SAMPLE LOG MANAGEMENT EVENT IDS FOR PCI DSS REQUIREMENT 10.2.X

Searching for Windows Event IDs are easier than parsing through *ix command lines. See below for helpful links on both types of operating systems.

Requirement	Windows Event ID	*IX
10.2.1.1 Successful Logons	4624	/var/log/auth.log or /var/log/secure
10.2.1.4 Unsuccessful Logons	4625	/var/log/faillog /var/log/btmp
10.2.1.5 New User Account	4720	cat /var/log/auth.log
10.2.1.5 Privelege escalation	4672, 4673	cat /var/log/auth.log (this is the user authorization file)
10.2.1.5 A user account was changed	4738	cat /var/log/auth.log

Logging, Log File Rotation, and Syslog Tutorial

12 Critical Linux log files

Windows Log Events