

# Comando de montaje

Última actualización: 2023-07-17

## Objetivo [↗](#)

Hace que un sistema de archivos esté disponible para su uso.

## Sintaxis [↗](#)

```
mount [ -f ] [ -n node ] [ -o options ] [ -p ] [ -r ] [ -v vfsname ] [ -F AltFSfile ] [ -t type ] [ device | node:directory ] directory | all | -a ] [ -V [generic_options] special_mount_points ]
```

## Description [↗](#)

The **mount** command instructs the operating system to make a file system available for use at a specified location (the mount point). In addition, you can use the **mount** command to build other file trees made up of directory and file mounts. The **mount** command mounts a file system expressed as a device using the *device* or *node:directory* parameter on the directory specified by the *directory* parameter. After the **mount** command has finished, the directory specified becomes the root directory of the newly mounted file system.

Solo los usuarios con autorización de raíz o miembros del grupo del sistema y que tengan acceso de escritura al punto de montaje pueden realizar montajes de archivos o directorios. El archivo o directorio puede ser un enlace simbólico. El comando **de montaje** utiliza el ID de usuario real, no el ID de usuario efectivo, para determinar si el usuario tiene el acceso adecuado. Los miembros del grupo del sistema pueden emitir montajes de dispositivos, siempre que tengan acceso de escritura al punto de montaje y a los montajes especificados en el archivo **/etc/filesystems** . Los usuarios con autoridad de usuario raíz pueden emitir cualquier comando **de montaje** .

Los usuarios pueden montar un dispositivo siempre que pertenezcan al grupo del sistema y tengan el acceso adecuado. Al montar un dispositivo, el comando **de montaje** utiliza el parámetro *de dispositivo* como el nombre del dispositivo de bloque y el parámetro *de directorio* como el directorio en el que montar el sistema de archivos.

Si ingresa el comando **de montaje** sin marcas, el comando muestra la siguiente información para los sistemas de archivos montados:

- el nodo (si el montaje es remoto)
- el objeto montado
- el punto de montaje

- el tipo de sistema de archivos virtual
- el tiempo montado
- cualquier opción de montaje

Si especifica solo el *directorio* o *nodo* : parámetro de *directorio* , el comando **de montaje** lo toma como el nombre del directorio o archivo en el que normalmente se monta un sistema de archivos, directorio o archivo (como se define en el archivo `/etc/filesystems` ) . El comando **de montaje** busca el dispositivo, directorio o archivo asociado y lo monta. Esta es la forma más conveniente de usar el comando **de montaje** , porque no requiere que recuerde lo que normalmente se monta en un directorio o archivo. También puede especificar solo el dispositivo. En este caso, el comando obtiene el punto de montaje del archivo `/etc/filesystems` .

The `/etc/filesystems` file should include a stanza for each mountable file system, directory, or file. This stanza should specify at least the name of the file system and either the device on which it resides or the directory name. If the stanza includes a mount attribute, the **mount** command uses the associated values. It recognizes five values for the mount attributes: **automatic**, **true**, **false**, **removable**, and **readonly**.

The **mount all** command causes all file systems with the **mount=true** attribute to be mounted in their normal places. This command is typically used during system initialization, and the corresponding mount operations are referred to as automatic mount operations.

By default, the **mount** command runs the **wlmcntrl** command to refresh the current assignment rules in the kernel after mounting the file system. In some situations (such as when many file systems are mounted at once, or when a rule for an inaccessible remote mount is present in the workload manager configuration), calling **wlmcntrl** automatically after mount might be undesirable.

If you wish to override this behavior, set the environment variable `MOUNT_WLMCNTRL_SELFMANAGE` to any value. This will avoid calling the **wlmcntrl** command during the mount operation. You must manually run `wlmcntrl -u -d ""` to refresh the current assignment rules in the kernel. For more information, see [wlmcntrl command](#).

#### **Note:**

1. If the **cdromd** CD and DVD **automount** daemon is enabled, those devices will be automatically mounted as specified in the `/etc/cdromd.conf` file. Use the **cdumount** or **cdeject** command to unmount an automatically mounted CD or DVD. Use **stopsrc -s cdromd** to disable the CD/DVD **automount** daemon.
2. For CacheFS, the remote file system that is to be cached locally must be exported such that the root ID of the local system is not remapped on the remote host to nobody (or the ID that the remote host uses as the anonymous user). For example, if host A were to export a file system **/F**, which would be mounted with CacheFS on host B, then the `/etc/exports` on host A would need to have an entry similar to:

```
/F -rw,root=B  
or  
/F -ro,root=B
```



depending on the mount options used for the local CacheFS mount.

3. Mounting a JFS file system on a read-only logical volume is not supported.
4. Mounting a JFS2 file system with EAv1 on Trusted AIX® system converts the file system to EAv2.

## Using mount on a JFS2 File System

The **mount** command can also be used to access a snapshot of a JFS2 file system as a directory tree. The snapshot on *device* is mounted read-only at *directory*. A snapshot can only be mounted once. When mounting a JFS2 file system with snapshots, the snapshots are activated.

You can use the System Management Interface Tool (SMIT) **smit mount** fast path to run this command.

**Note:** If the **mount** command encounters a Journaled File System (JFS) or Enhanced Journaled File System (JFS2) which was not unmounted before reboot, a replay of any JFS or JFS2 log records is attempted. In order to move a compatible JFS file system to a system running an earlier release of the operating system, the file system must always be unmounted cleanly prior to its movement. Failure to unmount first may result in an incompatible JFS log device. If the movement results in an unknown log device, the file system should be returned to the system running the latter operating system release, and **fsck** should be run on the file system.

## Flags [↗](#)


Item	Description
<b>-a</b>	Mounts all file systems in the <b>/etc/filesystems</b> file with stanzas that contain the <b>true</b> mount attribute.
<b>all</b>	Same as the <b>-a</b> flag.
<b>-f</b>	Requests a forced mount during system initialization to enable mounting over the root file system.
<b>-F</b> <i>AltFSfile</i>	Mounts on a file of an alternate file system, other than the <b>/etc/filesystems</b> file.

Item	Description
<b>-n</b> <i>node</i>	Specifies the remote node that holds the directory to be mounted. The node can be specified as a colon-separated IPv6 address. If this is done with the <code>node:directory</code> format, the colon-separated IPv6 address must be enclosed in square brackets.
<b>-p</b>	Mounts a file system as a removable file system. While open files are on it, a removable mounted file system behaves the same as a normally mounted file system. However, when no files are open (and no process has a current directory on the file system), all of the file system disk buffers in the file system are written to the medium, and the operating system forgets the structure of the file system.
<b>-r</b>	Mounts a file system as a read-only file system, regardless of its previous specification in the <code>/etc/filesystems</code> file or any previous command-line options.
<b>-t</b> <i>type</i>	Mounts all stanzas in the <code>/etc/filesystems</code> file that contain the <b>type=type</b> attribute and are not mounted. The <i>type</i> parameter specifies the name of the group.
<b>-v</b> <i>vfsname</i>	Specifies that the file system is defined by the <i>vfsname</i> parameter in the <code>/etc/vfs</code> file.

## File System Specific Options

Item	Description
<b>-o</b> <i>options</i>	<p>Specifies options. Options entered on the command line should be separated only by a comma. The following file system-specific options do not apply to all virtual file system types:</p> <p><b>atime</b></p> <p>Turns on access-time updates. If neither <b>atime</b> nor <b>noatime</b> is specified, <b>atime</b> is the default value.</p> <p><b>bsy</b></p> <p>Prevents the mount operation if the directory to be mounted over is the current working directory of a process.</p>
	<p><b>cio</b></p> <p>Specifies the file system to be mounted for concurrent readers and writers. I/O on files in this file system will behave as if they had been opened with <b>O_CIO</b> specified in the <b>open()</b> system call. Using this option will prevent access in any manner other than CIO. It is impossible to use cached I/O on a file system mounted with the <b>cio</b> option. This means that mapping commands such as <b>mmap()</b> and <b>shmat()</b> will fail with EINVAL when used on any file in a file system</p>

Item	Description
	<p>mounted with the <b>cio</b> option. One side-effect of this is that it is impossible to run binaries out of a <b>cio</b> mounted file system, since the loader may use <b>mmap()</b>.</p> <div> <p><b>i</b> <b>Note:</b> When you mount the file system by using the <b>cio</b> option, all applications must manage the serialization of files. Quotas are not supported by the <b>cio</b> option because quotas have their own serialization code.</p> </div>
	<p><b>dev</b></p> <p>Specifies that you can open devices from this mount. If neither <b>dev</b> nor <b>nodev</b> is specified, <b>dev</b> is the default value.</p> <p><b>dio</b></p> <p>Specifies that I/O on the file system will behave as if all the files had been opened with <b>O_DIRECT</b> specified in the <b>open()</b> system call.</p> <div> <p><b>i</b> <b>Note:</b> Using the <b>-odio</b> or <b>-ocio</b> flags can help performance on certain workloads, but users should be aware that using these flags will prevent file caching for these file systems. Because readahead is disabled for these file systems, this may decrease performance for large sequential reads.</p> </div>
	<p><b>fmode=octal</b></p> <p>Specifies the mode for a file and directory. The default is 755.</p>
	<p><b>gid=gid</b></p> <p>Specifies the GID that is assigned to files in the mount. The default is <b>bin</b>.</p>
	<p><b>log=lvname</b></p> <p>Specifies the full path name of the file system logging logical volume name where the following file-system operations are logged.</p>
	<p><b>log=NULL</b></p> <p>Turns off logging and flushing of metadata for JFS2 file systems. Metadata is not flushed to the disk until the file system is unmounted. If the system stops abnormally before the file system is unmounted, the metadata changes are lost.</p> <p>The JFS2 file system depends on the log information for metadata consistency. If the system stops abnormally during the metadata flush process for the JFS2</p>

Item	Description
	<p>file system when the unmount operation is in progress, the file system cannot be recovered to a consistent state upon system reboot. In this case, the file system must be re-created.</p> <div>  <b>Attention:</b> Because of the risk of data loss, use this flag with caution. </div>
	<p><b>maxpout=value</b></p> <p>Specifies the pageout level for files on this file system at which threads should be slept. If <b>maxpout</b> is specified, <b>minpout</b> must also be specified. Value must be non-negative and greater than <b>minpout</b>. The default is the kernel <b>maxpout</b> level.</p>
	<p><b>minpout=value</b></p> <p>Specifies the pageout level for files on this file system at which threads should be readied. If <b>minpout</b> is specified, <b>maxpout</b> must also be specified. Value must be non-negative. The default is the kernel <b>minpout</b> level.</p>
	<p><b>noatime</b></p> <p>Turns off access-time updates. Using this option can improve performance on file systems where a large number of files are read frequently and seldom updated. If you use the option, the last access time for a file cannot be determined. If neither <b>atime</b> nor <b>noatime</b> is specified, <b>atime</b> is the default value.</p>
	<p><b>nocase</b></p> <p>Turns-off case mapping. This is useful for CDRoms using the ISO 9660:1998/HSG standard.</p>
	<p><b>nodev</b></p> <p>Specifies that you cannot open devices from this mount. This option returns a value of <b>ENXIO</b> if a failure occurs. If neither <b>dev</b> nor <b>nodev</b> is specified, <b>dev</b> is the default value.</p>
	<p><b>noguard</b></p> <p>Mount the filesystem regardless of the current mountguard setting which would otherwise guard the filesystem against unsupported concurrent mounts in a PowerHA® or other clustering environment. If mountguard is enabled by the</p>

Item	Description
	<b>chfs</b> or <b>crfs</b> command, the filesystem cannot be mounted if it appears to be mounted on another node or system. Specifying the <b>noguard</b> option temporarily overrides the <b>mountguard</b> setting.
	<b>norbr</b> Mounts the file system without the release-behind-when-reading capability. If none of the release-behind options are specified, <b>norbrw</b> is the default value.
	<b>norbrw</b> Mounts the file system without both the release-behind-when-reading and release-behind-when-writing capabilities. If none of the release-behind options are specified, <b>norbrw</b> is the default value.
	<b>norbw</b> Mounts the file system without the release-behind-when-writing capability. If none of the release-behind options are specified, <b>norbrw</b> is the default value.
	<b>nosuid</b> Specifies that execution of <b>setuid</b> and <b>setgid</b> programs by way of this mount is not allowed. This option returns a value of <b>EPERM</b> if a failure occurs. If neither <b>suid</b> nor <b>nosuid</b> is specified, <b>suid</b> is the default value.
	<b>rbr</b> Mount file system with the release-behind-when-reading capability. When sequential reading of a file in this file system is detected, the real memory pages used by the file will be released once the pages are copied to internal buffers. If none of the release-behind options are specified, <b>norbrw</b> is the default. <div> <i>i</i> <b>Note:</b> When <b>rbr</b> is specified, the <b>D_RB_READ</b> flag is ultimately set in the <b>_devflags</b> field in the <b>pdentry</b> structure. </div>
	<b>rbw</b> Mount file system with the release-behind-when-writing capability. When sequential writing of a file in this file system is detected, the real memory pages used by the file will be released once the pages written to disk. If none of the release-behind options are specified, <b>norbrw</b> is the default.

Item	Description
	<div> <i>i</i> <b>Note:</b> When <b>rbw</b> is specified, the <b>D_RB_WRITE</b> flag is set. </div>
	<p><b>rbrw</b></p> <p>Mount file system with both release-behind-when-reading and release-behind-when-writing capabilities. If none of the release-behind options are specified, <b>norbrw</b> is the default.</p> <div> <i>i</i> <b>Note:</b> If <b>rbrw</b> is specified, both the <b>D_RB_READ</b> and the <b>D_RB_WRITE</b> flags are set. </div>
	<p><b>remount</b></p> <p>Changes the mount options of a mounted file system. For JFS2 file systems, you can specify the following mount options with the remount option to change the settings of a mounted file system. For any mount options not specified, no change is made to the current corresponding settings of the file system.  <b>atime, noatime; dev, nodev; maxpout, minpout; rbr, norbr; rbw, norbw; rbrw, norbrw, rw, ro, rox; suid, nosuid.</b></p> <div> <i>i</i> <b>Note:</b> <ol style="list-style-type: none"> <li>External-snapshot mounted file systems cannot be remounted to read-write file systems.</li> <li>You cannot use the <b>rw</b> and <b>ro</b> remount options on a file system that is managed by data management application programming interface (DMAPI).</li> </ol> </div> <p>For NFS, there are three types of mount requests.</p> <p><b>duplicate mount</b></p> <p>If the node, object, mount point, and the options that are specified in the <b>mount</b> command are the same as those for an existing mount, the <b>mount</b> command returns information about a successful mount, but a new mount is not created.</p> <p><b>new mount</b></p> <p>If the remount option is not specified, the <b>mount</b> command creates a new mount. If the node, object, mount point, or the constant options that are</p>



Item	Description
	<p>specified in the <b>mount</b> command are different than those for the existing mounts, the <b>mount</b> command fails if the remount option is specified.</p> <p><b>remount</b></p> <p>If the node, object, and mount point are the same as those for a top-most mount, but the remount options are different, the remount operation modifies the mount options of an existing mount. In this case, NFS performs the remount operation.</p> <p>A top-most mount does not have another mount on top of it. For remount requests, the following options can be modified: <b>acdirmax</b>, <b>acdirmin</b>, <b>acregmax</b>, <b>acregmin</b>, <b>actimeo</b>, <b>fastattr</b>, <b>grpuid</b>, <b>hard</b>, <b>intr</b>, <b>noac</b>, <b>nocto</b>, <b>nodev</b>, <b>nointr</b>, <b>nosuid</b>, <b>posix</b>, <b>retrans</b>, <b>ro</b>, <b>rsize</b>, <b>rw</b>, <b>secure</b>, <b>sec</b>, <b>soft</b>, <b>timeo</b>, <b>wsize</b>, <b>biods</b>, <b>extraattr</b>, <b>nodircache</b>, <b>prefer</b>, <b>otwattr</b>, <b>maxgroups</b>, and <b>proto</b>. Other options are classified as constant options.</p>
	<p><b>ro</b></p> <p>Specifies that the mounted file is read-only, regardless of its previous option specification in the <b>/etc/filesystems</b> file or any previous command-line options. The default value is <b>rw</b>.</p>
	<p><b>rw</b></p> <p>Specifies that the mounted file is read/write accessible, regardless of its previous option specification in the <b>/etc/filesystems</b> file or any previous command-line options. The default value is <b>rw</b>.</p>
	<p><b>snapshot</b></p> <p>Specifies the <i>device</i> to be mounted is a snapshot. The snapped file system for the specified snapshot must already be mounted or an error message will display.</p>
	<p><b>snapto=snapshot</b></p> <p>Specifies the location to start a snapshot with the value of <i>snapshot</i> when mounting the specified JFS2 file system. The <i>snapshot</i> parameter specifies the name of an internal snapshot if the <i>snapshot</i> parameter does not included a forward slash (/), that is, no path information.</p>
	<p><b>suid</b></p> <p>Specifies that execution of <b>setuid</b> and <b>setgid</b> programs by way of this mount is allowed. If neither <b>suid</b> nor <b>nosuid</b> is specified, <b>suid</b> is the default value.</p>

Item	Description
	<b>upcase</b> Changes case mapping from default lowercase to uppercase. This is useful for CDROMs using the ISO 9660:1998/HSG standard.
	<b>uid=uid</b> Specifies the UID that is assigned to files in the mount, the default is bin.
	<b>wrkgrp=workgroup</b> Specifies the workgroup that the SMB server belongs.

## NFS Specific Options

Item	Description
<b>-o options</b>	Specifies options. Options you enter on the command line should be separated only by a comma, not a comma and a space. The following NFS-specific options do not apply to all virtual file system types:
	<b>acdirmax=<i>n</i></b> Holds cached attributes for no more than <i>n</i> seconds after directory update. The default is 60 seconds.
	<b>acdirmin=<i>n</i></b> Holds cached attributes for at least <i>n</i> seconds after directory update. The default is 30 seconds.
	<b>acl</b> Requests using the Access Control List RPC program for this NFS mount. If the <b>acl</b> option is used, the ACL RPC program is used only if the NFS server provides it. The default is <b>noacl</b> .
	<b>acregmax=<i>n</i></b> Holds cached attributes for no longer that <i>n</i> seconds after file modification. The default is 60 seconds.
	<b>acregmin=<i>n</i></b> Holds cached attributes for at least <i>n</i> seconds after file modification. The default is 30 seconds.
	<b>actimeo=<i>n</i></b>

Item	Description
	Sets minimum and maximum times for regular files and directories to <i>n</i> seconds. If this option is set, it overrides any settings for the <b>acregmin</b> , <b>acregmax</b> , <b>acdirmin</b> , and <b>acdirmax</b> options.
<b>bg</b>	Attempts mount in background if first attempt is unsuccessful. The default value is <b>fg</b> .
<b>biops=<i>n</i></b>	Sets the maximum number of <b>biops</b> threads that perform asynchronous I/O RPC requests for an NFS mount. The maximum value that can be set is 128. Values greater than 128 are limited to 128 within the NFS client. The NFS client dynamically manages the number of running <b>biops</b> threads up to the maximum based on activity. The default maximums for the different NFS protocols are 7 for NFS version 2 and 32 for NFS version 3 and NFS version 4. These defaults are subject to change in future releases.
<b>cio</b>	<p>Specifies the file system to be mounted for concurrent readers and writers. I/O on files in this file system will behave as if they had been opened with <b>O_CIO</b> specified in the <b>open()</b> system call. Using this option will prevent access in any manner other than CIO. It is impossible to use cached I/O on a file system mounted with the <b>cio</b> option. This means that mapping commands such as <b>mmap()</b> and <b>shmat()</b> will fail with EINVAL when used on any file in a file system mounted with the <b>cio</b> option. One side-effect of this is that it is impossible to run binaries out of a <b>cio</b> mounted file system, since the loader may use <b>mmap()</b>.</p> <div> <p><b>Note:</b> When you mount the file system by using the <b>cio</b> option, all applications must manage the serialization of files. Quotas are not supported by the <b>cio</b> option because quotas have their own serialization code.</p> </div>
<b>cior</b>	<p>Specifies to allow read-only files to open in the file system. I/O on files in this file system will behave as if they had been opened with <b>O_CIO   O_CIOR</b> specified in the <b>open()</b> system call. Using this option will prevent access in any manner other than <b>O_CIO   O_CIOR</b> and read-only. An attempt to open with <b>O_CIO</b> only will also fail. This option can only be used in conjunction with <b>cio</b>.</p>

Item	Description
	<p>Specifies that I/O on the file system will behave as if all the files had been opened with <b>O_DIRECT</b> specified in the <b>open()</b> system call.</p> <div> <p><b>i</b> <b>Note:</b> Using the <b>-odio</b> or <b>-ocio</b> flags can help performance on certain workloads, but users should be aware that using these flags will prevent file caching for these file systems. Because readahead is disabled for these file systems, this may decrease performance for large sequential reads.</p> </div>
	<p><b>fastattr</b></p> <p>Bypasses the requirement that files currently being written will be sent to the server before the attributes of the file is read. This option is to be used with caution, since it will cause the client to assume that the file data that has not yet reached the server will be written without problem. In case of write errors, the client and server will have different opinions on what the size of the file really is. Likewise, a client will not be aware of attribute changes to the file being made by another client, so this option must not be used in environments where two clients are writing to the same files.</p>
	<p><b>fg</b></p> <p>Attempts mount in foreground if first attempt is unsuccessful. <b>fg</b> is the default value.</p>
	<p><b>grpidd</b></p> <p>Directs any file or directory created on the file system to inherit the group ID of the parent directory.</p>
	<p><b>hard</b></p> <p>Retries a request until server responds. The option is the default value.</p>
	<p><b>intr</b></p> <p>Allows keyboard interrupts on hard mounts.</p>
	<p><b>llock</b></p> <p>Requests that files lock locally at the NFS client. NFS network file locking requests are not sent to the NFS server if the <b>llock</b> option is used.</p>
	<p><b>maxgroups=<i>n</i></b></p>

Item	Description
	<p>Indicates that NFS RPC calls using <b>AUTH_UNIX</b> may include up to <i>n</i> member groups of information. Using this option to increase the number of member groups beyond the RPC protocol standard of 16 will only work against servers that support more than 16 member groups. Otherwise, the client will experience errors.</p> <p>Values below 16 or greater than 64 will be ignored. By default, the protocol standard maximum of 16 is adhered to. AIX NFS servers will accept and process <b>AUTH_UNIX</b> credentials with up to 64 groups starting with AIX 5L Version 5.2 with the 5200-01 Recommended Maintenance package. The actual number of member groups sent by the NFS client is dependent on the number of groups the involved user is a member of, and may be limited by the length of the NFS client's hostname (which is included in the <b>AUTH_UNIX</b> information).</p>
	<p><b>noac</b></p> <p>Specifies that the <b>mount</b> command performs no attribute or directory caching. If you do not specify this option, the attributes (including permissions, size, and timestamps) for files and directories are cached to reduce the need to perform over-the-wire <b>NFSPROC_GETATTR</b> Remote Procedure Calls (RPCs). The <b>NFSPROC_GETATTR</b> RPC enables a client to prompt the server for file and directory attributes. The <b>acregmin</b>, <b>acregmax</b>, <b>acdirmin</b>, and <b>acdirmax</b> options control the length of time for which the cached values are retained.</p>
	<p><b>noacl</b></p> <p>Specifies not to use the Access Control List RPC program for this NFS mount request. The default is <b>noacl</b>.</p>
	<p><b>nointr</b></p> <p>Specifies no keyboard interrupts allowed on hard mounts.</p>
	<p><b>port=<i>n</i></b></p> <p>Sets server Internet Protocol (IP) port number to <i>n</i>. The default value is the 2049.</p>
	<p><b>posix</b></p> <p>Requests that pathconf information be exchanged and made available on an NFS Version 2 mount. Requires a mount Version 2 <b>rpc.mountd</b> at the NFS server.</p>
	<p><b>proto=[udp tcp]</b></p>

Item	Description
	<p>Specifies the transport protocol. The default is <b>tcp</b>. Use the <b>proto=[udp tcp]</b> option to override the default.</p> <p><b>proto=udp</b> cannot be specified if <b>vers=4</b>.</p>
	<p><b>retrans=<i>n</i></b></p> <p>Sets the number of NFS transmissions to <i>n</i>. The default value is 5. The <b>retrans</b> setting determines how many times the NFS client retransmits a given UDP RPC request to an NFS server for file system operations. The <b>retrans</b> setting is not used during communication with the NFS server <b>rpc.mountd</b> service when processing NFS version 2 and 3 mounts. Retries to <b>rpc.mountd</b> are controlled with the <b>retry mount</b> option.</p>
	<p><b>retry=<i>n</i></b></p> <p>Sets the number of times the mount is attempted to <i>n</i>; the default value is 1000. When the retry value is 0, the system makes 10,000 attempts.</p>
	<p><b>rsize=<i>n</i></b></p> <p>Sets the read buffer size to <i>n</i> bytes. Beginning with AIX Version 6.1, the default value is 64 KB and the maximum value is 512 KB when using Version 3 and Version 4 of the NFS protocol.</p>
	<p><b>secure</b></p> <p>Specifies that the <b>mount</b> command uses Data Encryption Standard (DES) for NFS transactions. Data Encryption Standard (DES) is not supported in NFS Version 4, use <i>krb5</i> instead.</p>
	<p><b>sec=<i>flavor[:flavor...]</i></b></p> <p>Specifies a list of security methods that may be used to access files under the mount point. Allowable flavor values are:</p> <p><b>sys</b></p> <p>UNIX authentication. This is the default method.</p> <p><b>dh</b></p> <p>DES authentication. Data Encryption Standard (DES) is not supported in NFS Version 4, use <i>krb5</i> instead.</p> <p><b>krb5</b></p> <p>Kerberos. Authentication only.</p> <p><b>krb5i</b></p> <p>Kerberos. Authentication and integrity.</p>

Item	Description
	<p><b>krb5p</b></p> <p>Kerberos. Authentication, integrity, and privacy.</p> <p>The <b>secure</b> option may be specified, but not in conjunction with a <b>sec</b> option.</p> <p>The <b>secure</b> option is deprecated and may be eliminated in a future release.</p> <p>Use <b>sec=dh</b> instead.</p>
	<p><b>sec=[flavor1:....:flavorn]</b></p> <p>The <b>sec</b> option specifies the security flavor list for the NFS mount. The available flavors are <b>des</b>, <b>unix</b>, <b>sys</b>, <b>krb5</b>, <b>krb5i</b>, and <b>krb5p</b>. This option only applies to AIX 5.3 or later.</p>
	<p><b>shortdev</b></p> <p>Specifies that you are mounting a file system from a host that does not support 32-bit device special files.</p>
	<p><b>soft</b></p> <p>Returns an error if the server does not respond. The default value is <b>hard</b>.</p>
	<p><b>timeo=n</b></p> <p>Sets the Network File System (NFS) time out period to <i>n</i> tenths of a second. For TCP mounts, the default timeout is 100, which equals 10 seconds. For UDP mounts, the default timeout is 11, which equals 1.1 seconds, but varies depending on the NFS operation taking place. For UDP mounts, the timeout will increase for each failed transmission, with a maximum value of 20 seconds. Each transmission will be attempted twice, after which the timeout value is updated. The <b>timeo</b> option does not apply to communication from the NFS client to the <b>rpc.mountd</b> service on NFS servers. A timeout of 30 seconds is used when making calls to <b>rpc.mountd</b>.</p>
	<p><b>vers=[2 3 4]</b></p> <p>Specifies NFS version. The default is the version of NFS protocol used between the client and server and is the highest one available on both systems. If the NFS server does not support NFS Version 3, the NFS mount will use NFS Version 2. Use the <b>vers=[2 3 4]</b> option to select the NFS version. By default, the NFS mount will never use NFS Version 4 unless specified. The <b>vers=4</b> only applies to AIX 5.3 or later.</p>
	<p><b>wsiz=n</b></p>

Item	Description
	Sets the write buffer size to <i>n</i> bytes. Beginning with AIX Version 6.1, the default value is 64 KB and the maximum value is 512 KB when using Version 3 and Version 4 of the NFS protocol.

## CacheFS Specific Options

The CacheFS-specific version of the **mount** command mounts a cached file system; if necessary, it NFS-mounts its back file system. It also provides a number of CacheFS-specific options for controlling the caching process.

To mount a CacheFS file system, use the **mount** command with the **-V** flag followed by the argument. The following **mount** flags are available.

The following arguments to the **-o** flag are specifically for CacheFS mounts. Options you enter on the command line should be separated only by a comma, not a comma and a space.


**Note:** The **backfstype** argument must be specified.

Item	Description
<b>-o</b>	Specifies options. <b>acdirmax=<i>n</i></b> Specifies that cached attributes are held for no more than <i>n</i> seconds after directory update. Before <i>n</i> seconds, CacheFS checks to see if the directory modification time on the back file system has changed. If it has, all information about the directory is purged from the cache and new data is retrieved from the back file system. The default value is 60 seconds.
	<b>acdirmin=<i>n</i></b> Specifies that cached attributes are held for at least <i>n</i> seconds after directory update. After <i>n</i> seconds, CacheFS checks to see if the directory modification time on the back file system has changed. If it has, all information about the directory is purged from the cache and new data is retrieved from the back file system. The default value is 30 seconds.
	<b>acregmax=<i>n</i></b> Specifies that cached attributes are held for no more than <i>n</i> seconds after file modification. After <i>n</i> seconds, all file information is purged from the cache. The default value is 30 seconds.




Item	Description
<b>acregmin=<i>n</i></b>	Specifies that cached attributes are held for at least <i>n</i> seconds after file modification. After <i>n</i> seconds, CacheFS checks to see if the file modification time on the back file system has changed. If it has, all information about the file is purged from the cache and new data is retrieved from the back file system. The default value is 30 seconds.
<b>actimeo=<i>n</i></b>	Sets <b>acregmin</b> , <b>acregmax</b> , <b>acdirmin</b> , and <b>acdirmax</b> to <i>n</i> .
<b>backfstype=<i>file_system_type</i></b>	The file system type of the back file system (for example, nfs).
<b>backpath=<i>path</i></b>	Specifies where the back file system is already mounted. If this argument is not supplied, CacheFS determines a mount point for the back file system.
<b>cachedir=<i>directory</i></b>	The name of the cache directory.
<b>cacheid=<i>ID</i></b>	ID is a string specifying a particular instance of a cache. If you do not specify a cache ID, CacheFS will construct one.
<b>demandconst</b>	<p>Enables maximum cache consistency checking. By default, periodic consistency checking is enabled. When you enable <b>demandconst</b>, it checks on every read and write.</p> <div> <p><b>Note:</b> If this option is used the first time a specific CacheFS is mounted, then the option must also be specified for subsequent mounts. There is state information stored in the cache control files that enforces consistent use of this option.</p> </div>
<b>local_access</b>	Causes the front file system to interpret the mode bits used for access checking instead of having the back file system verify access permissions. Do not use this argument with secure NFS.
<b>noconst</b>	

Item	Description
	<p>Disables cache consistency checking. By default, periodic consistency checking is enabled. Specify <b>noconst</b> only when you know that the back file system will not be modified. Trying to perform cache consistency check using <b>cfsadmin-s</b> will result in error. <b>demandconst</b> and <b>noconst</b> are mutually exclusive.</p> <div data-bbox="461 434 1518 680"> <p><b>Note:</b> If this option is used the first time a specific CacheFS is mounted, then the option must also be specified for subsequent mounts. There is state information stored in the cache control files that enforces consistent use of this option.</p> </div>
	<p><b>purge</b></p> <p>Purges any cached information for the specified file system.</p> <div data-bbox="461 852 1518 1098"> <p><b>Note:</b> If this option is used the first time a specific CacheFS is mounted, then the option must also be specified for subsequent mounts. There is state information stored in the cache control files that enforces consistent use of this option.</p> </div>
	<p><b>rw   ro</b></p> <p>Read-write (default) or read-only.</p>
	<p><b>suid   nosuid</b></p> <p>Allows (default) or disallows set-uid execution</p>
	<p><b>write-around   non-shared</b></p> <p>Writes modes for CacheFS. The write-around mode (the default) handles writes the same as NFS does; that is, writes are made to the back file system, and the affected file is purged from the cache. You can use the non-shared mode when you are sure that no one else will be writing to the cached file system.</p> <div data-bbox="461 1740 1518 1986"> <p><b>Note:</b> If this option is used the first time a specific CacheFS is mounted, then the option must also be specified for subsequent mounts. There is state information stored in the cache control files that enforces consistent use of this option.</p> </div>

Item	Description
<b>mfsid</b>	Turns on global view. In NFS v4 system, you can traverse through the exported namespace on the server side. You need to specify this option to go over the file system.
<div>  <b>Restriction:</b> <b>mfsid</b> is an option if the backend file system for CacheFS is NFS v4. </div>	
<b>-V</b>	Mounts a CacheFS file system.

## Server Message Block (SMB) client file system specific options

Item	Description
<b>-o options</b>	<p>Specifies options for mounting the SMB client file system. Options that you enter on the command line must be separated only by a comma. Do not insert a space before or after a comma. The following options are available for the SMB client file system:</p> <p><b>fmode</b></p> <p>Sets a file or directory to octal mode for access permissions. The default value is 755.</p> <p><b>uid</b></p> <p>Assigns a user ID to files during the mount operation. The default value is root.</p> <p><b>gid</b></p> <p>Assigns a group ID to files during the mount operation. The default value is system.</p> <p><b>wrkgrp</b></p> <p>Specifies the workgroup to which the SMB server belongs. This parameter is mandatory to mount the SMB client file system.</p> <p><b>port</b></p> <p>Specifies the port number. The valid values are 445 and 139. The default value is 445. Port 139 is supported only when the specified server address is in IPv4 format.</p> <div>  <b>Note:</b> encryption option is not supported when the port specified is 139. </div> <p><b>pver</b></p> <p>Specifies version of the SMB protocol that is used to communicate with the SMB server. The valid values are 2.1, 3.0.2 and auto. For the value auto, the SMB</p>

Item	Description
	<p>protocol version 2.1 or version 3.0.2 is used based on the specified SMB server.</p> <p><b>signing</b></p> <p>Specifies whether the file system in the SMB client needs digital signature for communication with the SMB server filesystem. The valid values are <code>enabled</code> and <code>required</code>. When this parameter is set to <code>enabled</code>, the file system in the SMB client does not digitally sign the data packets unless the file system in the SMB server needs digital signatures for communication with the file system in the SMB server. When this is set to <code>required</code>, the file system in the SMB client must digitally sign the data packets for communication with the file system in the SMB server. If you do not specify the value for the <code>signing</code> parameter by using the <b>mount</b> command, a default value is used from the tunable parameter values of the kernel that are set by using the <b>smbctune</b> command.</p> <p><b>secure_negotiate</b></p> <p>Specifies whether the file system in the SMB client needs secure dialect negotiation capability. SMB Dialect 3.0.2 implements secure dialect negotiation to protect against security-downgrade attacks. The valid values are <code>desired</code>, <code>required</code>, and <code>disabled</code>. If you do not specify the value by using the <b>mount</b> command, a default value is used from tunable parameter values of the kernel that are set by using the <b>smbctune</b> command.</p> <p><b>encryption</b></p> <p>Specifies whether the file system in the SMB client requires data encryption. The valid values are <code>desired</code>, <code>required</code>, and <code>disabled</code>. If you do not specify the value by using the <b>mount</b> command, a default value is used from the tunable parameter values of the kernel that are set by using the <b>smbctune</b> command.</p> <div> <p><b>Note:</b> encryption option is not supported when the port specified is 139.</p> </div> <p><b>spn</b></p> <p>Specifies the <b>service principal name</b> (SPN) that must be used in the SMB client mount points. The format of the <b>spn</b> parameter is <code>cifs/&lt;smbServerHostName&gt;</code>, where <i>smbServerHostName</i> is the fully qualified domain name (FQDN) of the SMB server or the name that the Kerberos resolves as the SMB server. By default, SPN is constructed automatically by the SMB client file system as <code>cifs/&lt;smbServerHostName&gt;</code>.</p>

If the options that are used with the **mount** command (`pver`, `signing`, `secure_negotiate`, or `encryption`) are unspecified by using the **-o** flag, the default values for the **mount** command options are initialized by using the new values of the kernel tunable parameters (`smbc_protocol_version`, `smbc_signing`, `smbc_secure_negotiate`, `smbc_encryption`). The kernel tunable parameters are initialized from tunable parameters defined in the `smbctune.conf` file. These parameters can also be modified by using the **smbctune** command.

The following table shows the kernel tunable parameters of the **mount** command and the corresponding kernel tunable parameters that can be set in the `smbctune.conf` file:

Options of the -o flag (mount command)	Corresponding kernel tunable parameter of the smbctune.conf file	Valid values
pver	smbc_protocol_version	2.1, 3.0.2, auto
signing	smbc_signing	enabled, required
secure_negotiate	smbc_secure_negotiate	desired, required, disabled
encryption	smbc_encryption	desired, required, disabled

## Security [↗](#)

**i Attention RBAC users and Trusted AIX users:** This command can perform privileged operations. Only privileged users can run privileged operations. For more information about authorizations and privileges, see Privileged Command Database in *Security*. For a list of privileges and the authorizations that are associated with this command, see the **lssecattr** command or the **getcmdattr** subcommand.

## Examples [↗](#)

1. To list the mounted file systems, enter the following command:

```
mount
```



This command produces output similar to the following:

```
node    mounted      mounted over  vfs    date           options
----    -
/dev/hd0 /             /           jfs    Dec 17 08:04   rw, log  =/dev/hd8
/dev/hd3 /tmp          /tmp        jfs    Dec 17 08:04   rw, log  =/dev/hd8
/dev/hd1 /home        /home       jfs    Dec 17 08:06   rw, log  =/dev/hd8
```



```
sue      /dev/hd2      /usr      jfs      Dec 17 08:06   rw, log   =/dev/hd8
sue      /home/local/src /usr/code  nfs      Dec 17 08:06   ro, log   =/dev/hd8
```

For each file system, the **mount** command lists the node name, the device name, the name under which it is mounted, the virtual-file-system type, the date and time it was mounted, and its options.

2. To mount all default file systems, enter the following command:

```
mount all
```

This command sequence mounts all standard file systems in the **/etc/filesystems** file marked by the **mount=true** attribute.

3. To mount a remote directory, enter the following command:

```
mount -n nodeA /home/tom.remote /home/tom.local
```

This command sequence mounts the **/home/tom.remote** directory located on nodeA onto the local **/home/tom.local** directory. It assumes the default *VfsName* parameter=**remote**, which must be defined in the **/etc/vfs** file.

4. To mount a file or directory from the **/etc/filesystems** file with a specific type, enter the following command:

```
mount -t remote
```

This command sequence mounts all files or directories in the **/etc/filesystems** file that have a stanza that contains the **type=remote** attribute.

5. To CacheFS-mount the file system which is already NFS-mounted on **/usr/abc**, enter the following command:

```
mount -V cachefs -o backfstype=nfs,backpath=/usr/abc,
cachedir=/cache1 server1:/user2 /xyz
```

The lines similar to the following appear in the **/etc/mnttab** file after the mount command is executed:

```
server1:/user2 /usr/abc nfs
/usr/abc /cache1/xyz cachefs backfstype=nfs
```

6. To mount a snapshot, enter the following command:

```
mount -o snapshot /dev/snapsb /home/janet/snapsb
```



This command mounts the snapshot contained on the **/dev/snapsb** device onto the **/home/janet/snapsb** directory.

7. To mount a file system and create a snapshot, enter the following command:

```
mount -o snapto=/dev/snapsb /dev/sb /home/janet/sb
```



This command mounts the file system contained on the **/dev/sb** device onto the **/home/janet/sb** directory and creates a snapshot for the file system on the **/dev/snapsb** device.

8. To access files on an SMB server as a local file system, enter the following command:

```
mount -v cifs -n pezman/user1/pass1 -o uid=201,fmode=750 /home /mnt
```



9. To mount an SMB client file system as a local mount point, enter the following command:

```
mount -v smbc -n llm140.xyz.com/cec102usr1/Passw0rd \
-o wrkgrp=SMB_21.FVT,port=445,signing=required /some_share /mnt
```



Where, **llm140.xyz.com** is the Windows server, **cec102usr1** is the Kerberos user name, **Passw0rd** is the password of the Kerberos user, **SMB\_21.FVT** is the workgroup, **some\_share** is the share point on the Windows system, and **/mnt** is the local mount point.

10. To remount the mounted read-only JFS2 file system to a read-write file system, enter the following command:

```
mount -o remount,rw fsname
```



11. To mount all on a file **/tmp/fs1** of an alternate file system, enter the following command:

```
mount -F /tmp/fs1 all
```



## Files [↗](#)

Item	Description
<b>/etc/filesystems</b>	Lists the known file systems and defines their characteristics.
<b>/etc/vfs</b>	Contains descriptions of virtual-file-system types.

**Parent topic:**

→ [m](#)

**Related information**

→ [cdumount command](#)

→ [umount command](#)

→ [mount subroutine](#)

→ [/etc/filesystems file](#)