Area51 Roll: Users Guide

Version 4.1 Edition

Area51 Roll: Users Guide :

Version 4.1 Edition

Published Oct 2005

Copyright © 2005 UC Regents

Table of Contents

Preface

The Rocks Area51 Roll contains utilities and services used to analyze the integrity of the files and the kernel on your cluster.

The following software packages are included in the Area51 Roll:

- Tripwire[1]
- chkrootkit[2]

Notes

1. http://www.tripwire.org/
2. http://www.chkrootkit.org/

Chapter 1. Requirements

1.1. Rocks Version

The Area51 Roll is for use on x86 systems (e.g., Pentium and Athlon) with Rocks version 4.1 (Fuji).

1.2. Other Rolls

The Area51 Roll is does not require any other Rolls (other than the HPC Roll) to be installed on the Frontend. Compatiblity has been verified with the following Rolls.

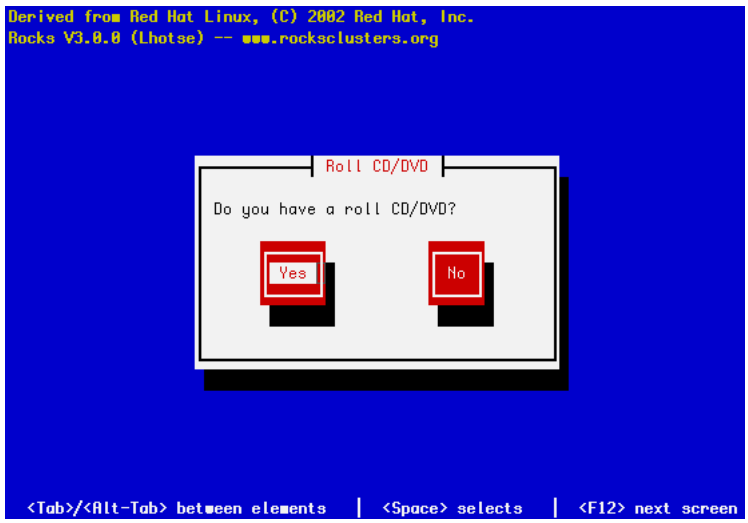
- HPC
- Grid
- Intel
- SGE

Chapter 2. Installing the Area51 Roll

2.1. Adding the Roll

The Area51 Roll must be installed during the Frontend installation step of your cluster (refer to section 1.2 of the Rocks usersguide). Future releases will allow the installation of the Area51 Roll onto a running system.

The Area51 Roll is added to a Frontend installation in exactly the same manner as the required HPC Roll. Specifically, after the HPC Roll is added the installer will once again ask if you have a Roll (see below). Select 'Yes' and insert the Area51 Roll.



Chapter 3. Using the Area51 Roll

3.1. Using Tripwire

Tripwire is configured to automatically scan the files on your frontend daily. This is accomplished via `cron`. To test the tripwire cron script, execute:

```
# /etc/cron.daily/tripwire
```

When this cron script runs successfully, tripwire sends mail to root (default). The cron script also creates a web page which shows the most recent tripwire report and web-archives of previous reports. See http://localhost/tripwire

To view the mail message, execute `mail`, then hit return at the & prompt. You'll see a mail message that looks similar to:

```
[root@rocks22 root]# mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/root": 1 message 1 new
>N  1 root@rocks22.sdsc.ed  Thu May 20 22:37 210/8552  "Tripwire: Daily repor"
&
Message 1:
From root@rocks22.sdsc.edu  Thu May 20 22:37:42 2004
X-Original-To: root@rocks22.sdsc.edu
Delivered-To: root@rocks22.sdsc.edu
Date: Thu, 20 May 2004 22:37:41 GMT
From: root <root@rocks22.sdsc.edu>
To: root@rocks22.sdsc.edu
Subject: Tripwire: Daily report from rocks22.sdsc.edu

Parsing policy file: /opt/tripwire/etc/tw.pol
*** Processing Unix File System ***
Performing integrity check...
Wrote report file: /opt/tripwire/db/report/rocks22.sdsc.edu-20040520-223648.twr


Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Thu 20 May 2004 10:36:48 PM GMT
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================

Host name:                    rocks22.sdsc.edu
Host IP address:              127.0.0.1
Host ID:                      None
Policy file used:             /opt/tripwire/etc/tw.pol
Configuration file used:      /opt/tripwire/etc/tw.cfg
Database file used:           /opt/tripwire/db/rocks22.sdsc.edu.twd
```

```
Command line used:            /opt/tripwire/bin/tripwire --check --cfgfile /opt/
tripwire/etc/tw.cfg
```

3.1.1. Changing the Target Email Address

To have tripwire email its report to a different email address. Simply run the `/opt/tripwire/etc/tw-email-to -set address1 [address2]`. For example, say you want to email the tripwire reports to go to `wopr@wargames.org` and `root`.

```
/opt/tripwire/etc/tw-email-to -set wopr@wargames.org root@‘hostname‘
```

To view the set of addresses for the Tripwire Daily Report

```
/opt/tripwire/etc/tw-email-to
```

3.2. Using chkrootkit

To see if your frontend has been infected by a rootkit, simply run:

```
# /opt/chkrootkit/bin/chkrootkit
```

This will return output similar to:

```
ROOTDIR is ‘/’
Checking ‘amd’... not found
Checking ‘basename’... not infected
Checking ‘biff’... not found
Checking ‘chfn’... not infected
Checking ‘chsh’... not infected
Checking ‘cron’... not infected
Checking ‘date’... not infected
Checking ‘du’... not infected
Checking ‘dirname’... not infected
Checking ‘echo’... not infected
Checking ‘egrep’... not infected
Checking ‘env’... not infected
Checking ‘find’... not infected
Checking ‘fingerd’... not found
Checking ‘gpm’... not infected
```

Make sure none of the tests report *INFECTED*.

For more information, login to the frontend and read `/opt/chkrootkit/README`.

Chapter 4. Area51 FAQ

1. How do I change the email addresses that receive the daily Tripwire report?

To have tripwire email its report to a different email address. Simply run the `/opt/tripwire/etc/tw-email-to -set address1 [address2]`. For example, say you want to email the tripwire reports to go to `wopr@wargames.org` and `root`.

```
/opt/tripwire/etc/tw-email-to -set wopr@wargames.org root@‘hostname‘
```

To view the set of addresses for the Tripwire Daily Report

```
/opt/tripwire/etc/tw-email-to
```

2. The MD5 Sums for My Policy/Config/Tripwire Executable Files at Installation are different than what my Latest Report tells me. How could this happen?

Rocks calculates MD5s Policy, Config, and Tripwire files after it initializes. If you have knowingly changed any of these, then the difference is OK. These might have changed if you reinitialized Tripwire interactively or in batch mode after initial installation. If you have NOT knowingly changed any of these items, then your computer may be at risk. Be very suspect of the Tripwire executable whose MD5 Sum has changed.

3. Is tripwire compiled statically?

Yes. Ideally the tripwire executable should be on a physically read-only file system. This is not very practical. Compiling statically guards against changed shared libraries.

4. What version of Tripwire is Used.

Rocks uses the open source Tripwire for Linux Version 2.3.1-2 with community supplied patches to enable it to compile on the most recent version of kernel/c-libraries. Currently only and x86 version is compiled.

5. How do I find out more about Tripwire and how it works?

Sourceforge Tripwire Homepage[1] is a good starting point.

6. I’ve checked all the problems that my Tripwire Report has flagged. How do I clear these for the next report?

As root, you need to re-initialize the Tripwire database. The Tripwire database is signed with a randomly generated key and the MD5 sum of this signature is reported each time the report runs. These MD5 sums should not change unless you re-initialize. To clear the flagged problems do

```
# cd /opt/tripwire/etc
# make initialize-batch
```

7. What is the password for the database so that I can selectively update Tripwire entries?

The default setup generates a random password for signing and then throws it away. Selective update requires an interactive initializion.

8. How do I setup Tripwire so that I can selectively update entries?

As root, you need to re-initialize the Tripwire database interactively with your self-selected site and local passphrases. You will first need to delete your site key and host keys then create a new one. Do the following and follow the on-screen directions.

```
# cd /opt/tripwire/etc
# /bin/rm *.key
# make initialize-interactive
# make check
```

Once you have initialized the database. Future Tripwire warnings can be addressed interactively with the following

```
# cd /opt/tripwire/etc
# make update
```

9. How do I add Files/Directories for Tripwire to Check?

The Tripwire Policy file (`/opt/tripwire/etc/twpol.txt`) is a monolithic text file that defines the files/directories to be Checked. Rocks builds this file in pieces from component files located in the directory `/opt/tripwire/etc/twpol-parts`. The Area51 roll creates files in the subdirectory `/opt/tripwire/etc/twpol-parts/base`. The `/opt/tripwire/etc/twpol-parts/addon` is where you should put new rules using the identical names of files in the base directory. You should the files in the base directory as a guide. Once you have added the files to watch you need to rebuild the tripwire database.

If you are using that basic setup provided by Rocks, then

```
# cd /opt/tripwire/etc
# make initialize-batch
```

If you have interactively setup Tripwire. Then

```
# cd /opt/tripwire/etc
# make updatedb
```

10. How should rolls add files for Tripwire to watch?

Rolls to should append to files in `/opt/tripwire/etc/twpol-parts/addon` using the files in `/opt/tripwire/etc/twpol-parts/base` as a template. For example, if an application Roll creates the directory `/opt/myapp` then it would be appropriate to add the following to `/opt/tripwire/etc/twpol-parts/base/appinfo` in post configuration section for your roll.

```
<post>
<file name="/opt/tripwire/etc/twpol-parts/base/appinfo" mode="append">
/opt/myapp  -> $(SEC_CRIT) (recurse = 1) ;
</file>
</post>
```

 Tripwire requires pathnames to be absolute pathnames

Notes

1. http://sourceforge.net/projects/tripwire