

Re: determining when root was logged in

Source: <http://unix.derkeiler.com/Mailing-Lists/AIX-L/2003-10/0314.html>

From: Bill Verzal (*BVerzal_at_KOMATSUNA.COM*)

Date: 10/24/03

Date: Fri, 24 Oct 2003 15:39:43 -0500
To: aix-l@Princeton.EDU

What if the user logged in and "su"-ed ? Can they "rlogin" without authentication ?

Look through the \$HOME/.sh_history files. Also be aware that under AIX 5.2 (and maybe AIX 5.1), if you do a "file <filename>", it will change the datestamp of a file. There is a PTF to fix this behaviour.

BV

"If everything is coming your way, then you are in the wrong lane"

Bill Verzal
AIX Administrator, Komatsu America
(847) 970-3726 - direct
(847) 970-4184 - fax

```
|----->
|| Vipin Khushu |
|| <vkhushu@GUERNSEY|
|| OP.COM> |
|| Sent by: IBM AIX |
|| Discussion List |
|| <aix-l@Princeton.|
|| EDU> |
||
||
|| 10/24/2003 02:58 |
|| PM |
|| Please respond to|
|| IBM AIX |
|| Discussion List |
||
|----->
>-----
||
|| To: aix-l@Princeton.EDU |
```

AIX-L: Re: determining when root was logged in

| cc: |
| Subject: Re: determining when root was logged in |

>-----
Thanks Mark / Bill.

However, this gets curiouser and curiouser.

The last root command shows that the last time root logged into the system was back on sep 09.

However, we are sure that this file was modified yesterday.

Is there a way to determine who modified this file?

Vipin

-----Original Message-----

From: Bill Verzal [mailto:BVerzal@KOMATSUNA.COM]
Sent: Friday, October 24, 2003 1:49 PM
To: aix-l@Princeton.EDU
Subject: Re: determining when root was logged in

last|more
/etc/passwd and /etc/group

"If everything is coming your way, then you are in the wrong lane"

Bill Verzal
AIX Administrator, Komatsu America
(847) 970-3726 - direct
(847) 970-4184 - fax

|-----+----->
	Vipin Khushu
	<vkhushu@GUERNSEY
	OP.COM>
	Sent by: IBM AIX
	Discussion List
	<aix-l@Princeton.
	EDU>
	10/24/2003 12:03
	PM
	Please respond to
	IBM AIX
	Discussion List
-----+----->	

Re: determining when root was logged in

AIX-L: Re: determining when root was logged in

>

-----|
|
|
| To: aix-l@Princeton.EDU
|
| cc:
|
| Subject: determining when root was logged in
|

>

-----|
I need to pinpoint who was logged in as root yesterday when this file was modified. So I would like to know what time the person / process got logged in as root and from what terminal / IP address.

Also does anyone know where the list of users that are set up on the system are stored?

I need to show the users that are set up as part of the system group.

-rw-rw-rw- 1 root sys 26624 Oct 23 13:46 -dayend.cdx

-rw-rw-rw- 1 root sys 42844 Oct 23 13:46 -dayend.dbf

-rw-rw-rw- 1 root sys 10 Aug 02 10:03 -dayend.key

TIA

Vipin Khushu