Nick Abbots Script

Nick Abbots Script:

```
vi ukfastmon;chmod u+x ukfastmon; ./ukfastmon; rm -f ukfastmon
```

```
#!/bin/bash
if [ "$1" = "w" ]; then
        locate wp-includes/version.php | xargs grep -H '^$wp_version' | grep -v virtfs
echo ""
echo ""
echo -n "The latest stable release of Wordpress is: "
curl -s https://wordpress.org/download/ | grep "Version" | awk '{print $9}' | cut -d ')' -f1
exit
fi

echo ""
echo ""
if [ ! -e /usr/bin/geoiplookup ]; then
        if [ -e /etc/network/interfaces ]; then
                apt-get install libgeoip1 geoip-bin
        else
                yum install GeoIP --enablerepo=epel -y
        fi
fi

if [ "$1" = "q" ]; then
        querydate=$2
elif [ "$1" = "d" ]; then
        querydate=$2
elif [ "$1" = "t" ]; then
        querydate="`date +%d/%b/%Y`:$2"
else
        querydate="`date +%d/%b/%Y`"
fi

if [ -e /dev/shm ]; then
```

```
        logs="$(TMPDIR=/dev/shm mktemp)"
else
        logs="$(mktemp)"
fi
if [ "$1" = "l" ]; then
        if [ "$3" = "d" ]; then
                querydate=$4
        fi
        if [ "$5" = "r" ]; then
                zgrep $querydate $2 | grep -v $6 > $logs
        else
                zgrep $querydate $2 > $logs
        fi
else

echo "Searching all access logs for $querydate"
echo ""

if [ -e /usr/local/cpanel/cpanel ]; then
        if [ "$1" = "q" ]; then
                find /usr/local/apache/domlogs/* -maxdepth 1 -type f | grep -v ssl | grep -v
ftp | grep -v byte | grep -v siteupda | xargs zgrep "`date +%d/%b/%Y`" | grep $querydate
2>/dev/null > $logs
        else
                find /usr/local/apache/domlogs/* -maxdepth 1 -type f | grep -v ssl | grep -v
ftp | grep -v byte | grep -v siteupda | xargs grep $querydate 2>/dev/null > $logs
                find /home/*/logs -type f | grep -v ftp | xargs zgrep $querydate 2>/dev/null
>> $logs
                find /home/*/access-logs -type f | grep -v ftp | xargs zgrep $querydate
2>/dev/null >> $logs
        fi
elif [ -e /usr/local/psa/version ]; then
        if [ "$1" = "d" ]; then
                if [ -e /var/www/vhosts/system ]; then
                        find /var/www/vhosts/system -name access_log* -o -name *proxy_access*
| xargs zgrep $querydate 2>/dev/null > $logs
                else
                        find /var/www/vhosts -name access_log* | xargs zgrep $querydate
2>/dev/null > $logs
                fi
```

```
        else
                if [ -e /var/www/vhosts/system ]; then
                        find /var/www/vhosts/system -name "*access_log" -o -name
*proxy_access* | xargs grep $querydate 2>/dev/null  > $logs
                else
                        find /var/www/vhosts -name "*access_log" -o -name *proxy_access* |
xargs grep $querydate 2>/dev/null > $logs
                fi
        fi
else
        find /var/log -name "*access_log*" -o -name "*access.log*" -o -name "*access_ssl_log*"
-o -name "varnishncsa.log" | xargs zgrep $querydate 2>/dev/null >> $logs
        find /home -name "*access_log*" -o -name "*access.log*" | xargs zgrep $querydate
2>/dev/null >> $logs
        find /var/www/vhosts -name "*access_log*" -o -name "*access.log*" | xargs zgrep
$querydate 2>/dev/null >> $logs
        find /var/www -name "*requests.log*" | xargs zgrep $querydate 2>/dev/null >> $logs
        find /root -name log | xargs zgrep $querydate 2>/dev/null >> $logs
        find /root -name varnishncsa.log | xargs zgrep $querydate 2>/dev/null >> $logs
fi
fi

if [ "$1" = "l" ]; then
echo "Searching specific log file $2 for $querydate"
echo ""
echo "Total number of requests"
echo ""
wc -l $logs | awk '{print $1}'
echo ""
else
echo "Total number of requests"
echo ""
wc -l $logs | awk '{print $1}'
echo ""
echo "Top 20 access log:IPs being hit"
echo ""
awk '{print $1}' $logs | sort | uniq -c | sort -gr | head -n 20
echo ""
fi
echo "Top 20 IPs"
```

```
echo ""
awk '{print $1}' $logs | cut -d: -f2 | sort | uniq -c | sort -gr | head -20 | awk '{
printf("%5d\t%-15s\t", $1, $2); system("geoiplookup " $2 " | head -1 | cut -d \\: -f2 ") }'
echo ""
echo "Top 10 /24s - treat country code with caution"
echo ""
awk '{print $1}' $logs | cut -d: -f2 | cut -d. -f1-3 | awk -F'[ .]' '{print $1 "." $2 "." $3
".0"}' | sort | uniq -c | sort -gr | head -10 | awk '{ printf("%5d\t%-15s\t", $1, $2);
system("geoiplookup " $2 " | head -1 | cut -d \\: -f2 ") }'
echo ""
echo "Top 20 requests"
echo ""
awk  '{print $6 " " $7 " " $9}' $logs | sort | uniq -c | sort -gr | head -n 20
echo ""
echo "Top 20 referrers"
echo ""
awk '{print $11}' $logs | sort | uniq -c | sort -gr | head -n 20
echo ""
echo "Top 20 user agents"
echo ""
cut -d\" -f6 $logs | sort | uniq -c | sort -gr | head -n 20
```

Revision #3
Created 2023-07-30 16:05:18 UTC by Daniel
Updated 2024-02-25 04:07:54 UTC by Daniel