución para la mayoría de las necesidades multiusuario y multiproceso.

Se presenta en dos versiones que son Workstation y Server, que aunque ofrecen el mismo entorno gráfico de Windows 95, además proporcionan más servicios de conexión con otras redes como NetWare, y herramientas para trabajar con aplicaciones cliente/servidor distribuidas por toda una red.

También proporcionan servicios Web para el intercambio de información a través de Intranets, y mucho más. Por supuesto que ofrecen un entorno de trabajo más estable que Windows 95/98 ya que trabajan con un nuevo Kernel creado por los desarrolladores del sistema operativo VMS de IBM.

Básicamente la diferencia entre las dos versiones de Windows NT4 es que la versión Server cuenta con muchos más programas de servicios de red y herramientas de administración. Todo esto se comenta con mas detalle dentro de los capítulos siguientes.

Desafortunadamente Windows NT no es completamente plug and play, por lo que la configuración de algunos componentes de hardware no es tan sencilla como en Windows 95/98, pero esta situación quedará resuelta con la versión 5 de Windows NT. Mientras tanto aquí se encuentra información concisa y práctica de la versión actual.

1. PLAN DE AUDITORIA.

Windows NT puede seguir actividades específicas de los usuarios auditando sucesos de seguridad e incluyendo entradas en el registro de seguridad. Utilice el Plan de auditoría para determinar los tipos de suceso de seguridad que registrará.
Cuando se administren dominios, el Plan de auditoría afecta a los registros de seguridad del controlador del dominio y de todos los servidores en el dominio, ya que comparten el mismo plan de auditoría.

Cuando se administra un equipo con Windows NT Workstation o a Windows NT Server que no sea controlador de dominio, este plan solamente afecta al registro de seguridad del equipo.

Debido a que el registro de seguridad tiene un tamaño limitado, elija cuidadosamente los sucesos que desee auditar. El tamaño máximo del registro de seguridad se define en el Visor de sucesos. Las entradas del registro de seguridad se pueden examinar utilizando el Visor de sucesos.

1.1. Dominio.

Nombre del dominio o del equipo que se está administrando.

1.2. No auditar.

No se registrará ningún suceso en el registro de seguridad.

1.3. Auditar estos sucesos.

Se registrarán los sucesos seleccionados.

1.4. Correcto.

Si esta casilla de verificación está activada, se agregará una entrada en el registro de seguridad cuando un suceso del tipo seleccionado se lleve a cabo correctamente.

1.5. Erróneo.

Si esta casilla de verificación está activada, se agregará una entrada en el registro de seguridad cuando un suceso del tipo seleccionado no se pueda llevar a cabo o se haga incorrectamente.

1.6. Inicio y cierre de sesión.

Un usuario ha iniciado o cerrado una sesión o ha establecido una conexión de red.

1.7. Acceso a archivos y objetos.

Un usuario ha tenido acceso a un directorio o archivo cuya auditoría se ha establecido en el Administrador de archivos o a enviado un trabajo de impresión a una impresora cuya auditoría se ha establecido en el Administrador de impresión.

1.8. Uso de los derechos de usuario.

Un usuario ha utilizado un derecho, excluyendo los relacionados con el inicio y cierre de sesión.

1.9. Administración de usuarios y grupos.

Se ha creado, modificado o eliminado un grupo o cuenta de usuario Se ha desactivado, activado o cambiado el nombre de una cuenta de usuario; o bien se ha establecido o modificado una contraseña.

1.10. Cambios en el plan de seguridad.

Se ha modificado el plan de derechos de usuario o de auditoría.

1.11. Reinicio, apagado y sistema.

Un usuario ha reiniciado o apagado el sistema, o bien ha ocurrido un suceso que afecta a la seguridad del sistema o al registro de seguridad.

1.12. Seguimiento de procesos.

Estos sucesos proporcionan información de seguimiento detallada acerca de sucesos como activación de programas, algunas formas de duplicación de identificadores, acceso indirecto a objetos y salida de procesos.

2. PARA ADMINISTRAR EL PLAN DE AUDITORIA.

a.) Elija Auditoría en el menú Directivas.
b.) Para grabar sucesos en el registro de seguridad, seleccione Auditar estos sucesos. O para no registrar ningún suceso en el registro de seguridad, seleccione No auditar.
c.) Si ha seleccionado Auditar estos sucesos, especifique los sucesos que deberán auditarse, activando o desactivando las casillas Correcto y Erróneo para cada tipo de suceso.

2.1. Notas y sugerencias.

Cuando administra dominios, el Plan de auditoría afecta a la seguridad de los inicios de sesión de todos los controladores del dominio por que comparten el mismo Plan de auditoría.

Cuando administra un equipo que ejecuta Windows NT Workstation o Windows NT Server que no es un dominio, el Plan de auditoría solamente afecta a la seguridad del inicio de sesión en ese equipo.

Puede revisar las entradas de un registro de seguridad usando el Visor de sucesos.

Debido a que el registro de seguridad tiene un tamaño limitado, seleccione con cuidado los sucesos que quiere registrar. El tamaño máximo del registro de seguridad en cada equipo viene definido en el Visor de sucesos.

3. VISOR DE SUCESOS.

3.1. Introducción al Visor de sucesos.

El Visor de sucesos es la herramienta que puede utilizar para controlar los sucesos del sistema. Con el Visor de sucesos puede examinar y administrar registros de sucesos de Sistema, de Seguridad y de Aplicación. También puede archivar registros de sucesos.
El servicio de registro de sucesos se inicia automáticamente al ejecutar Windows NT. Puede detenerlo con la herramienta Servicios del Panel de control.

3.1.1. Origen.

Software que ha registrado el suceso. Puede tratarse de una aplicación o de un componente del sistema, por ejemplo un controlador.

3.1.2. Usuario.

Texto específico que coincide exactamente con el del campo Usuario. Este campo no distingue entre mayúsculas y minúsculas.

3.1.3. Categoría.

Clasificación del suceso, según lo define el origen.
Por ejemplo, las categorías de los registros de sucesos de seguridad son Inicio y cierre de sesión, Cambio de plan, Uso de privilegios, Suceso de sistema, Acceso a objetos, Seguimiento detallado y Administración de cuentas.

3.1.4. Equipo.

El nombre exacto del equipo en el que se ha producido el suceso registrado. Este campo no distingue entre mayúsculas y minúsculas.

3.1.5. Identificador.

Muestra un número que identifica un suceso específico.
El Identificador ayuda a los técnicos de soporte de producto a hacer un seguimiento de los sucesos del sistema.

3.1.6. Tipo.

Clasificación del suceso por parte del sistema operativo Windows NT dentro de categorías como Error, Advertencia, Información, Acceso correcto auditado o Acceso erróneo auditado.

3.2. Registros.

3.2.1. Sistema.

El Registro de sistema almacena los sucesos que registran los componentes del sistema Windows NT. Por ejemplo, un fallo al cargar un controlador de dispositivo u otro componente del sistema durante el inicio del equipo se registra en el Registro de sistema.

3.2.2. Seguridad.

El Registro de seguridad almacena los sucesos relacionados con la seguridad. Esto es útil para hacer un seguimiento de los cambios en el sistema de seguridad y detectar cualquier posible fallo en él. Por ejemplo, los intentos de iniciar una sesión en el sistema pueden almacenarse en el Registro de seguridad, dependiendo de la configuración de Auditoría en el Administrador de usuarios.
Solamente es posible examinar el Registro de seguridad si usted es Administrador del equipo.

3.2.3. Aplicación.

El Registro de aplicación almacena los sucesos que registran las aplicaciones. Por ejemplo, una aplicación de bases de datos puede agregar al Registro de Aplicación un error de archivo.

3.3. Suceso.

En el sistema operativo Windows NT, un suceso es cualquier acontecimiento significativo del sistema o de una aplicación que requiera una notificación al usuario. En el caso de sucesos críticos, como por ejemplo un servidor lleno o una interrupción de la alimentación eléctrica, puede ser que aparezca un mensaje en la pantalla. En el caso de muchos otros sucesos que no requieren atención inmediata, el sistema operativo Windows NT agrega información a un archivo de registro de sucesos sin interferir en el trabajo habitual de los usuarios. Este servicio de registro de sucesos comienza automáticamente cada vez que se inicia el equipo con Windows NT.

3.3.1. Origen.

Software que ha registrado el suceso. Puede tratarse de una aplicación o de un componente del sistema, por ejemplo un controlador.

3.3.2. Categoría.

Clasificación del suceso, según lo define el origen.
Por ejemplo, las categorías de los registros de sucesos de seguridad son Inicio y cierre de sesión, Cambio de plan, Uso de privilegios, Suceso de sistema, Acceso a objetos, Seguimiento detallado y Administración de cuentas.

3.3.3. Identificador.

Muestra un número que identifica un suceso específico.
El Identificador ayuda a los técnicos de soporte de producto a hacer un seguimiento de los sucesos del sistema.

3.3.4. Equipo.

El nombre exacto del equipo en el que se ha producido el suceso registrado. Este campo no distingue entre mayúsculas y minúsculas.

3.3.5. Usuario.

Texto específico que coincide exactamente con el del campo Usuario. Este campo no distingue entre mayúsculas y minúsculas.

3.3.6. Descripción

Texto que describe el suceso, creado por la causa u origen del propio suceso.
Puede elegir Buscar para localizar sucesos específicos indicando cualquier fragmento de su descripción. La descripción también se guarda en todos los registros archivados.

3.4. Configurar registros de sucesos

Puede utilizar el cuadro de diálogo Configurar registros de sucesos para definir el tamaño máximo del registro y las medidas que debe tomar Windows NT cuando un registro de sucesos está lleno.

3.4.1. Cambiar configuración del registro

Se utiliza para seleccionar el tipo de registro cuya configuración desea cambiar: Sucesos de sistema, Sucesos de seguridad o Sucesos de aplicación.

3.4.2. Máximo tamaño de registro

Se utiliza para especificar el tamaño máximo del archivo de registro. El tamaño máximo predeterminado es 512 KB.

Para cambiar el tamaño máximo, haga clic en las flechas hacia arriba o hacia abajo.

3.4.3. Sobrescribir sucesos cuando sea necesario.

Cuando esta opción está seleccionada, todos los sucesos nuevos se escriben en el registro, incluso cuando el registro está lleno. En este caso, cada nuevo suceso reemplazará al más antiguo.

Sugerencia: Esta opción es la mejor por su facilidad de mantenimiento y es la predeterminada.

3.4.4. Sobrescribir sucesos con más de [ ] días.

Cuando esta opción está seleccionada, cada registro se mantiene durante un número de días determinado antes de sobrescribirse. Es posible especificar el número de días que deben transcurrir para que un registro se sobrescriba indicando un número entre 1 y 365.

Sugerencia: El valor predeterminado de esta opción es 7 días. Este valor es el más adecuado si desea archivar los registros semanalmente.

3.4.5. No sobrescribir sucesos (borrado manual).

Cuando está seleccionada, esta opción conserva todos los sucesos existentes cuando el registro está lleno.
Esta opción requiere que usted borre manualmente el registro. Elíjala solamente si tiene que conservar todos los sucesos.

3.4.6. Predeterminada.

Restablece todas las opciones predeterminadas del registro seleccionado.

3.5. Qué hacer cuando un registro de sucesos está lleno

Para liberar un registro lleno (en el que no pueden registrarse más sucesos), elija Borrar todos los sucesos en el menú Registro.

También puede liberar el registro reduciendo el intervalo de conservación en el cuadro de diálogo Configurar registros de sucesos.

Nota: No es posible continuar registrando sucesos aumentando el tamaño máximo del registro. Para aumentar el tamaño del registro, primero hay que borrarlo, luego incrementar el tamaño en el cuadro de diálogo Configurar registros de sucesos y después reiniciar el sistema.

BIBLIOGRAFÍA

SHELDOM, Tom, "Manual de Seguridad de Windows NT", 1997, Osborne/McGraw – Hill

WYATT, Allen, "Aprendiendo Windows NT Server 4", 1997, Prentice Hall Hispanoamericana