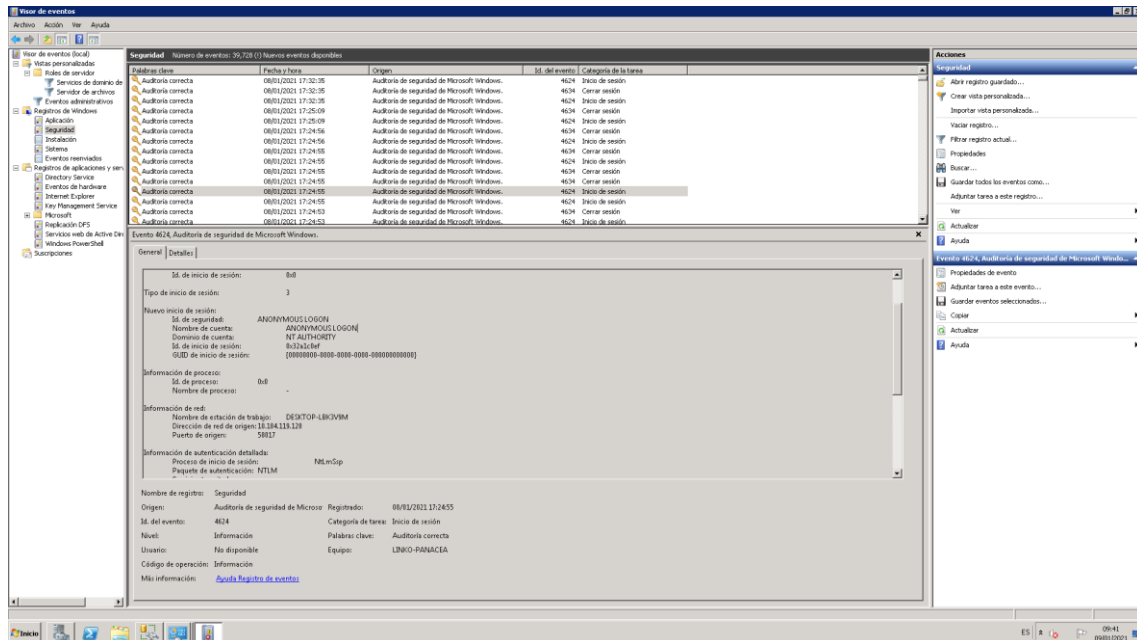


LOGS SISTEMA OPERATIVO

Windows Server 2008 R2

Panel de Control / Herramientas Administrativas / Visor de Eventos

Se encuentra los logs del Windows server así como el historial de los usuarios que se conectaron.



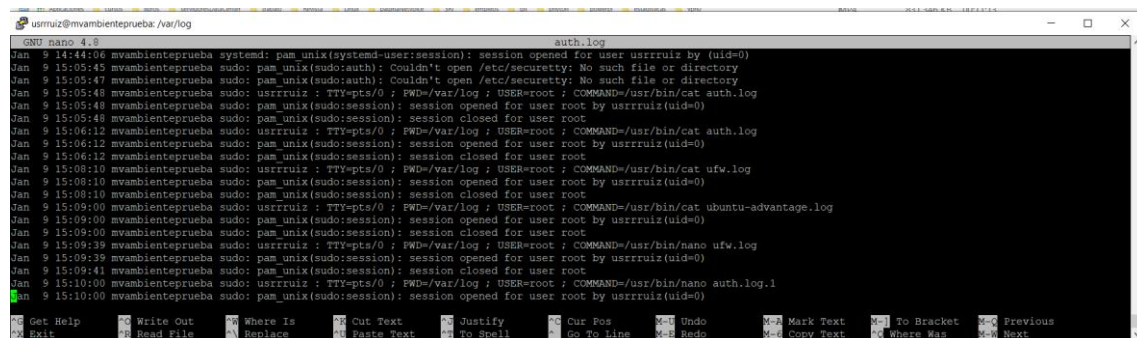
Ubuntu Server 20.04

Cd /var/log/

Se encuentran los diferentes archivos de logs que tiene el sistema. Depende el tipo de información que vayamos a buscar.

Para buscar con la palabra especifica sobre un archivo.

Ejemplo: grep "server" /etc/nginx/sites-available/default



```
GNU nano 4.8 auth.log
Jan 9 14:44:06 mvambienteprueba systemd: pam_unix(systemd-user:session): session opened for user usrruiz by (uid=0)
Jan 9 15:05:45 mvambienteprueba sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 9 15:05:47 mvambienteprueba sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jan 9 15:05:48 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat auth.log
Jan 9 15:05:48 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)
Jan 9 15:05:48 mvambienteprueba sudo: pam_unix(sudo:session): session closed for user root
Jan 9 15:06:12 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat auth.log
Jan 9 15:06:12 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)
Jan 9 15:06:12 mvambienteprueba sudo: pam_unix(sudo:session): session closed for user root
Jan 9 15:08:10 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat ufw.log
Jan 9 15:08:10 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)
Jan 9 15:08:10 mvambienteprueba sudo: pam_unix(sudo:session): session closed for user root
Jan 9 15:09:00 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat ubuntu-advantage.log
Jan 9 15:09:00 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)
Jan 9 15:09:00 mvambienteprueba sudo: pam_unix(sudo:session): session closed for user root
Jan 9 15:09:39 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/nano ufw.log
Jan 9 15:09:39 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)
Jan 9 15:09:41 mvambienteprueba sudo: pam_unix(sudo:session): session closed for user root
Jan 9 15:10:00 mvambienteprueba sudo: usrruiz : TTY=pts/0 ; FWD=/var/log ; USER=root ; COMMAND=/usr/bin/nano auth.log.1
Jan 9 15:10:00 mvambienteprueba sudo: pam_unix(sudo:session): session opened for user root by usrruiz(uid=0)

Get Help  Write Out  Where Is  Cut Text  Justify  Cur Pos  M-U Undo  M-A Mark Text  M-T To Bracket  M-P Previous
Exit      Read File  Replace  Paste Text  To Spell  Go To Line  M-R Redo  M-C Copy Text  M-W Where Was  M-N Next
```