How do file permissions in Linux work?

Article Number: 54 | Rating: 2/5 from 4 votes | Last Updated: Wed, Aug 18, 2021 at 1:12 PM

File permissions are an essential part of web hosting, as they prevent your site from being compromised and private data being accessed. Certain files, such as CGI scripts, require particular permissions to be set up in order to run. Linux uses a specific model to define permissions, with three user categories that have their own permissions. The user categories are: Owner â€“ the user that owns the file or folder Group â€“ a defined group of users assigned to a file or folder All Users â€“ all other users on the system And each category can have one of the following permissions: Read â€“ being able to view the file or folder Write â€“ being able to write to the file or folder Execute â€“ being able to execute the file or folder These permissions are required for files on the Internet, and anything that should be directly accessible by the public will need at least a Read permission. There are two ways that Linux permissions are typically denoted â€“ either by a three digit code, or by specifying each available permission for each user. In both ways, the user categories are organised by Owner, then Group, then All Users. **Three Digit Code** On Linux, each permission is assigned a number: Read: 4 Write: 2 Execute: 1 Each user category is given a number, with the permissions for each category added up. So, for example, if you were to assign a file the permission 755, this would mean: Owner has Read/Write/Execute permission (4+2+1 = 7) Group has Read/Execute permission (4+1 = 5) All Users has Read/Execute permission (4+1 = 5) **Each Permission Specification** You can also list each permission by a single letter: Read: r Write: w Execute: x You then include each permission you want each user category to have, with dashes (-) representing where you don't assign a permission to a user category. So, for example, if you were to assign a file the permission rwxr-xr-x, this would mean: Owner has Read/Write/Execute permission (rwx) Group has Read/Execute permission (r-x) All Users has Read/Execute permission (r-x) For security reasons, this permission level (755 or rwxr-xr-x) is the highest permission we allow. It is important to set your permissions to the minimum needed in order for your site to function correctly. The eXtend Control Panel has 'Check Site Permission', a feature which will let you check the files you have on your site to ensure they have the right permissions or would possibly result in security issues. You can also change file permissions within the eXtend Control Panel's File Manager, through your FTP client, or directly via SSH.

Posted - Tue, Mar 3, 2015 at 4:00 PM.
Online URL: https://www.heartinternet.uk/support/article/how-do-file-permissions-in-linux-work.html