ZephyrTel Mobile Messaging

Backup and Restore Utility - RHEL7

Release 22.12 Revision A

May 2023

Table of Contents

Chapter 1: Introduction....6

1.1 About this Document....7
1.2 Scope....7
1.3 Intended Audience....7
1.4 Documentation Conventions....7
1.5 Locate Product Documentation on the Customer Support Site....8

Chapter 2: Backup....10

2.1 Introduction....11
2.2 System Layout....11
2.3 Extended File Attributes....11
2.4 Backup and Restore Tool....12
2.5 System Information....12
2.6 Backup Location....13
2.7 Files and Directories for Backup....13
2.8 Excluded from Backup....14
2.9 Databases for Backup....14
2.9.1 MGR and BAT Database....14
2.9.2 CCI Database....15
2.9.3 SPF MySQL Cluster Database....15
2.9.4 AMS-Specific Backup....16
2.9.5 PBC Database Backup....16
2.9.6 STV and LGP Database....17
2.10 Unscheduled Backup....18
2.11 Scheduled Backup....18

Chapter 3: Recovery....20

3.1 Introduction....21
3.2 Prerequisites....21
3.3 System Recovery....21
3.4 Subscriber Element Restore....24
3.5 After the Restore....27

Appendix A: Manual Backup and Restore....28

A.1 Introduction....29
A.2 Estimated Backup Capacity....29
A.2.1 OAM Element....29
A.2.2 Traffic Element....29
A.2.3 Subscriber Element....30
A.2.4 Logging Element....30
A.3 Rotation Schema....31
A.4 Backup Procedure....31
A.4.1 OAM Element Backup....31
A.4.2 Traffic Element Backup....34
A.4.3 Subscriber Element Backup....37
A.4.4 Logging Element Backup....40
A.5 Restore Procedure....41
A.5.1 Introduction....41
A.5.2 System Restore....41
A.5.3 OAM Element Restore....41
A.5.4 Traffic Element Restore....42
A.5.5 Subscriber Element Restore....43
A.5.6 Logging Element Restore....47

Appendix B: References....48
B.1 References....49
Glossary....50

List of Figures

Figure 1: System Layout.....11
Figure 2: iLO Web GUI.....22

Chapter 1

Introduction

Topics:

- *About this Document.....7*
- *Scope.....7*
- *Intended Audience.....7*
- *Documentation Conventions.....7*
- *Locate Product Documentation on the Customer Support Site.....8*

1.1 About this Document

This document contains the description of the configuration backup and restore tools for the ZephyrTel Mobile Messaging products.

The manual procedure to take the backup and restore to earlier state is described in *Manual Backup and Restore*.

Because the available functions are licensed and depend on the specific Mobile Messaging implementation, not all functions and/or applications contained in this document may be relevant or applicable to the Mobile Messaging system you will be working with.

1.2 Scope

This document covers the backup and restore procedures for ZephyrTel Mobile Messaging elements on Red Hat Enterprise Linux 7.6 (RHEL7). It covers the restore of such a backup of the same system or a new system from scratch with the same configuration.

This document does not cover the backup and restore for the operating system (e.g. Ethernet configuration, disk configuration, and so on). Also, fast-changing run-time data is not backed up and recovered by the tools covered in this document. This includes statistical data, call detail record files, log files and the store and forward message database. This data is not backed up because restoring out of date data would lead to messages being sent twice or CDRs submitted twice.

1.3 Intended Audience

This document is intended for anyone interested in how Mobile Messaging can best be used, but mainly for:

- Implementation engineers who are responsible for the pre-installation, on-site installation and configuration of Mobile Messaging in the end-user environment,
- Maintenance and support engineers who are responsible for maintaining the total system environment of which Mobile Messaging is a part or just the Mobile Messaging devices,
- Network operators who are in charge of the daily operation of the Mobile Messaging systems and infrastructure.

1.4 Documentation Conventions

Typeface or Symbol	Meaning	Example
Bold	Refers to part of a graphical user interface.	Click **Cancel**.

Typeface or Symbol	Meaning	Example
`Courier`	Refers to a directory name, file name, command, or output.	The `billing` directory contains...
`<pointed brackets>`	Serves as a placeholder for text that the user will replace, as appropriate in context.	The file is called `MGRdata.xml.<ip>.gz`, where `<ip>` is the server's IP address.
`[square brackets]`	Indicates an optional command.	`[--validateonly]`
Note:	Indicates information alongside normal text, requiring extra attention.	**Note:** Ensure that the configuration...
\ (Unix)	Denotes line continuation; the character should be ignored as the user types the example, and ENTER should only be pressed after the last line.	`% grep searchkey \` `data/*.dat`

1.5 Locate Product Documentation on the Customer Support Site

Access to ZephyrTel's Customer Support site is restricted to current ZephyrTel customers only. This section describes how to log into the ZephyrTel Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the ZephyrTel Customer Support site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Backup

Topics:

- *Introduction.....11*
- *System Layout.....11*
- *Extended File Attributes.....11*
- *Backup and Restore Tool.....12*
- *System Information.....12*
- *Backup Location.....13*
- *Files and Directories for Backup.....13*
- *Excluded from Backup.....14*
- *Databases for Backup.....14*
- *Unscheduled Backup.....18*
- *Scheduled Backup.....18*

2.1 Introduction

This chapter describes the backup and restore tools and the files and directories included in a backup using the backup and restore tools.

2.2 System Layout

This document is structured according to the ZephyrTel Mobile Messaging standard system layout, illustrated below. It is recommended to perform backups per element.

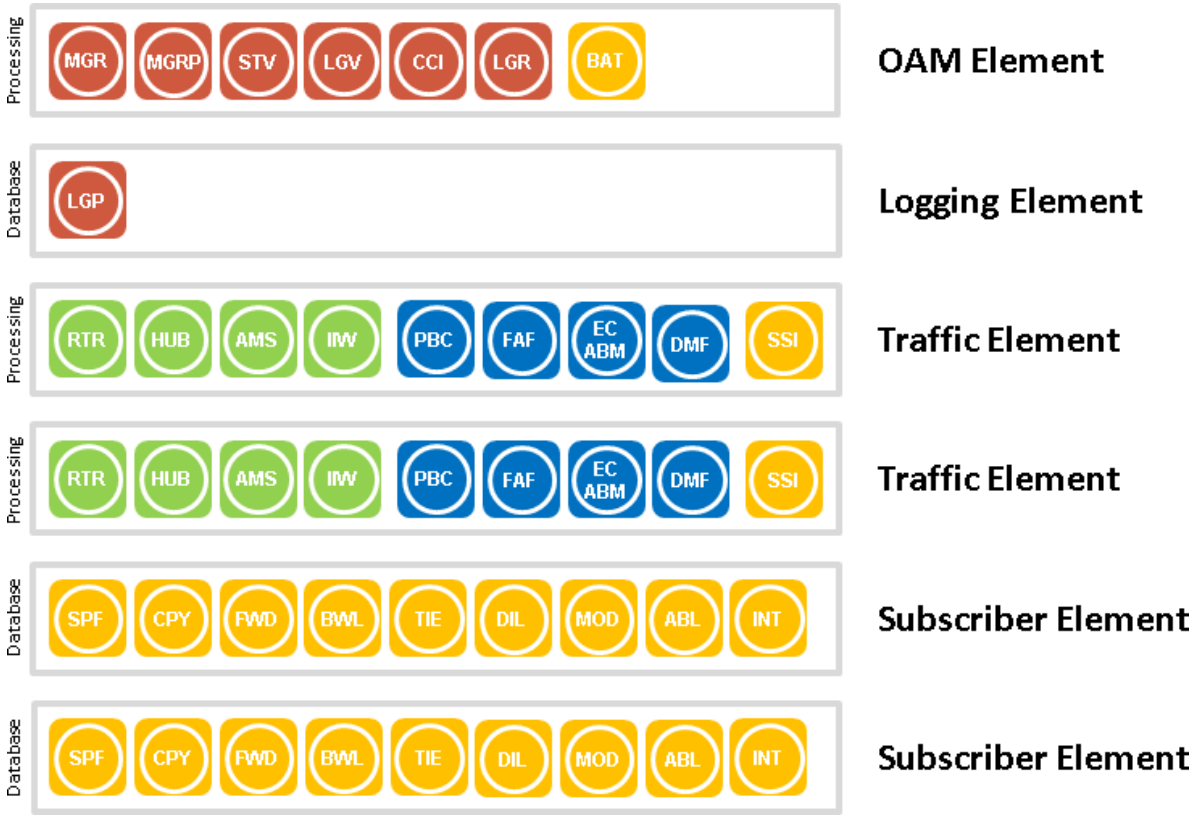

Figure 1: System Layout

2.3 Extended File Attributes

Some of the ZephyrTel software files on RHEL use the extended file attributes.

Warning: If an external backup tool is used to make backups of the ZMM systems, then this tool must backup and restore the extended file attributes.

2.4 Backup and Restore Tool

Mobile Messaging provides backup and restore tools to create a backup and restore from a certain backup. The backup and restore tools are intended for disaster recovery. The system provides the following command scripts on every Mobile Messaging element:

- `tp_backup`
- `tp_restore`

`tp_backup` creates a local backup. The backup can be used by `tp_restore` to restore the system to an earlier state.

The files that are backed up are controlled by `<name>.tp_backup` files. These files contain the paths and file names to be backed up. Different components and multi-instance users (`tpuserxx` where `xx` is 01 to 09) can add different configuration files to the mix. These files can also add scripts to be run before or after a backup. During the upgrade the files are copied to a staging area in `/var/TextPass/backup`, then `tar` and `gzip` are used to create the backup.

Ensure that enough free space (equal to double the size of an uncompressed backup file) exists in the staging area. You can check the amount of space needed by an uncompressed backup file by using the following command:

```
zcat -l <backup file>
```

Sample Check for Space Required

```
# zcat -l borneo.tar.gz
         compressed        uncompressed  ratio uncompressed_name
            3279152             4290560  23.6% borneo.tar
```

To check the available disk space, use the `df` command:

```
df -h
```

Sample Space Check

```
# df -h /var/TextPass/backup
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vgroot-TMMvar
                       99G  388M   94G   1% /var/TextPass
```

The `tp_backup` command can only be run as the root user. It needs permissions to access all files from the system. It will give an error message if it is run as non root user. Refer to the Tools Operator Manual for more information about `tp_backup` and `tp_restore`.

2.5 System Information

During the backup, information about the system is gathered and added to the backup. This can be used to validate and interpret backup files. This file is called `system_info`. It can be found in the root directory of the backup.

2.6 Backup Location

The backup is created in `/var/TextPass/backup/`.

It is the operator's responsibility to keep the backup files in a safe location outside the system. File transfer utilities like `scp` or `ftp` can be used to copy the backup file to a remote file server. Also, it is the operator's responsibility to remove old backups to ensure that there is enough free disk space on the system.

Note: Unsecured protocols such as FTP and telnet may introduce security risk to your network. The customers are at their own risks if the unsecured protocols are enabled and used on their systems.

2.7 Files and Directories for Backup

The following locations are backed up per Mobile Messaging element:

Backup Locations	OAM Element	Traffic Element	Logging Element	Subscriber Element	Full Element
`/etc`	X	X	X	X	X
`/usr/TextPass/etc`	X	X	X	X	X
`/usr/TextPass/.store`	X	X	X	X	X
`/usr/TextPass/.fcl`		X			X
`/usr/TextPass/.crypt`	X	X			X
`/dbspf/mysqlcluster/BACKUP`				X	
`/var/TextPass/MGR`	X				X
`/var/TextPass/CCI`	X				X
`/var/TextPass/STV`	X				X
`/var/TextPass/BAT`	X				X
`/var/log/STV`	X				X
`/var/lib/mysql-cluster/config.ini`	X				
`/usr/tpuserxx` [1]		X	X		X
`/var/tpuserxx` [1]		X	X		X
`/var/TextPass/textpassdmf`	X	X			
`/var/TextPass/DMF`		X			

Directories are recursively backed up.

[1] When multiple instances run on the same ZMM node.

Note: `tpuserxx` (where `xx` is 01 to 09) is an additional user that can be provisioned to execute a single instance of traffic element or logging element component depending on the server type (for more information refer to ZMM Multi instance Configuration Manual).

The backup tool creates a log file of the actions and error messages from the last backup in `/var/TextPass/backup`. The file is called `backup.log`.

The restore tool creates a log file of the actions and error messages from the last restore in `/var/TextPass/backup`. The file is called `restore.log`.

Important: Restoring the directory`/ust/TextPass/etc` will result in the CDR sequence number being reset back to the value at the time of the backup. If this is not acceptable and you want to start from 0 again, the CDR sequence number files must not be restored to start from 0.

2.8 Excluded from Backup

The following items are excluded from the backup by default:

- Billing files
- Logging files and database
- Statistics files and database
- AMS message database used for store and forward SMS traffic
- System and application software

It is the operator's responsibility to store the backup in a safe place, and to make it available on the system during a restore.

2.9 Databases for Backup

2.9.1 MGR and BAT Database

The scripts will automatically trigger a backup of the databases for MGR and BAT. These will automatically be included in the resulting backup.

The MGR backup file is located at `/opt/TextPass/MGR/<MGR-release>/etc/`

To back up the MGR configurations:

1. Copy the MGR backup file to `/usr/TextPass/etc`:
   ```
   cp /opt/TextPass/MGR/<MGR-release>/etc/mgr.tp_backup /usr/TextPass/etc/
   ```
2. Edit the `mgr.tp_backup` backup file. Uncomment the applicable statements and adjust it to your specific installation.
3. Save and close the file.

The next time `tp_backup` executes, the `mgr.tp_backup` file will be included in the backup.

2.9.2 CCI Database

The scripts will automatically trigger a backup of the databases for CCI. This will automatically be included in the resulting backup.

The CCI backup file is located at `/opt/TextPass/CCI/<CCI-release>/etc/`.

To back up the CCI configurations:

1. Copy the CCI backup file to `/usr/TextPass/etc`:
   ```
   cp /opt/TextPass/CCI/<CCI-release>/cci.tp_backup /usr/TextPass/etc/
   ```
2. Edit the `cci.tp_backup` backup file. Uncomment the applicable statements and adjust it to your specific installation.
3. Save and close the file.

The next time `tp_backup` executes, the `cci.tp_backup` file will be included in the backup.

2.9.3 SPF MySQL Cluster Database

Two backups are required:

- The MySQL database cluster for the SPF element
- The SPF database schema.

The MySQL database cluster must be manually backed up.

Execute the command given below on the cluster management node (the OAM Element) to back up the MySQL database cluster:

```
$ ndb_mgm -e "START BACKUP"
```

The command given above creates the backup on the Subscriber element in `/dbspf/mysqlcluster/BACKUP`.

To backup the SPF database schema, execute the following commands on the Subscriber element. These are specific to a range of releases.

For releases earlier than 12.4:

```
$ mysqldump -uroot -plokal$ -no-data spf > /var/TextPass/backup/spf_db_schema_only.sql
```

For release 12.4 and later:

```
$ mysqldump --login-path=mysql_root -no-data spf >
/var/TextPass/backup/spf_db_schema_only.sql
```

The backup can also be created by updating the `spf.tp_backup` file as follows:

For releases earlier than 12.4:

```
PRE_BACKUP:mysqldump -uroot -plokal$ -no-data spf >
/var/TextPass/backup/spf_db_schema_only.sql
```

For release 12.4 and later:

```
PRE_BACKUP:mysqldump --login-path=mysql_root -no-data spf >
/var/TextPass/backup/spf_db_schema_only.sql
```

2.9.4 AMS-Specific Backup

It is not recommended to back up the AMS database as the information stored in the AMS database has a very limited lifetime. At the same time, the AMS database is for redundancy purposes replicated on another system.

If a backup is desired, it is recommended to update the `ams.tp_backup` file under `/usr/TextPass/etc`.

1. Edit the `ams.tp_backup` file and adjust it to your specific installation.

   For example, the AMS databases and AMS databases log files can be backed up if `ams.tp_backup` file is updated with the following entries:

   ```
   #backup files
   DIR:/dbamsstore
   DIR:/dbamslog
   ```

2. Save and close the file.

The next time `tp_backup` executes, the `ams.tp_backup` file will be included in the backup.

2.9.5 PBC Database Backup

A Traffic Element can be configured to run a PBC and a database.

The PBC supports the following database types:

- A local or external MySQL database
- An external operator managed LDAP database
- An external operator managed Oracle database

Depending on your specific implementation of the PBC, it might be necessary to backup additional locations, like the configuration of the database that is used and, in rare cases, it might be good to backup (parts) of the database. Because the situation is very implementation-specific, please contact ZephyrTel Support to obtain a specific recommendation for your situation.

If a backup of the PBC database is desired, it is recommended to update the `pbc.tp_backup` file under `/usr/TextPass/etc`.

1. Edit the `pbc.tp_backup` file and adjust it to your specific installation.

   For example, the PBC database "`pbcservice`" can be backed up if `pbc.tp_backup` file is updated with the following entry:

   For releases earlier than 12.4:

   ```
   PRE_BACKUP:mysqldump -uroot -plokal$ pbcservice > /var/TextPass/backup/pbc.sql
   ```

   For release 12.4 and later:

   ```
   PRE_BACKUP:mysqldump --login-path=mysql_root  pbcservice >
   /var/TextPass/backup/pbc.sql
   ```

2. Save and close the file.

The next time `tp_backup` executes, the `pbc.tp_backup` file will be included in the backup.

2.9.6 STV and LGP Database

For the backup of the STV and LGP database, templates are added, but these are not active by default. The STV and LGP backup templates are located at `/usr/TextPass/etc/STV/stv.tp_backup_template` and `/usr/TextPass/etc/lgp.tp_backup_template`.

2.9.6.1 STV Database Backup

To back up the STV database:

1. Copy the template to a backup file:
   ```
   cp /usr/TextPass/etc/STV/stv.tp_backup_template /usr/TextPass/etc/stv.tp_backup
   ```
2. Edit the `stv.tp_backup` backup file. Uncomment the applicable statements, and adjust to your specific installation.
3. Save and close the file.

The next time `tp_backup` executes, the `stv.tp_backup` file will be included in the backup.

2.9.6.2 LGP Database Backup

It is not recommended to backup the LGP database, as the information stored in the LGP database has a limited lifetime. Also, the LGP database can be very large depending on your specific setup.

To back up the LGP database:

1. Copy the template to a backup file:
   ```
   cp /usr/TextPass/etc/lgp.tp_backup_template /usr/TextPass/etc/lpg.tp_backup
   ```
2. Edit the `lgp.tp_backup` backup file. Uncomment the applicable statements, and adjust to your specific installation.

   In case multi-instances are running on the LGP node, ensure that each user database is backed up.

   For example, the `tpuser01` LGP database "`lgpuse01`" can be backed up if `lgp.tp_backup` file is updated with the following entry:

   For releases earlier than 12.4:
   ```
   PRE_BACKUP:mysqldump -uroot -plokal$ lgpuser01 > /var/TextPass/backup/lgpuse01.sql
   ```
   For release 12.4 and later:
   ```
   PRE_BACKUP:mysqldump --login-path=mysql_root  lgpuser01 >
   /var/TextPass/backup/lgpuse01.sql
   ```
3. Save and close the file.

The next time `tp_backup` executes, the `lgp.tp_backup` file will be included in the backup.

2.10 Unscheduled Backup

To perform a backup, execute the following command as user `root`:

```
tp_backup -v
```

The `-v` option will show the log and error messages also to the screen. The backup will stop in case errors are reported, and no valid backup file is created. In this case, please fix the errors and rerun the backup.

If the messages have scrolled from your screen you can review the messages in the backup log file (`/var/TextPass/backup`).

2.11 Scheduled Backup

For all the network elements to create scheduled backups, the backup script can be included in the `crontab` for the `root` user.

For example, if you want the backup to be taken each night at 2 AM, put the following in the `crontab` for `root`:

```
00 2 * * * /usr/TextPass/bin/tp_backup
```

With the following command:

```
crontab -e
```

Chapter 3

Recovery

Topics:

- *Introduction.....21*
- *Prerequisites.....21*
- *System Recovery.....21*
- *Subscriber Element Restore.....24*
- *After the Restore.....27*

3.1 Introduction

This chapter describes how to restore a Mobile Messaging element.

3.2 Prerequisites

Contact ZephyrTel

CAUTION: Contact the ZephyrTel Customer Care Center and inform them of restore plans prior to beginning this procedure.

Phone: +1-888-586-3257 (direct support number) or +1-512-861-1974 (zephyrtel general support number)

Email: mmsupport@zephyrtel.com

Hardware Setup

Hardware installation and recovery: Please make sure the hardware is in proper condition before commencing a restore.

Backup File

Make sure you have the right backup file that corresponds to the system that you want to restore. Any configuration changes made after the backup is done, are not included in the backup, they will need to be reapplied after the backup is restored.

Licenses

The ZephyrTel Mobile Messaging system requires license tied to specific server hardware. If you are restoring on replacement hardware you need to apply for new license files indicating the specific hardware you want to software to be restored on. Contact ZephyrTel support to obtain new license files.

OS and Application Software ISO

This restore procedure assumes that you have available the same OS software (RHEL7) and application software as was previously installed on the server when you created the backup file. Please store the ISO files or create CD-ROM/DVD and store on a safe location for recovery. If you do not have the right software versions available, contact ZephyrTel support.

3.3 System Recovery

To restore the system:

1. **Hardware recovery**

   Verify that hardware is correct; this would involve at least connecting to the iLO (using the Web GUI as below) and verifying no errors are reported.

   Figure 2: iLO Web GUI

   If the target server is a previously used server and you had a previous RAID configuration, you will need to remove the original RAID configuration, as detailed in Appendix A of ZephyrTel Mobile Messaging RHEL 7.6 Installation Manual (MO006404)

2. **Operating system recovery**

   Install RHEL7 according to ZephyrTel Mobile Messaging RHEL 7.6 Installation Manual (MO006404).

3. **Install Mobile Messaging software**

   Determine the type of element you need to install on the server:

   - OAM Element
   - Traffic Element
   - Logging Element
   - Subscriber Element
   - Standalone STV Element
   - Full Element (all packages excluding SPF and XS)

   Install the Mobile Messaging software by following the complete installation manual for the element type that you need to install:

For...	Follow...
OAM Element	ZephyrTel Mobile Messaging Installation Manual - RHEL7
Traffic Element	ZephyrTel Mobile Messaging Installation Manual - RHEL7
Logging Element	ZephyrTel Mobile Messaging Installation Manual - RHEL7

For...	Follow...
Subscriber Element	ZephyrTel Mobile Messaging Subscriber Element Installation Manual - RHEL7
Standalone STV Element	ZephyrTel Mobile Messaging Standalone STV Element Installation Manual - RHEL7
Full Element	ZephyrTel Mobile Messaging Full Element Installation Manual - RHEL7

4. **Restore backup**

   Transfer the backup file (created by `tp_backup`) on the system, to a location on the server that has enough space to keep the backup file. If you are using `scp` to transfer files, execute the following commands:

   ```
   cd /var/TextPass/backup
   scp <username>@<remote server>:<backup_file>
   ```

   Enter the password for the username on the remote server if requested. Watch the output of the `scp` command to verify the backup file is completely and correctly transferred.

   To start a restore, execute the following command as a root user:

   ```
   /usr/TextPass/bin/tp_restore -f <backup_file>
   ```

   This will restore the backed up application data, including all system files, such as IP address, `ntpd` settings, `hostid`, etc. Note that:

   - The default location for backup files is `/var/TextPass/backup`.
   - Other options for file transfer (FTP, CD-ROM, or USB storage) can also be used to copy the backup file to the system.

     Note: Unsecured protocols such as FTP and telnet may introduce security risk to your network. The customers are at their own risks if the unsecured protocols are enabled and used on their systems.

   - You may not want to restore the Subscriber Element from backup; because it is a MySQL Cluster, it can recover from the other live systems.

5. **Reboot**

   The `tp_backup` utility will reboot after it has restored all files. This ensures that all services run according to the replaced configuration.

   The OAM Element is set up with the databases from the backup. You may need to restart the Traffic Elements to enable them to obtain and load the configuration XML files in `/usr/TextPass/etc` from the OAM Element. STV and LGP will be set up if the provided templates are used.

3.4 Subscriber Element Restore

This section only describes restoring the Subscriber Element on the master site. These instructions assume that the database user name is `root`, the database password is `lokal$`, and the database name is `spf`.

Note: If there are clients in the network that replicate from the master database (such as local SSIs or a slave site), you must have access to the ZephyrTel Mobile Messaging OAM Element and Traffic Element Installation Manuals to complete this procedure.

To fully restore the database on the Subscriber Elements:

1. Restore the files from the backup location.
2. On all Subscriber Elements, stop the SPF core:

   ```
   # su - textpass -c "tp_stop"
   ```

   Sample output:

   ```
   Stopping SPFCORE on spf3
   Stopping tp_fclient on spf3
   Stopping tp_mgrd on spf3
   ```

3. On all Subscriber Elements, log in to MySQL and stop the slave:

   For releases earlier than 12.4:

   ```
   mysql -uroot -plokal$ -e "stop slave;"
   mysql -uroot -plokal$ -e "show slave status;"
   ```

   For release 12.4 and later:

   ```
   mysql --login-path=mysql_root  -e "stop slave;"
   mysql --login-path=mysql_root  -e "show slave status;"
   ```

4. On all Subscriber Elements, stop MySQL:

   ```
   # systemctl stop mysql
   ```

5. On the OAM Element, verify that the Subscriber Elements are no longer connected:

   ```
   $ ndb_mgm -e "SHOW"
   ```

   Note: If the node is connected, the IP address, MySQL and NDB versions will be shown. Otherwise, the node is described as "not connected".

6. On the OAM Element, stop the data nodes:

   ```
   $ ndb_mgm -e "ALL STOP"
   ```

   Sample output:

   ```
   Connected to Management Server at: localhost:1186
   Executing STOP on all nodes.
   NDB Cluster has shutdown.
   ```

   Execute:

   ```
   $ ndb_mgm -e "SHOW"
   ```

7. On all Subscriber Elements, restart the data nodes with the initial flag to remove all data from the database:

   ```
   # /usr/sbin/ndbmtd --initial
   ```

Wait until the state of the Subscriber Elements is no longer "starting" before you continue to the next step (verify the state using the `ndb_mgm -e "SHOW"` command on the OAM Element).

At this point, no SPF tables will be in the database (only views will remain, as they are not clustered).

8. On all Subscriber Elements, start MySQL:
```
# systemctl start mysql
```
9. Restore the SPF DB schema on any of the master nodes only:

   For releases earlier than 12.4:
```
$ mysql -uroot -plokal$ spf < /var/TextPass/backup/spf_db_schema_only.sql
```
   For release 12.4 and later:
```
$ mysql --login-path=mysql_root spf < /var/TextPass/backup/spf_db_schema_only.sql
```
10. On all Subscriber Elements, stop MySQL:
```
# systemctl stop mysql
```
11. On all Subscriber Elements, execute `ndb_restore` (do so on one Subscriber Element after another):
```
# /usr/mysql/bin/ndb_restore -c <OAM Element>:1186 -n \
<node_id> -b <backup_id> -r --backup_path=</path/to/backup/files> \
--include-databases=<database_name>
```
   For example, on Subscriber Element 1, execute:
```
# /usr/local/bin/ndb_restore -n 2 -b 1 -r \
--backup_path=/dbspf/mysqlcluster/BACKUP/BACKUP-1/ --include-databases=spf
```
   For example, on Subscriber Element 2, execute:
```
# /usr/local/bin/ndb_restore -n 3 -b 1 -r \
--backup_path=/dbspf/mysqlcluster/BACKUP/BACKUP-1/ --include-databases=spf
```
   Sample output:
```
Nodeid = 2
Backup Id = 1
backup path = /dbspf/mysqlcluster/BACKUP/BACKUP-1
Opening file '/dbspf/mysqlcluster/BACKUP/BACKUP-1/BACKUP-1.2.ctl'
Backup version in files: ndb-6.3.11 ndb version: mysql-5.1.51 ndb-7.1.9
Connected to ndb!!

   < -- SNIP -- >

Opening file '/dbspf/mysqlcluster/BACKUP/BACKUP-1/BACKUP-1.2.log'
Restored 50207713 tuples and 244 log entries

NDBT_ProgramExit: 0 - OK
```
12. Bring the MySQL Cluster back online.

    a. On the OAM Element, exit single user mode:
```
$ ndb_mgm -e "EXIT SINGLE USER MODE"
```
    b. On all Subscriber Elements, start MySQL:
```
# systemctl start mysql
```
    c. On the OAM Element, verify that the MySQL Cluster is back online:
```
$ ndb_mgm -e "SHOW"
```
13. On all Subscriber Elements, confirm that the data is restored:

For releases earlier than 12.4:

```
# mysql -uroot -plokal$  -Dspf -e "SELECT COUNT(*) FROM SUBSCRIBER"
```

For release 12.4 and later:

```
# mysql --login-path=mysql_root  -Dspf -e "SELECT COUNT(*) FROM SUBSCRIBER"
```

Sample output:

```
+----------+
| COUNT(*) |
+----------+
|   465001 |
+----------+
```

Note: The total subscriber count does not have to be equal to the subscriber count at the time of backup, but realistically it should not differ much.

14. On all Subscriber Elements, stop MySQL:

```
# systemctl stop mysql
```

15. On the OAM Element, stop the data nodes:

```
$ ndb_mgm -e "ALL STOP"
```

Sample output:

```
Connected to Management Server at: localhost:1186
Executing STOP on all nodes.
NDB Cluster has shutdown.
```

Execute:

```
$ ndb_mgm -e "SHOW"
```

16. On all Subscriber Elements, start `ndbmtd`:

```
# systemctl restart ndbmtd
```

17. On all Subscriber Elements, start MySQL:

```
# systemctl start mysql
```

If there are no clients in the network that replicate from the master database, then the restore procedure is complete.

Note: After `ndb_restore` has finished and `ndbmtd` is running with the restored data, the internal counter that is used as implicit backup ID will be to 1. If you perform a backup using the command `ndb_mgm -e "start backup"`, the `ndb_mgm` process will attempt to create backup number 1 in the backup directory (by default, `/dbspf/mysqlcluster/BACKUP`). If a backup with ID 1 already exists (that is, `/dbspf/mysqlcluster/BACKUP/BACKUP-1`), the command will fail and no backup will be created. To resolve this situation, you must do one of the following:

- Explicitly set the internal counter to the first non-existing backup ID. For example, if the first non-existing backup ID is 51, execute `ndb_mgm -e "start backup 51"`
- Resolve the conflicting paths, such as by moving the backups to another location. For example, `mv /dbspf/mysqlcluster/BACKUP /dbspf/mysqlcluster/BACKUP-OLD`

After you have restored the database restored from backup, all backups that you created after the one that you used for restoration, up to the restoration time, are obsolete.

18. On all Subscriber Elements, log in to MySQL and reset the master:

For releases earlier than 12.4:

```
# mysql -uroot -plokal$
mysql> RESET MASTER;
```

For release 12.4 or later:

```
# mysql --login-path=mysql_root
mysql> RESET MASTER;
```

19. On all Subscriber Elements, start the SPF core:

    ```
    # su - textpass -c "tp_start"
    ```

    Sample output:

    ```
    Starting SPFCORE on spf3
    Starting tp_fclient on spf3
    Starting tp_mgrd on spf3
    ```

    If there are any clients in the network that replicate from the master database (local SSIs or a slave site), continue with the procedure to restore replication:

20. Follow the "Configure MySQL Cluster Replication" procedure in the Subscriber Element Installation Manual for RHEL7.

Replication of the master database should now be restored.

3.5 After the Restore

Verify that call detail records (CDRs) are generated. Verify with standard tests that short messages are properly handled by the system.

After initial verification is positive, take a new unscheduled backup to record the state of the server as done after backup.

Appendix A

Manual Backup and Restore

Topics:

- *Introduction.....29*
- *Estimated Backup Capacity.....29*
- *Rotation Schema.....31*
- *Backup Procedure.....31*
- *Restore Procedure.....41*

A.1 Introduction

This Appendix describes the manual procedures for backup and restore without using `tp_backup` and `tp_restore` tools.

Important: It is highly recommended that the customer runs the backups during off-peak hours and also avoids scheduling of the backups around the same time that mobile messaging off-peak hour tasks are scheduled. Also, check with the system administrator about the scheduled jobs such as `cron` jobs and arrange the automatic backup accordingly.

A.2 Estimated Backup Capacity

A backup should be moved to a safe location. It is up to the operator, depending on its IT architecture, to decide on the best backup location.

The recommended free space depends very much on the installation size. Average backup capacity is approximately 10 GB per server.

The following sections describe the estimated backup capacity per Mobile Messaging element. The required capacity may vary from the numbers listed here they depend on the system capacity and dimensioning. The capacities listed here are average numbers.

A.2.1 OAM Element

The following table describes the estimated backup capacity for the Mobile Messaging OAM Element.

Component	Average Backup Capacity Required
MGR	10 GB
STV	10 GB (this average indicates the backup capacity, including the database; however, the database size depends on your configuration and may be much larger than this average)
Red Hat Linux system	5 - 10 GB

A.2.2 Traffic Element

The following table describes the estimated backup capacity for the Mobile Messaging Traffic Element. The required capacity may vary from the numbers listed here they depend on the system capacity and dimensioning. The capacities listed here are average numbers.

Component	Average Backup Capacity Required
RTR	50 - 100 MB
HUB	<10 MB

Component	Average Backup Capacity Required
AMS	500 - 2500 MB (this average indicates the backup capacity, including the database; however, the database size depends on your configuration and may be much larger than this average)
PBC	50 - 100 MB
FAF	50 - 100 MB
DMF	500-1000 MB (this average indicates the backup capacity, including the Intercept and output files; however, the size depends on your configuration and may be larger than this average).
Red Hat Linux system	5 - 10 GB

A.2.3 Subscriber Element

The following table describes the estimated backup capacity for the Mobile Messaging Subscriber Element.

Component	Average Backup Capacity Required
SPF	10 - 100 GB (depending on the amount of subscribers and provisioned data)
Red Hat Linux system	5 - 10 GB

A.2.4 Logging Element

The following table describes the estimated backup capacity for the Mobile Messaging Logging Element.

Component	Average Backup Capacity Required
LGP	Can be terabytes (this average indicates the backup capacity, including the database; however, the database size depends on your configuration and may be much larger than this average)
Red Hat Linux system	5 - 10 GB

Note: Using the following step we can find the size of LGP, PBC and SPF database in GB:

1. Login to LGP/PBC/SPF machine as `root`:
2. Execute:

```
# mysql --login-path=mysql_root

mysql> SELECT round(sum( data_length + index_length ) / 1024 / 1024 /1024,6)
"Data Base Size in GB" FROM information_schema.TABLES  WHERE table_schema like
"<database name>";
# exit;
```

Example:

In case of LGP database:

```
# mysql --login-path=mysql_root
```

```
mysql> SELECT round(sum( data_length + index_length ) / 1024 / 1024 /1024,6)
"Data Base Size in GB" FROM information_schema.TABLES  WHERE table_schema like
"lgp";
```

Sample output:

```
+----------------------+
| Data Base Size in GB |
+----------------------+
|            33.556931 |
+----------------------+
1 row in set (9.99 sec)
```

A.3 Rotation Schema

This following table describes the recommended backup rotation schema per Mobile Messaging component. It is a recommendation and therefore other rotation can be used for backup.

Schema	Time	Backup Locations
Daily Backup	03:00	See *Backup Procedure*
Monthly Full Backup	03:00	Full system backup

A.4 Backup Procedure

A.4.1 OAM Element Backup

This section describes the backup of the Operations, Administration, and Maintenance (OAM) Element, which is running the following Mobile Messaging components:

- Manager (MGR)
- Statistics Viewer (STV)
- Customer Care Interface (CCI)

A.4.1.1 Backup Locations

The following files and directories should be backed up for an OAM Element:

Locations	Description
`/usr/TextPass/etc`	Mobile Messaging configuration, data, and license files
`/usr/TextPass/.store`	License data
`/usr/TextPass/.crypt`	SMS Content Encryption files (Red Hat Linux only)
`/var/TextPass/MGR`	MGR data file, logs, and traces

Locations	Description
`/var/TextPass/CCI`	CCI data file, logs, and traces
`/var/TextPass/STV`	STV data file, logs, and traces
`/var/TextPass/BAT`	BAT data file, logs, and traces
`/backup`	Crontab backups
`/var/log/STV`	Log files
`/etc`	Configuration files
`/var/lib/mysql-cluster/config.ini`	MySQL Cluster configuration file

To backup the paths mentioned in the above table, execute the following commands as user `root`:

```
mkdir -p /Backup/textpass

chown -R textpass:textpass /Backup/textpass
cp -r /usr/TextPass/etc /Backup
cp -r /var/TextPass/MGR /Backup
cp -r /var/TextPass/CCI /Backup
cp -r /var/TextPass/STV /Backup
cp -r /var/TextPass/BAT/ /Backup
cp -r /var/TextPass/textpassdmf /Backup

cp -r /backup /Backup
cp -r /data /Backup
cp -r /var/log/STV /Backup
cp -r /etc /Backup


cp -r /var/lib/mysql-cluster/config.ini /Backup
cp -r /var/TextPass/BAT/ /Backup
su - textpass -c "cp -r .store /Backup/textpass"
su - textpass -c "cp -r .crypt /Backup"
```

Note: If the multiple instance feature is enabled, the `.store` directory needs to be stored for the multiple-instance users too. For each multi-instance user name `<username>`, execute:

```
mkdir -p /Backup/<username>
chown -R <username>:<username> /Backup/<username>
su - <username> -c "cp -r .store /Backup/<username>"
```

A.4.1.2 MySQL Database Backup

The OAM Element has a MySQL database and it is recommended to back up this database.

Mobile Messaging components use MySQL databases for which the data is located in specific partitions for each component. Refer to the Mobile Messaging operating system installation manuals (see *References*) for the recommended Mobile Messaging partition schemes. To ensure the correct state of the database, a cronjob can be used to create a daily copy of the database and put this in the `/backup` partition.

It is recommended to backup the MGR and STV databases separately as outlined in *MGR Database Backup* and *STV Database Backup*.

The CCI does not have its own database, but it writes/queries information that are in the AMS and/or SPF databases.

A.4.1.2.1 MGR Database Backup

To make a backup of the MGR databases only, the line below should be placed in the root `crontab`. It will first lock the database tables at 02:00 in the morning and create a database dump to the following dump file: `/backup/mgr_backup_YYYYMMDDHHMMSS.sql.gz`.

The required time for the copy depends on the size of the database. During this time the database is not available for queries or inserts.

Rotation Schema	Crontab Command
`00 2 * * *`	`su - root -c "/usr/TextPass/bin/tp_mgr_backup -name=/Backup/mgr_backup"`

It will create a backup file containing all domains. When no name is specified, the default name is: `/backup/mgr_databases.sql_<date>.gz`

Note: A backup is automatically made when you use `tp_install_mgr`.

A.4.1.2.2 STV Database Backup

To make a backup of the STV databases only, the line below should be placed in the root `crontab`. It first will lock the database tables at 02:30 in the morning and create a database dump to the following dump file: `/backup/stv_backup_YYYYMMDDHHMMSS.sql.gz`.

The required time for the copy depends on the size of the database. During this time the database is not available for queries or inserts.

Note: Due to the size of the STV database, this can require a considerable amount of disk space and time.

Rotation Schema	Crontab Command
`30 2 * * *`	`mysqldump --login-path=mysql_root --opt --add-drop-database --databases stv_statistics stv_aggregates stv_poller stv_import stv_log > /Backup/stv_backup_`date +\%Y_\%m_\%d_\%H_\%M_\%S`.sql`

A.4.1.2.3 CCI Database Backup

To make a backup of the CCI database only, the line below should be placed in the root `crontab`. First , it will lock the database tables at 02:00 in the morning and create a database dump to the following dump file: `/tmp/cci_databases.sql_2007_12_13_15_41_00.gz`.

The required time for the copy depends on the size of the database. During this time the database is not available for queries or inserts.

Rotation Schema	Crontab Command
`00 2 * * *`	`su - root -c "/usr/TextPass/bin/tp_cci_backup -name=/tmp/"`

It will create a backup file containing all domains. When no name is specified, the default name is `/tmp/cci_databases.sql_<date>.gz`.

A.4.2 Traffic Element Backup

This section describes the backup of the Traffic Element, which is running the following Mobile Messaging components:

- Router (RTR)
- HUB
- Active Message Store (AMS)
- Firewall Advanced Filters (FAF)
- Prepaid Billing Controller (PBC) without database
- Subscriber Subscription Information (SSI) server
- IMS Interworker (IIW)
- Direct Message Filter (DMF)

A.4.2.1 Backup Locations

The following files and directories should be backed up for a Traffic Element:

Locations	Description
`/usr/TextPass/etc`	Mobile Messaging configuration, data, PBC scripts, and license files **Important:** Restoring this entire directory will result in the CDR sequence number being reset back to the value at the time of the backup. If this is not acceptable and you want to start from 0 again, the CDR sequence number files must not be restored to start from 0.
`/usr/TextPass/.store`	License data
`/usr/TextPass/.crypt`	SMS Content Encryption files (Red Hat Linux only)
`/usr/TextPass/.fcl`	AMS identifier
`/etc`	Configuration files

Note: If the multiple instance feature is enabled, the Backup should be taken from each user.

To backup the paths mentioned in the above table, execute the following commands as user `root`:

```
mkdir -p /Backup/textpass
chown -R textpass:textpass /Backup/textpass
cp -r /usr/TextPass/etc /Backup
cp -r /etc /Backup
su - textpass -c "cp -r .fcl /Backup/textpass; cp -r .store /Backup/textpass; cp -r
 .crypt /Backup/textpass;"
```

Note: If the multiple instance feature is enabled, the `.fcl` and `.store` directories need to be stored for the multiple-instance users too. For each multi-instance user name `<username>`, execute:

```
mkdir -p /Backup/<username>
chown -R <username>:<username> /Backup/<username>
su - <username> -c "cp -r .fcl /Backup/<username>; cp -r .store /Backup/<username>"
```

A.4.2.2 RTR-Specific Backup

On the RTR, it is up to the operator whether to back up (and even restore) log and billing files. Typically, the frequency of the backups is much slower than the life-time of the log and billing files, between their creation and processing/removal.

When periodically backing up the log and billing files, you should only back up the `finished` directories, as specified in the logging and billing profiles. You should not back up the `processing` directory, as the files in this directory are incomplete.

- For logging records, execute the following command:
  ```
  cp -r /var/TextPass/log/available/ /Backup
  ```
- For billing records, execute the following command:
  ```
  cp -r /var/TextPass/available/ /Backup
  ```

Note: There may be a `/data` mount point/directory present in the traffic element where logging file and billing files are. User should take back this up as well.

A.4.2.3 AMS-Specific Backup

It is **not recommended** to back up the AMS database as the information stored in the AMS database has a very limited lifetime, at the same time the AMS database is for redundancy purposes replicated to another system.

If a backup is desired (for example, for offline inspection), it is recommended that you create a backup script to make a snapshot of the database to a temporary location (for example `/backup`). Then backup the database from this temporary location.

Parameter	Sample Locations
`amsdbdatabasedirectorymaster`	`/dbamstore/TextPass/MessageStore/master`
`amsdbtransactiondirectorymaster`	`/dbamslog/TextPass/MessageStore/master`
`amsdbdatabasedirectoryreplica`	`/dbamstore/TextPass/MessageStore/replica`
`amsdbtransactiondirectoryreplica`	`/dbamslog/TextPass/MessageStore/replica`

Note: AMS will be unavailable when taking AMS database backup.

To manually back up the master and replica AMS databases and log files, use following steps as example:

1. Log in to the Traffic Element (master AMS) server as user `textpass`.
2. Stop the AMS process:
   ```
   $ tp_stop --tp_ams
   ```
3. Back up the AMS databases:
   ```
   $ cp -R /dbamsstore/TextPass/MessageStore/master
   /Backup/tpbackup/dbamsstore_master_recover
   $ cp -R /dbamsstore/TextPass/MessageStore/replica
   /Backup/tpbackup/dbamsstore_replica_recover
   ```

4. Back up the AMS database log files

```
$ cp -R /dbamslog/TextPass/MessageStore/master
/Backup/tpbackup/dbamslog_master_recover
$ cp -R /dbamslog/TextPass/MessageStore/replica
/Backup/tpbackup/dbamslog_replica_recover
```

5. Start the AMS process:

```
$ tp_start --tp_ams
```

Note: If you are using volatile storage, there is no static database. If there is only one AMS present, the replica will be empty.

Note: If the multiple instance feature is enabled, the backup should be taken for all AMS databases created for multiple users.

A.4.2.4 PBC Database Backup

A Traffic Element can be configured to only run a PBC + database. The database can be a local MySQL database or an external operator managed Oracle or LDAP database.

It is **not recommended** to back up the PBC transaction database as the information stored in the transaction database has a limited lifetime (24 -72 hours).

The PBC supports the following database types:

- A local or external MySQL database
- An external operator managed LDAP database
- An external operator managed Oracle database

Depending on your specific implementation of the PBC it might be necessary to back up additional locations like the configuration of the database that is used and in rare cases it might be good to backup (parts) of the database.

Because the situation is very implementation-specific, please contact ZephyrTel Support to obtain a specific recommendation for your situation.

Use the following MySQL command line tool to backup the DB:

```
mysqldump --login-path=mysql_root <PBC Database name> > pbc.sql
```

A.4.2.5 DMF Specific Backup

To manually back up the DMF files, use following steps as an example:

1. Log in to the Traffic Element server as user `root`.
2. Stop the DMF process:

```
# su - textpass -c "tp_stop --tp_dmf"
```

3. Back up the DMF files:

```
$ cp -Rp /var/TextPass/DMF /Backup/tpbackup/
$ cp -Rp /var/TextPass/textpassdmf /Backup/tpbackup/
```

4. Start the DMF process:

```
# su - textpass -c "tp_start --tp_dmf"
```

Note: If the multiple instance feature is enabled, the backup should be taken for all the users.

A.4.3 Subscriber Element Backup

This section describes the backup of the Subscriber Element, which is running the following Mobile Messaging components:

- Subscriber Provisioning Framework (SPF)
- Black- and Whitelist (XS-BWL)
- Short Message Copy (XS-CPY)
- Distribution List (XS-DIL)
- Short Message Forward (XS-FWD)
- Auto-Reply (XS-ARP)
- Signature (XS-SIG)
- MultiList Control (XS-MLC)
- Modifier (XS-MOD)
- Text Insertion Engine (XS-TIE)

Note: It is not necessary to back up the "slave" site in a MySQL Cluster replication configuration.

A.4.3.1 Backup Locations

The following files and directories should be backed up for a Subscriber Element:

Locations	Description
`/usr/TextPass/etc`	Mobile Messaging configuration, data, and license files
`/usr/TextPass/.store`	License data
`/etc`	Configuration files
`/dbspf/mysqlcluster/BACKUP/`	Default MySQL Cluster backup

To backup the paths mentioned in the above table, execute the following commands as user `root`:

```
mkdir -p /Backup/textpass
chown -R textpass:textpass /Backup/textpass
cp -r /usr/TextPass/etc /Backup
cp -r /etc /Backup
su - textpass -c "cp -r .store /Backup/textpass;"
```

A.4.3.2 MySQL Database Backup

The Subscriber Element has a MySQL Cluster database for the SPF. This section describes a backup procedure that is native to the NDBcluster storage engine used by MySQL Cluster. For more information, refer to *http://dev.mysql.com/doc/mysql-cluster-excerpt/5.5/en/mysql-cluster-backup.html*

This procedure allows for a hot snapshot, and will generate the following files per data node in the default backup directory `/dbspf/mysqlcluster/BACKUP/`:

1. A *metadata* file, containing names and definitions of all database tables: `/dbspf/mysqlcluster/BACKUP/BACKUP-<backup_id>.<node_id>.ctl`
2. A *records* file, containing the data actually stored in the database tables at the time that the backup was made: `/dbspf/mysqlcluster/BACKUP/BACKUP-<backup_id>.<node_id>.data`

3. A *transaction* log file, which records how and when data was stored in the database `/dbspf/mysqlcluster/BACKUP/BACKUP-<backup_id>.<node_id>.log`

`<backup_id>` stands for the backup identifier and `<node_id>` is the unique identifier for the node creating the file. `<backup_id>` can be specified in the `START BACKUP` command, but it is easier to accept the backup identifier that is generated automatically.

The backup process is initiated simply by issuing the following command on the MySQL Cluster management node (the OAM Element):

```
$ ndb_mgm -e "START BACKUP"
```

This command causes the shell to wait until the backup process is complete before returning to the prompt. The output of this command will contain the backup identifier. This will be used during the restore procedure later on.

It is also possible to abort a backup in progress from a system shell using this command:

```
$ ndb_mgm -e "ABORT BACKUP <backup_id>"
```

If the MySQL server and cluster software are going to change as part of the Subscriber Element upgrade, then the backup procedure also needs to take care of the 'spf' database schema, by issuing the following command:

```
$ mysqldump --login-path=mysql_root  --no-data  spf > /backup/tpbackup/
spf_db_schema_only.sql
```

A.4.3.3 Sample Backup Session

This section describes the installation and configuration of a MySQL Cluster on the following elements (the IP addresses are examples only):

- Two combined data/SQL nodes: Subscriber Element 1 (IP 10.0.0.111) and Subscriber Element 2 (IP 10.0.0.112)
- One management node: OAM Element (IP 10.0.1.240)

To verify the current MySQL Cluster setup, execute the following commands on the OAM Element:

```
$ ndb_mgm
```

Sample output:

```
-- NDB Cluster -- Management Client --
ndb_mgm> show
```

Note: If the node is connected, the IP address, MySQL and NDB versions will be shown. Otherwise, the node is described as "not connected".

To verify the current SPF database characteristics, on the Subscriber Elements use the following commands:

```
# mysql --login-path=mysql_root  -Dspf -e "SELECT COUNT(*) FROM SUBSCRIBER"
```

Sample output:

```
+----------+
| COUNT(*) |
+----------+
|   465001 |
+----------+
```

Note: There can be a few seconds lag time between cluster nodes, therefore the total subscriber count may differ a little bit between cluster nodes.

```
# mysql --login-path=mysql_root  -Dspf -e "SHOW TABLES"
```

Sample output:

```
+---------------------------------+
| Tables_in_spf                   |
+---------------------------------+
| 1_originator_list               |
| 1_recipient                     |
| 1_recipient_base_disabled       |
| 1_recipient_base_enabled        |
| 2_cpy_disabled                  |
| 2_cpy_enabled                   |
| 3_cpy_disabled                  |
| 3_cpy_enabled                   |
| 4_list                          |
| 4_recip_list                    |
| 4_recipient                     |
| 4_subscriber                    |
| 4_subscriber_base_disabled      |
| 4_subscriber_base_enabled       |
| 5_fwd_disabled                  |
| 5_fwd_enabled                   |
| chr_subscriber                  |
| profile                         |
| profile_contains_service        |
| profile_indexes                 |
| properties                      |
| service                         |
| service_status                  |
| subscriber                      |
| subscriber_active_orig_services |
| subscriber_active_recip_services|
| subscriber_times                |
+---------------------------------+
```

To start the backup:

1. Log in as textpass on the OAM Element (the MySQL management node).
2. Start the backup as follows:

   ```
   $ ndb_mgm -e "START BACKUP"
   ```

   Sample output:

   ```
   Connected to Management Server at: localhost:1186
   Waiting for completed, this may take several minutes
   Node 3: Backup 1 started from node 1
   Node 3: Backup 1 started from node 1 completed
    StartGCP: 162918 StopGCP: 162937
    #Records: 17088312 #LogRecords: 72
    Data: 799839272 bytes Log: 33768 bytes
   ```

3. On both Subscriber Elements, verify that the required backup files were generated as follows:

   a. Log in as root on Subscriber Element 1.

   b. Execute:

      ```
      # ls -ltr /dbspf/mysqlcluster/BACKUP/BACKUP-1/
      ```

      Sample output:

      ```
      total 390940
      -rw-r--r-- 1 root root 399821940 Oct 15 12:17 BACKUP-1-0.2.Data
      -rw-r--r-- 1 root root     83880 Oct 15 12:17 BACKUP-1.2.ctl
      -rw-r--r-- 1 root root     11320 Oct 15 12:17 BACKUP-1.2.log
      ```

      Note: The `<backup_id>` of 1 will be incremented every time a backup is made.

c. Log in as root on Subscriber Element 2.

d. Execute:

```
# ls -ltr /dbspf/mysqlcluster/BACKUP/BACKUP-1/
```

Sample output:

```
total 391148
-rw-r--r-- 1 root root 400019500 Oct 15 12:17 BACKUP-1-0.3.Data
-rw-r--r-- 1 root root     83880 Oct 15 12:17 BACKUP-1.3.ctl
-rw-r--r-- 1 root root     22552 Oct 15 12:17 BACKUP-1.3.log
```

Note: The <backup_id> of 1 will be incremented every time a backup is made.

A.4.4 Logging Element Backup

This section describes the backup of the Logging Element, which is running the Log Processor (LGP) component.

A.4.4.1 Backup Locations

The following files and directories should be backed up for a Logging Element:

Locations	Description
/usr/TextPass/etc	Mobile Messaging configuration, data, and license files
/usr/TextPass/.store	License data
/etc	Configuration files

To backup the paths mentioned in the above table, execute the following commands as user root:

```
mkdir -p /Backup/textpass
chown -R textpass:textpass /Backup/textpass
cp -r /usr/TextPass/etc /Backup
cp -r /etc /Backup
su - textpass -c "cp -r .store /Backup"
```

Note: If the multiple instance feature is enabled, the .store directory needs to be stored for the multiple-instance users too. For each multi-instance user name <username>, execute:

```
mkdir -p /Backup/<username>
chown -R <username>:<username> /Backup/<username>
su - <username> -c "cp -r .store /Backup/<username>"
```

A.4.4.2 LGP Database Backup

The Logging Element has a MySQL database.

It is **not recommended** to backup the LGP database as the information stored in the LGP database has a limited lifetime. Also, the LGP database can be very large depending on your specific setup.

If backups of this database are required, mysqldump is recommended to be used for creating the backup. Before backing up the LGP database you need to verify if enough disk space is available for the backup.

For example, use the following commands to create a `mysqldump` of the complete database:

```
# su - textpass
/etc/init.d/textpass_tools stop
mysqldump --login-path=mysql_root  --all-databases > /Backup/LGP_Database_backup_`date
+%Y%m%d`.sql
/etc/init.d/textpass_tools start
```

A.5 Restore Procedure

A.5.1 Introduction

This chapter describes recommendations for restoring Mobile Messaging elements.

CAUTION: Before beginning any of these procedures, contact the ZephyrTel Support Hotline and inform them. ZephyrTel Support Hotline number is available 24X7 across the globe.

- Direct Support Number: +1-888-586-3257
- ZephyrTel General Support Number: +1-512-861-1974
- Email: mmsupport@zephyrtel.com

A.5.2 System Restore

If a node suffers serious damage, you may want to restore from backup. In that case, ZephyrTel recommends fully re-installing the element, including the operating system (OS). This procedure is the same as the OS installation procedure. Afterwards, replace the backup files.

Install Mobile Messaging software
Determine the type of element you need to install on the server:

- OAM Element
- Traffic Element
- Logging Element
- Subscriber Element
- Full Element (all packages excluding SPF and XS)

Install the Mobile Messaging software by following the complete installation manual for the element type that you need to install.

Refer to *References* for a list of the OS and Mobile Messaging installation manuals.

A.5.3 OAM Element Restore

To restore the OAM Element backups:

1. Restore the files from the backup location specified in *Backup Locations*.

```
cp -r /Backup/etc/* /usr/TextPass/etc
cp -r /Backup/textpass/.store/* /usr/TextPass/.store
cp -r /Backup/textpass/.crypt/* /usr/TextPass/.crypt
cp -r /Backup/MGR/* /var/TextPass/MGR
cp -r /Backup/CCI/* /var/TextPass/CCI
cp -r /Backup/STV/* /var/TextPass/STV
```

```
cp -r /Backup /BAT/* /var/TextPass/BAT/
cp -r /Backup/backup/* /backup
cp -r /Backup /data/* /data
cp -r /Backup/var/log/STV/* /var/log/STV
cp -r /Backup/etc/hosts* /etc/hosts
cp -r /Backup/etc/my.cnf /etc/my.cnf
cp -r /Backup/var/lib/mysql-cluster/config.in /var/lib/mysql-cluster/config.ini
cp -r /Backup/etc/sysconfig/rsyslog/* etc/sysconfig/rsyslog
```

2. To restore the MGR database only, use the following command:

   ```
   /usr/TextPass/bin/tp_mgr_restore -name=/backup/mgr_backup_<date>.sql.gz
   ```

   Note: The MGR database backup is made by the `tp_mgr_backup` tool. The `tp_mgr_restore` tool is used to restore the MGR database backup.

3. To restore the CCI database only, use the following command:

   ```
   /usr/TextPass/bin/tp_cci_restore -name=/tmp/cci_databases.sql_<date>.gz
   ```

   Note: The CCI database backup is made by the `tp_cci_backup` tool. The `tp_cci_restore` tool is used to restore the `cci` database backup.

4. To restore the STV database only, use the following command:

   ```
   mysql -uroot -plokal$ < /backup/stv_backup_<date>.sql
   ```

5. Restart the MGR.

A.5.4 Traffic Element Restore

To restore the Traffic Element backups:

1. Restore the files from the backup location specified in *Backup Locations*.

   ```
   cp -r /Backup/usr/TextPass/etc/* /usr/TextPass/etc
   cp -r /Backup/textpass/.fcl /usr/TextPass/.fcl
   cp -r /Backup/textpass/.store /usr/TextPass/.store
   cp -r /Backup/textpass/.crypt /usr/TextPass/.crypt
   cp -r /Backup/etc/hosts /etc/hosts
   cp -r /Backup/etc/my.cnf /etc/my.cnf
   cp -r /Backup/etc/sysconfig/rsyslog/ etc/sysconfig/rsyslog
   ```

   Note: If the backup is taken from multiple users, the backup directory for each user shall also be restored.

   Important: Restoring this entire directory will result in the CDR sequence number being reset back to the value at the time of the backup. If this is not acceptable and you want to start from 0 again, the CDR sequence number files must not be restored to start from 0.

2. Restore the files from the backup location specified in *AMS-Specific Backup*.

   ```
   cp -r /Backup/tpbackup/dbamsstore_master_recover
   /dbamsstore/TextPass/MessageStore/master
   cp -r /Backup/tpbackup/dbamsstore_replica_recover
   /dbamsstore/TextPass/MessageStore/replica
   cp -r /Backup/tpbackup/dbamslog_master_recover
   /dbamslog/TextPass/MessageStore/master
   cp -r /Backup/tpbackup/dbamslog_replica_recover
   /dbamslog/TextPass/MessageStore/replica
   ```

3. Restore the PBC database.

Create the database `<database name>` with the command:

```
mysql --login-path=mysql_root <database name> < pbc.sql
```

Because the situation is very implementation-specific, please contact ZephyrTel Support to obtain a specific recommendation for your situation.

4. Restore the DMF files:

```
cp -Rp /Backup/tpbackup/DMF/* /var/TextPass/DMF/
cp -Rp /Backup/tpbackup/textpassdmf/* /var/TextPass/textpassdmf/
```

A.5.5 Subscriber Element Restore

This section only describes restoring the Subscriber Element on the master site. These instructions assume that the database user name is `root`, the database password is `lokal$`, and the database name is `spf`.

Note: If there are clients in the network that replicate from the master database (such as a slave site), you must have access to the ZephyrTel Mobile Messaging OAM Element and Traffic Element Installation Manuals to complete this procedure.

To fully restore the database on the Subscriber Elements:

1. Restore the files from the backup location specified in *Backup Locations*.

   The following steps describe how to restore the MySQL Cluster using the example described in *Sample Backup Session*

2. On all Subscriber Elements, stop the SPF core:

```
# su - textpass -c "tp_stop"
```

   Sample output:

```
Stopping SPFCORE on spf3
Stopping tp_fclient on spf3
Stopping tp_mgrd on spf3
```

3. On all Subscriber Elements, log in to MySQL and stop the slave:

```
mysql -uroot -plokal$ -e "stop slave;"
mysql -uroot -plokal$ -e "drop database spf;"
mysql -uroot -plokal$ -e "create database spf;"
```

4. On all Subscriber Elements, stop MySQL.

```
# systemctl stop mysql
```

   Sample output:

```
Shutting down MySQL.....                                   [  OK  ]
```

5. On the OAM Element, verify that the Subscriber Elements are no longer connected:

```
$ ndb_mgm -e "SHOW"
```

   Note: If the node is connected, the IP address, MySQL and NDB versions will be shown. Otherwise, the node is described as "not connected".

6. On the OAM Element, stop the data nodes:

```
$ ndb_mgm -e "ALL STOP"
```

Sample output:

```
Connected to Management Server at: localhost:1186
Executing STOP on all nodes.
NDB Cluster has shutdown.
```

Execute:

```
$ ndb_mgm -e "SHOW"
```

7. On all Subscriber Elements, restart the data nodes with the initial flag to remove all data from the database.

   ```
   # /usr/local/sbin/ndbmtd --initial
   ```

   Wait until the state of the Subscriber Elements is no longer "starting" before you continue to the next step (verify the state using the `ndb_mgm -e "SHOW"` command on the OAM Element).

   At this point, no SPF tables will be in the database (only views will remain, as they are not clustered).

8. On any one of the Subscriber Elements, execute the following steps to restore the SPF database schema:

   a. Start MySQL:

   ```
   # systemctl start mysql
   ```

   Sample output:

   ```
   Starting MySQL.....        [  OK  ]
   ```

   b. Restore the SPF database schema:

   ```
   # mysql --login-path=mysql_root spf < /backup/tpbackup/spf_db_schema_only.sql
   ```

   Note: SPF Schema restore must be performed on one SPF server only.

   c. Verify that the SPF DB tables are correctly restored:

   ```
   # mysql --login-path=mysql_root
   mysql> use spf;
   mysql> show tables;
   ```

   Sample Output:

   ```
   mysql> show tables;
   +-------------------------+
   | Tables_in_spf           |
   +-------------------------+
   | 1_cpy                   |
   | 2_fwd                   |
   | abl_template            |
   | arp_template            |
   | bwl_template            |
   | contact                 |
   | contact_group           |
   | cpy_template            |
   | dil_template            |
   | fwd_template            |
   | master_time             |
   | profile                 |
   | profile_contains_service |
   | profile_indexes         |
   | profile_stats           |
   | properties              |
   | schedule                |
   | schedule_template       |
   | service                 |
   | service_status          |
   ```

```
| sig_template              |
| subscriber                |
| subscriber_times          |
+---------------------------+
23 rows in set (0.01 sec)

mysql> show table status like '1_cpy';
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Name  | Engine     | Version | Row_format | Rows | Avg_row_length |
Data_length | Max_data_length | Index_length | Data_free | Auto_increment |
Create_time | Update_time | Check_time | Collation  | Checksum | Create_options
     | Comment |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 1_cpy | ndbcluster |      10 | Fixed      |    0 |              0 |
   0 |              0 |            0 |         0 |           NULL | NULL
    | NULL        | NULL       | latin1_bin |     NULL | max_rows=100000000 |
         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
1 row in set (0.00 sec)
```

d. Stop MySQL:

```
# systemctl stop mysql
```

Sample output:

```
Shutting down MySQL.....                                         [ OK ]
```

9. On all Subscriber Elements, execute `ndb_restore` (do so on one Subscriber Element after another):

```
# /usr/local/mysql/bin/ndb_restore -c <OAM Element>:1186 -n \
<node_id> -b <backup_id> -r --backup_path=</path/to/backup/files> \
--include-databases=<database_name>
```

For example, on Subscriber Element 1, execute this command:

```
# /usr/local/bin/ndb_restore -n 2 -b 1 -r \
--backup_path=/dbspf/mysqlcluster/BACKUP/BACKUP-1/ --include-databases=spf
```

For example, on Subscriber Element 2, execute this:

```
# /usr/local/bin/ndb_restore -n 3 -b 1 -r \
--backup_path=/dbspf/mysqlcluster/BACKUP/BACKUP-1/ --include-databases=spf
```

10. Bring the MySQL Cluster back online.

a. On all Subscriber Elements, start MySQL.

```
# systemctl start mysql
```

Sample output:

```
Starting MySQL.....                                      [  OK  ]
```

b. On the OAM Element, verify that the MySQL Cluster is back online:

```
$ ndb_mgm -e "SHOW"
```

11. On all Subscriber Elements, confirm that the data is restored:

```
# mysql --login-path=mysql_root -Dspf -e "SELECT COUNT(*) FROM SUBSCRIBER"
```

Sample output:

```
+----------+
| COUNT(*) |
+----------+
|   465001 |
+----------+
```

Note: The total subscriber count does not have to be equal to the subscriber count at the time of backup, but realistically it should not differ much.

12. On all Subscriber Elements, stop MySQL.

```
# systemctl stop mysql
```

Sample output:

```
Shutting down MySQL.....                                   [  OK  ]
```

13. On the OAM Element, stop the data nodes:

```
$ ndb_mgm -e "ALL STOP"
```

Sample output:

```
Connected to Management Server at: localhost:1186
Executing STOP on all nodes.
NDB Cluster has shutdown.
```

Execute:

```
$ ndb_mgm -e "SHOW"
```

14. On all Subscriber Elements, start `ndbmtd`.

```
# systemctl start ndbmtd
```

Sample output:

```
2011-03-23 16:17:54 [ndbd] INFO     -- Angel connected to '10.0.1.240:1186'
2011-03-23 16:17:54 [ndbd] INFO     -- Angel allocated nodeid: 2
Starting /usr/local/sbin/ndbmtd succeeded.
```

15. On all Subscriber Elements, start MySQL.

```
# systemctl start start
```

Sample output:

```
Starting MySQL.....                                        [  OK  ]
```

If there are no clients in the network that replicate from the master database, then the restore procedure is complete.

Note: After `ndb_restore` has finished and `ndbmtd` is running with the restored data, the internal counter that is used as implicit backup ID will be to 1. If you perform a backup using the command `ndb_mgm -e "start backup"`, the `ndb_mgm` process will attempt to create backup number 1 in the backup directory (by default, `/dbspf/mysqlcluster/BACKUP`). If a backup with ID 1 already exists (that is, `/dbspf/mysqlcluster/BACKUP/BACKUP-1`), the command will fail and no backup will be created. To resolve this situation, you must do one of the following:

- Explicitly set the internal counter to the first non-existing backup ID. For example, if the first non-existing backup ID is 51, execute `ndb_mgm -e "start backup 51"`
- Resolve the conflicting paths, such as by moving the backups to another location. For example, `mv /dbspf/mysqlcluster/BACKUP /dbspf/mysqlcluster/BACKUP-OLD`

After you have restored the database restored from backup, all backups that you created after the one that you used for restoration, up to the restoration time, are obsolete.

16. On all Subscriber Elements, log in to MySQL and reset the master:

```
# mysql --login-path=mysql_root
mysql> RESET MASTER;
```

17. On all Subscriber Elements, start the SPF core:

    ```
    # su - textpass -c "tp_start"
    ```

    Sample output:

    ```
    Starting SPFCORE on spf3
    Starting tp_fclient on spf3
    Starting tp_mgrd on spf3
    ```

    If there are any clients in the network that replicate from the master database (a slave site), continue with the procedure to restore replication:

18. Follow the "Configure MySQL Cluster Replication" procedure in the Subscriber Element Installation Manual.

Replication of the master database should now be restored.

A.5.6 Logging Element Restore

To restore the Logging Element backups:

1. Restore the files from the backup location specified in *Backup Locations*.

   ```
   cp -r /Backup/usr/TextPass/etc  /usr/TextPass/etc
   cp -r /Backup/textpass/.store  /usr/TextPass/.store
   cp -r /Backup/etc/hosts   /etc/hosts
   cp -r /Backup/etc/my.cnf  /etc/my.cnf
   cp -r /Backup/etc/sysconfig/rsyslog etc/sysconfig/rsyslog
   ```

   Note: If the multiple instance features is enabled, the following directories also need to be restored:

   - `/usr/<username>`
   - `/var/<username>`

   Replace the `<username>` with each multi-instance user name.

2. If a backup was made of the LGP database with `mysqldump` and you want to restore it:

   a. Stop the LGP process:

      ```
      # systemctl stop textpass
      ```

   b. Restore the LGP database:

      ```
      mysql --login-path=mysql_root < /Backup/LGP_Database_backup_<date>.sql
      ```

   c. Start the LGP process:

      ```
      # systemctl start textpass
      ```

Appendix B

References

Topics:

- *References.....49*

B.1 References

1. MySQL Reference Manual, Online Backup of MySQL Cluster (*http://dev.mysql.com/doc/mysql-cluster-excerpt/5.1/en/mysql-cluster-backup.html*)
2. ZephyrTel Mobile Messaging RHEL 7.6 Installation Manual (MO006404)
3. ZephyrTel Mobile Messaging Installation Manuals

Glossary

A

AMS	Active Message Store Provides store-and-forward functionality for SMS messages.

B

BAT	Batch Server Message distribution application that can send the same short message to multiple recipients.

C

CCI	Customer Care Interface A Web-based interface that allows customer care agents to assist SMS subscribers.
CDR	Call Detail Record This refers to the recording of all connections in a database to permit activities such as billing connection charges or network analysis. CDR files are used in public switched networks, IP networks, for IP telephony, and mobile communications networks. Charging Data Record Used for user billing: a telecom provider transfers them from time to time in order to send bills to their users.

D

DMF	Direct Message Filter Application component that consumes Intercept files generated by RTR, so it must run with RTR on the same Traffic Element. This

D	
	component will regularly monitor for new Intercept Files generated by the RTR.
F	
FAF	Firewall Advanced Filter Works in combination with the Firewall to filter messages, modify message content, and alert network operators of increases in SMS-related traffic.
FTP	File Transfer Protocol A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.
H	
HUB	Works in combination with the Router to manage traffic to and from SMS applications.
I	
IIW	IMS InterWorking Works in combination with the router to provide gateway functionality between IMS domain and SS7 domain.
ISO	International Standards Organization
L	
LGP	Log Processor Collects and processes data for the Log Viewer to display.
M	

M

MGR	A Web-based interface for managing ZephyrTel Mobile Messaging components. Prior to Suite 6, the Configuration Manager (CM) provided this functionality.

O

OAM	Operations, Administration, and Maintenance The application that operates the Maintenance and Administration Subsystem which controls the operation of many ZephyrTel products.
OS	Operating System

P

PBC	Prepaid Billing Controller Performs prepaid charging using the Diameter, CAMEL, or SMPP+ interface.

R

RTR	Router Routes all types of SMS traffic.

S

SPF	Subscriber Provisioning Framework The Mobile Messaging solution to enable the configuration, control and application of subscriber-specific services. The SPF provides a framework to store and retrieve service-specific data through a variety of provisioning interfaces.
SSI	Service Subscription Information The Mobile Messaging SSI can be queried to determine the applicable

S

	personalized subscriber services of the originator and recipient of the message.
STV	Statistics Viewer Collects statistical data about ZephyrTel Mobile Messaging components and displays it in the Manager.

X

XS	eXternal Service Value-adding component that communicates with the Router to provide a service.
XS-ARP	eXternal Service Auto Reply component eXternal Service component that provides SMS auto reply functionality.
XS-BWL	Black- and Whitelist component eXternal Service component that provides personalized blacklist and whitelist services for home network subscribers.
XS-CPY	Short Message Copy component eXternal Service component that can send a copy of MO, MT, and AT short messages to MSISDNs.
XS-DIL	Distribution List component eXternal Service component that provides distribution list functionality.
XS-FWD	Short Message Forward component

X

	eXternal Service component that can forward short messages to MSISDNs.
XS-MLC	MultiList Control component eXternal Service component that can look up a recipient address in a set of configured lists.
XS-MOD	Modifier component eXternal Service component that provides configurable manipulation of certain routing fields.
XS-SIG	eXternal Service Signature component eXternal Service component that provides SMS signature functionality.
XS-TIE	Text Insertion Engine component eXternal Service component that can insert additional text in a short message that is bound for home network subscriber.