Escuela Colombiana de Ingeniería Julio Garavito

Arquitectura Computacional y Sistemas Operativos 2025-1

Hoja de Respuestas Windows Server

Andersson David Sánchez Méndez

16 de febrero de 2025

- **¿Cómo se manejan permisos en Windows server?**

  Los permisos en Windows Server se basan en el control de acceso a recursos como archivos, carpetas, impresoras, servicios y aplicaciones. Estos permisos se asignan a usuarios o grupos y se gestionan mediante herramientas como:

  - **Active Directory (AD):** Para gestionar usuarios, grupos y permisos a nivel de dominio.
  - **Explorador de Archivos:** Para asignar permisos a nivel de archivos y carpetas.
  - **Directivas de Grupo (GPO):** Para aplicar políticas de seguridad y permisos de manera centralizada.

---

2. Tipos de Permisos

1. **Permisos NTFS:** Se aplican a archivos y carpetas en particiones NTFS. Incluyen:
   - **Control total:** Permite leer, escribir, modificar y eliminar archivos.
   - **Modificar:** Permite leer, escribir y eliminar archivos.
   - **Lectura y ejecución:** Permite leer y ejecutar archivos.
   - **Listar contenido:** Permite ver el contenido de una carpeta.
   - **Lectura:** Permite ver archivos y carpetas.
   - **Escritura:** Permite crear y modificar archivos.
2. **Permisos de recurso compartido:** Se aplican a carpetas compartidas en la red. Incluyen:
   - **Lectura:** Permite ver archivos.
   - **Cambiar:** Permite leer, escribir y eliminar archivos.
   - **Control total:** Permite realizar cualquier acción.

---

3. Asignación de Permisos

3.1. Permisos NTFS

Para asignar permisos NTFS:

1. Abre el Explorador de Archivos.
2. Haz clic derecho sobre el archivo o carpeta y selecciona Propiedades.

3. Ve a la pestaña Seguridad.
4. Haz clic en Editar para modificar los permisos existentes o en Agregar para incluir nuevos usuarios o grupos.
5. Selecciona el usuario o grupo y asigna los permisos necesarios.

3.2. Permisos de Recurso Compartido

Para asignar permisos de recurso compartido:

1. Abre el Administrador del Servidor.
2. Ve a Herramientas > Administración de equipos.
3. Selecciona Carpetas compartidas y elige la carpeta que deseas compartir.
4. Haz clic derecho y selecciona Propiedades.
5. En la pestaña Compartir, haz clic en Permisos de uso compartido avanzado.
6. Asigna los permisos necesarios.

---

4. Herramientas para Gestionar Permisos

4.1. Active Directory (AD)

Active Directory es la herramienta principal para gestionar usuarios, grupos y permisos en un dominio. Permite:

- Crear y gestionar usuarios y grupos.
- Asignar permisos a nivel de dominio.
- Aplicar directivas de grupo.

4.2. PowerShell

PowerShell es una herramienta avanzada para automatizar la gestión de permisos. Algunos cmdlets útiles incluyen:

- **Get-ACL:** Obtiene los permisos de un archivo o carpeta.
- **Set-ACL:** Modifica los permisos de un archivo o carpeta.
- **New-ADUser:** Crea un nuevo usuario en Active Directory.
- **Add-ADGroupMember:** Agrega un usuario a un grupo.

4.3. Directivas de Grupo (GPO)

Las directivas de grupo permiten aplicar permisos y configuraciones de seguridad de manera centralizada. Por ejemplo:

- Restringir el acceso a ciertas carpetas.
- Limitar el uso de dispositivos USB.
- Forzar el cambio de contraseñas periódicamente.

---

5. Buenas Prácticas para la Gestión de Permisos

1. **Principio de menor privilegio:** Asigna solo los permisos necesarios para que los usuarios realicen sus tareas.
2. **Uso de grupos:** En lugar de asignar permisos a usuarios individuales, utiliza grupos para simplificar la administración.
3. **Auditorías periódicas:** Revisa regularmente los permisos asignados para evitar accesos no autorizados.
4. **Documentación:** Mantén un registro de los permisos asignados y los cambios realizados.
5. **Capacitación:** Asegúrate de que los administradores estén capacitados en la gestión de permisos y seguridad.

---

6. Auditoría de Permisos

Windows Server incluye herramientas para auditar el acceso a recursos:

1. **Auditoría de Acceso a Archivos y Carpetas:**
    - Abre el Explorador de Archivos.
    - Haz clic derecho sobre el archivo o carpeta y selecciona Propiedades.
    - Ve a la pestaña Seguridad y haz clic en Auditoría.
    - Configura las acciones que deseas auditar (lectura, escritura, etc.).

2. **Event Viewer (Visor de Eventos):**
    - Abre el Visor de Eventos desde el Administrador del Servidor.
    - Revisa los registros de seguridad para ver eventos relacionados con el acceso a recursos.

---

7. Recuperación de Permisos

Si los permisos se configuran incorrectamente, puedes restaurarlos utilizando:

- Copia de seguridad de permisos: Utiliza herramientas como icacls o Set-ACL para guardar y restaurar permisos.
- Restauración del sistema: Si los cambios afectan el sistema, puedes usar un punto de restauración para revertir los cambios.

- **¿Cuál es la estructura de directorios de Windows server?**

1. Directorios Principales del Sistema

Estas son las carpetas principales que forman parte del sistema operativo y son comunes en todas las instalaciones de Windows Server:

1.1. C:\Windows

Es la carpeta principal del sistema operativo. Contiene todos los archivos necesarios para el funcionamiento de Windows Server. Algunas subcarpetas importantes incluyen:

- **System32**: Contiene archivos críticos del sistema, como DLLs (bibliotecas de enlace dinámico) y ejecutables.
- **SysWOW64**: En sistemas de 64 bits, almacena archivos de 32 bits para compatibilidad.
- **Temp**: Almacena archivos temporales generados por el sistema y las aplicaciones.
- **Logs**: Contiene archivos de registro (logs) del sistema.
- **Fonts**: Almacena las fuentes instaladas en el sistema.

1.2. C:\Program Files

Contiene los archivos de las aplicaciones instaladas en el servidor. En sistemas de 64 bits, también existe:

- **C:\Program Files (x86)**: Almacena aplicaciones de 32 bits.

1.3. C:\Users

Contiene los perfiles de los usuarios del sistema. Cada usuario tiene una carpeta personal con su nombre, donde se almacenan documentos, descargas, escritorio, etc. Las subcarpetas comunes incluyen:

- **Desktop**: Archivos del escritorio del usuario.
- **Documents**: Documentos personales.
- **Downloads**: Archivos descargados.
- **AppData**: Datos de configuración de aplicaciones (oculta por defecto).

1.4. C:\ProgramData

Almacena datos compartidos entre aplicaciones y usuarios. Es una carpeta oculta que contiene configuraciones globales y datos de programas.

1.5. C:\PerfLogs

Contiene registros de rendimiento generados por herramientas como el **Monitor de Rendimiento**.

1.6. C:\inetpub

Es la carpeta predeterminada para el servidor web **IIS (Internet Information Services)**. Contiene subcarpetas como:

- **wwwroot**: Raíz del sitio web, donde se almacenan los archivos web.
- **logs**: Registros de acceso y errores del servidor web.

---

2. Directorios Relacionados con Active Directory

Si el servidor está configurado como un controlador de dominio, existen carpetas adicionales relacionadas con Active Directory:

2.1. C:\Windows\NTDS

Contiene la base de datos de Active Directory (ntds.dit) y los archivos de registro asociados.

2.2. C:\Windows\SYSVOL

Almacena scripts, plantillas y objetos de directiva de grupo (GPO) que se replican entre controladores de dominio.

---

3. Directorios de Aplicaciones y Servicios

Dependiendo de los roles y características instalados en el servidor, pueden existir carpetas adicionales:

3.1. C:\Windows\System32\config

Contiene los archivos de configuración del registro de Windows.

3.2. C:\Windows\SoftwareDistribution

Almacena archivos relacionados con Windows Update.

3.3. C:\Windows\WinSxS

Contiene componentes del sistema y versiones de bibliotecas para garantizar la compatibilidad.

---

4. Directorios Personalizados

Además de las carpetas del sistema, es común crear directorios personalizados para organizar datos y aplicaciones. Por ejemplo:

- **C:\Data**: Para almacenar archivos de datos compartidos.
- **C:\Backups**: Para almacenar copias de seguridad.
- **C:\Scripts**: Para almacenar scripts de PowerShell o batch.

---

5. Estructura de Discos y Particiones

En Windows Server, es común utilizar múltiples discos y particiones para organizar los datos. Por ejemplo:

- **C:**: Partición del sistema operativo.
- **D:**: Partición para datos o aplicaciones.
- **E:**: Partición para copias de seguridad.

---

6. Herramientas para Explorar la Estructura de Directorios

- **Explorador de Archivos**: Para navegar manualmente por la estructura de directorios.
- **PowerShell**: Para listar y gestionar directorios mediante comandos como Get-ChildItem.
- **Administrador del Servidor**: Para gestionar roles y características que pueden crear directorios adicionales.

Bibliografía

- https://mundowin.com/permisos-de-usuario-en-windows-server/
- https://learn.microsoft.com/es-es/troubleshoot/windows-server/windows-security/grant-users-rights-manage-services
- https://mundowin.com/guia-completa-para-administrar-windows-server/