

ANDHRA PRADESH STATE ROAD TRANSPORT CORPORATE

Corporate office :: IT & MS Department

No.AME-2(Mgr.-IT)/Remote/2006-IT

O/o the VC & MD
MSRDJ3USBHAVAN
HYDERABAD-20
Dtd. 20.05.2006

CIRCULAR NO. 07/2006-IT Dated: 20.05.2006

Sub:- Computers(DCP)-Remote Backup- Implementation of remote backup at Linux Installed Depots-Auto copying of files from Server to Clients-Reg.

In April'05, Xeon Servers with latest configuration were Installed in 75 Depots. The operating system in the servers is Red Hat Enterprise Linux ES 3.0. A meeting was organized at Transport Academy on 15th, 16th & 17th December, 2005, with all the Regional Core Group Members and System Supervisors of the Depots where the new systems were installed, in order to take feedback on functioning of new systems. The feedback was that there is a necessity to have adequate backup of the data keeping in view the critical-ity of the applications. It was decided to expedite a solution for taking and preserving several backups **on different media available. In this context** a detailed study was made by IT Department on utilizing the Client hard disks for taking automatic back up from server to clients. This will be one of the backup media on which we can continuously and automatically store large data, according to the time limit specified by us.

Linux operating system has facility to copy files automatically from server to clients through "rsync" RPM. The "rsync" command is having built-in feature for copying files from server to the clients and vice versa.

The "rsync" is very efficient, reliable and faster in copying files from server to clients and vice-versa. The rsync remote-update protocol allows rsync to transfer just the differences between two sets of files across the network connection, using an efficient and reliable algorithm described in the technical report that accompanies this package. The rsync is fast because it just sends the differences in the files over the network instead of sending the complete files, i.e., only modified files will be copied after previous backup and this will result in less Input and Output loads. The "rsync" command copies linked files, Device files, owner, group and permissions with date stamping. We can implement scheduling Jobs in Linux through using "rsync" command i.e we can take automatic back up in different clients at different intervals. It is proposed to schedule backup of files in client2 at every 1st minute, 20th minute and 40th minute and in client 3 at 10th minute, 30th minute and 50th minute. In client 4, it is proposed to copy files at a frequency of every one hour. Through these scheduling scripts, the Server will automatically backup the files into the clients and there will be no manual intervention.

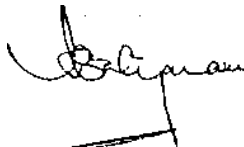
The major benefit that can be achieved by implementing this is, If Server is not booting due to hardware problems like HDDs, Mother board problem and RAM etc, one of the clients which is having latest backup can be made as an acting server immediately duly completing the minimum backlog work. If remote backup is successfully implemented there will not be any manual issuing of waybills at Depots, as backlog work can be fed immediately and the waybills can be issued to conductors from one of the clients which is made as an acting server.

The remote backup is successfully tested and implemented in the Depots of Musheerabad, Midhani and Hyderabad-II depots. A training program was conducted to all Regional Core Group Members on 21st March'2006 at Transport Academy, Hyderabad, where in a detailed demonstration was given on remote backup and its implementation at Linux Installed Depots. The procedure to implement remote backup at Depots and script files are filed in the Annexure "A".

All the Depot Managers are advised to implement remote backup at Linux Installed Depots duly utilizing the services-of the Regional Core Group Members, IT Department, Head office may also be contacted for any further clarification in implementing Remote backup.

-20.05.2006 EXECUTIVE DIRECTOR (IT&MS)

To

 ■L^JI
All the Depot Managers

CC to : All EDs for information please.

CC to : All RMs/DVMs for information. ,

CC to : All officers of the IT Department for information.

CC to : All the Central/Regional/Divisional Core Group Supervisors and Members.

Annexure "A"

PROCEDURE TO IMPLEMENT REMOTE BACKUP AT LINUX INSTALLED DEPOTS.

At Server side :

Copy all the "rsync-2.6.6" files in /tptobj/linux/rsync-2.6.6 and implement the following commands:

1. # cd /tptobj/linux/rsync-2.6.6
- 2.# make install
- 3.# cd /usr/bin
- 4.# mv rsync rsync.org
- 5.# cd /tptobj/linux/rsync-2.6.6

- 6.# cp rsync /usr/bin
- 7.# cd files
- 8.# cp bakup* /usr/bin (backup scripts commands to copy files)
- 9.# cp root /var/spool/cron (root is crontab entry)
- 10.# cp diskbak /usr/bin (Copy old diskbak as diskbakl)
11. Establish connection through ssh from server to client2.

```
# ssh root@client2
```

The authenticity of host 'client2 (192.168.1.2)' can't be established. RSA key fingerprint is f5:58:7d:84:d8:50:d5:2b:a6:ac:67:f0:6f:a8:3b:c6. Are you sure you want to continue connecting (yes/no)? < type yes > give password : < Type root password of client2>

```
# [root@client2 root] < press Ctrl + d >
```

- 12.. Establish connection through ssh from server to client3.

```
# ssh root@client3
```

The authenticity of host 'client3 (192.168.1.3)' can't be established. RSA key fingerprint is f5:58:7d:84:d8:50:d5:2b:a6:ac:67:f0:6f:a8:3b:c6. Are you sure you want to continue connecting (yes/no)? < type yes > give password : < Type root password of client3>

```
# [root@client3 root] < press Ctrl + d >
```

13. Establish connection through ssh from server to client4.

```
# ssh root@client4
```

The authenticity of host 'client4 (192.168.1.4)' can't be established. RSA key fingerprint is f5:58:7d:84:d8:50:d5:2b:a6:ac:67:f0:6f:a8:3b:c6 Are you sure you want to continue connecting (yes/no)? < type yes >

```
give password : < Type root password of client4>
```

```
# [root@client4 root] < press Ctrl + d >
```

14. Then apply the following command to generate private key and public key.

```
# ssh-keygen -t rsa
```

The output of the command is given below :

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id_rsa): < Press enter>

Enter passphrase (empty for no pass phrase): < Press enter >
Enter same passphrase again: < press enter >
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
a5:67:3a:5b:68:03:62:fd:48:38:45:40:27:52:83:5a root@server

The following files creates in /root/.ssh directory after this command:.

id_rsa id_rsa.pub

15. Copying the contents of file id_rsa.pub from clients in the server.

```
# cd /root/.ssh
```

Then create a file "authorized_keys".

```
# vi authorized_keys
```

In this file, copy the contents of file /root/.ssh/id_rsa.pub from client2, client3 and client4 systems in authorized_keys file without fail through cut and paste in a window. This copying of file contents will only after execution of "ssh-keygen -t rsa" command at client2, client3 and client4.

Caution : - After execution of the command " ssh-keygen -t rsa" at clients , then only, copy the contents of the file /root/.ssh/id_rsa.pub in authorized_keys. Without execution of this command, don't copy contents of the file root/.ssh/id_rsa.'pub.

16. # service crond restart

At client side:

Perform the following similar tasks in client2, client3 and client4 after one of another.

1. # ssh root@server

The authenticity of host'server (192.168.1.1)' can't be established. , , RSA key fingerprint is f5:58:7d:84:d8:50:d5:2b:a6:ac:67:f0:6f:a8:3b:c6. Are you sure you want to continue connecting (yes/no)? < type yes > give password : < Type root password of server>

```
# [root@server root] < press Ctrl + d >
```

2. # ssh-keygen -t rsa

The output of the command is given below :

Generating public/private rsa key pair.

Enter file in which to save the J<ey (/root/.ssh/id_rsa): < Press enter>

Enter passphrase (empty for no passphrase): < Press enter >

Enter same passphrase again: < press enter >

Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub.

The key fingerprint is:

2. a5:67:3a:5b:68:03:62:fd:48:38:45:40:27:52:83:5a root@server

The following files creates in/root/.ssh directory after this command:

id_rsa id_rsa.pub

3. Then create a file "authorized_keys".

```
#cd /root/, ssh
```

```
#vi authorized_keys
```

In this file copy the contents server's directory /root/.ssh/id_rsa.pub file in "authorized_keys" file without fail through cut and paste in window.

Note : The above procedure only one time job the time of implementation of remote backup. The above procedure establish trusted relation between hosts. Similar procedure for other clients as given above.

Things not to do :

Not to perform the following command at either server or clients more than once.

01. # ssh-keygen -t rsa

If you run the above command, the system will generate new private key and public keys i.e new authentication keys.

02. Not to run diskbak shell script more than once.

If Server fails :

1. Make one of the clients which is having the latest backup, as an acting server immediately.
2. See that "runcobol" software is installed in the client which is acting as a server.
3. Check files permissions and group and owner for /usr1 and /usr2 directories.
4. Complete the backup log work from the time, when the server has failed.
5. Connect the acting server from other clients, through telnet.
6. If original server is up and then copy files from /usr2 directory from acting server in /data directory.