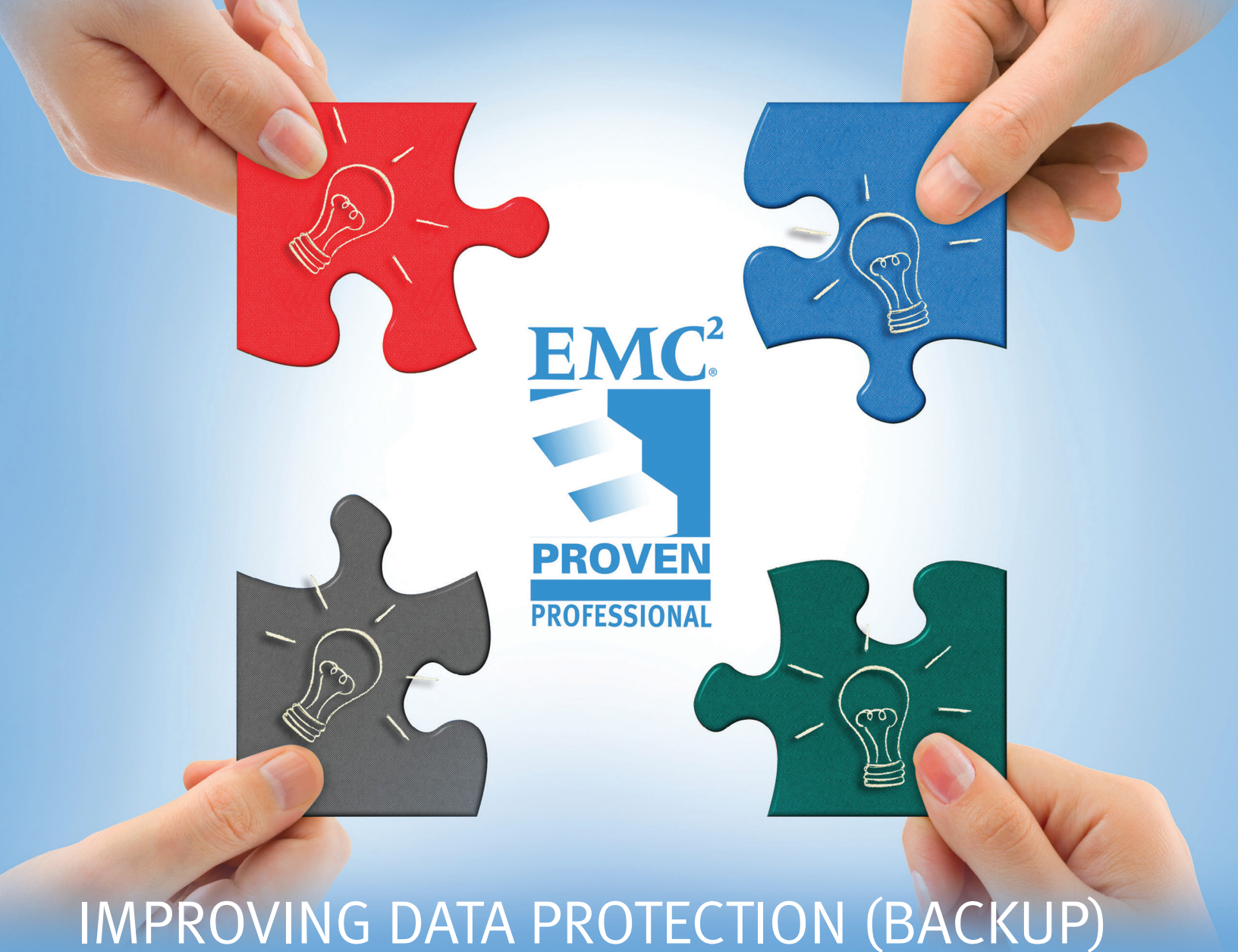




IMPROVING DATA PROTECTION (BACKUP) SUCCESS RATE PROACTIVELY

Mahendranag Jayanthi
Systems Architect
Tech Mahindra
dpnctl@gmail.com

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect EMC Corporation's views, processes or methodologies.

In general, a server's backup may fail for a number of reasons; name resolution on IP and name, backup client service is not running, backup NIC or primary NIC is not reachable over the network, traceroute is not functional, and so on. Essentially, any network pre-requisites that do not match or are altered will cause a backup to fail, thereby impacting the backup success rate metric. With distributed teams and different change processes in place, the volume of issues with dependencies of this kind was high and the time to resolve became a cause for concern. A Level 1 (L1) engineer takes 8-10 minutes to perform required pre-checks, identify the issue, and open a ticket to the host ownership team. The host ownership team then resolves the problem, communicating back to the backup team to re-fire a backup. This process introduces a few issues, including:

- a) Backup success rate – an important metric in a Managed Services organization – is reduced.
- b) Any delay in availability of host owner team will negatively impact SLA; another important metric in a managed services organization.
- c) Overall cost of manpower cycles involved increases.
- d) Face value of a data protection product decreases.
- e) RTO (recovery time objective) and RPO (recovery point objective) are impacted as data may not be available on some days.

The L1 team has opened nearly 1500 tickets (average 300 tickets per engineer). Time spent performing the pre-checks is a bit high, time which could otherwise be re-allocated to career improvement, contributing to other deliverables, or some other productive work.

There are multiple ways to remedy this situation.

- 1) Run a script a few hours ahead of backup schedule on all the backup clients that should be protected. However, a limitation is that backup engineers don't possess access to any of these backup clients. Coordination among all stakeholders is a big challenge.
- 2) A promising solution is to run pre-checks on the backup master server well before backup schedule. For example, a script can be scheduled to run two hours in advance enabling the backup team to see a report of all backup clients on which backups "may fail". As the team looks into the report, they can open tickets (ahead of backup failure) in advance to the host owners who then resolve the issue, thus reducing backup failures. In turn, this will reduce head count in L1 team considerably. Automation and taking a pro-active approach usually reduces effort turning metrics positive. All of these efforts fall into the "service excellence" bucket.

Overall, some manual intervention is required to accomplish this.

- 3) Sample proactive pre-check script to run on bash shell is provided for EMC NetWorker running on Solaris.
- 4) Basically, the algorithm of the script is:
 - a) List the backup clients
 - b) List their fqdn for both backup NIC and primary NIC
 - c) List their IPs
 - d) Run pre-checks such as hostname resolution, ping over network, and services running on the server with Telnet
 - e) Generate a consolidated list of servers where backups may fail



NWR_precheck_script.txt

```
$ cat nsradmin_input_file;cat precheck_report_script
. type: nsr client;scheduled backup: Enabled
show aliases
print
#!/bin/bash
rm -f ./full_client_list_on_this_nwr_server
rm -f ./nwr_client_ipaddress
rm -f ./nwr_client_precheck_fail_report
rm -f ./nwr_client_ipaddress
rm -f ./nwr_client_host2name_list

date >> ./nwr_client_precheck_fail_report

#      Generate a complete list of networker clients and save
FULL_CLIENT_LIST
nsradmin -i nsradmin_input_file|awk '{print $2"\n"$3"\n"$4}'|sed
'/^$/d'|cut -f1 -d";"| cut -f1 -d"," |grep "\." >
./full_client_list_on_this_nwr_server

#      For each of the client in FULL_CLIENT_LIST generate IPs

echo "                " >> ./nwr_client_precheck_fail_report
echo "HOSTNAME to IP RESOLUTION FAILED on FOLLOWING CLIENTS" >>
./nwr_client_precheck_fail_report
echo "                " >> ./nwr_client_precheck_fail_report

for nwr_client_name in $(cat ./full_client_list_on_this_nwr_server)
do
    host $nwr_client_name|grep -v handled|grep -v alias|grep
-v SERVFAIL|grep -v NXDOMAIN >> ./nwr_client_host2name_list
done
```

```

for nwr_client_name in $(cat ./full_client_list_on_this_nwr_server)
do
    host $nwr_client_name|grep -v handled|grep -v alias|grep
-v SERVFAIL|grep -v NXDOMAIN|awk '{print $4}' >> ./nwr_client_ipaddress
    host $nwr_client_name > /dev/null
    if [[ $? == 1 ]]
    then
        echo "$nwr_client_name" >>
./nwr_client_precheck_fail_report
    fi
done

echo "
" >> ./nwr_client_precheck_fail_report
echo "IP to HOSTNAME RESOLUTION FAILED on FOLLOWING IPs" >>
./nwr_client_precheck_fail_report
echo "
" >> ./nwr_client_precheck_fail_report

for nwr_client_ip in $(cat ./nwr_client_ipaddress)
do
    host $nwr_client_ip > /dev/null
    if [[ $? == 1 ]]
    then
        echo "$nwr_client_ip" >>
./nwr_client_precheck_fail_report
    fi
done

echo "
" >> ./nwr_client_precheck_fail_report
echo "NETWORKER CLIENT SERVICES ARE NOT RUNNING ON FOLLOWING CLIENTS" >>
./nwr_client_precheck_fail_report
echo "
" >> ./nwr_client_precheck_fail_report

for nwr_client_name in $(cat ./full_client_list_on_this_nwr_server)
do
    exec 3<>/dev/tcp/$nwr_client_name/7937 > /dev/null
    if [[ $? == 1 ]]
    then
        echo "$nwr_client_name" >>
./nwr_client_precheck_fail_report
    fi
done

echo "
" >> ./nwr_client_precheck_fail_report
echo "NETWORKER CLIENT NOT PINGABLE from Networker Master" >>
./nwr_client_precheck_fail_report
echo "
" >> ./nwr_client_precheck_fail_report

for nwr_client_name in $(cat ./full_client_list_on_this_nwr_server)
do
    ping -c 1 $nwr_client_name > /dev/null
    if [[ $? == 1 ]]
    then

```

```
                                echo "$nwr_client_name" >>
./nwr_client_precheck_fail_report
                                fi
                                done
date >> ./nwr_client_precheck_fail_report
*****
```

Conclusion

Managed services – in particular to backups – rely on multiple teams for resolution of issues. The chain of events after a backup failure may look small in a small environment but in a large environment, the scale can be higher. Backup administrators who automate such tasks will reduce effort and improve backup success rate.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.