trellis™

The TRELLIS™ Real-Time Infrastructure Optimization Platform

Backup and Restore Procedure for Red Hat® Linux®

Technical Bulletin

EMERSON™
Network Power

For important safety information, visit:
www.emersonnetworkpower.com/ComplianceRegulatoryInfo

This document supports versions up to and including release 4.0.2.

TABLE OF CONTENTS

Overview **1**
Platform Database Backup and Restore **3**
Cold Backup 3
Cold Restore 5
License Server Reset and Reinstall 5
License Reissue After the License Server Reset 6
Database Backup and Recovery Tool **9**
Incremental Backups 9
Oracle® Database Configuration 9
Host server file backup 10
Tool Configuration 10
Fast Recovery Area Size 10
Fast Recovery Area Location 11
Modify Backup Schedule 11
Reports 11
Restore Database 12
Database Threshold Notification 12
Avocent® Universal Management Gateway Appliance Backup and Restore **15**
MSS Engine Manual Backup Process 15
MSS Engine Automated Backup Process 16
Appliance and MSS Engine Restore Process 17
MSS Engine Restore 17

Overview

The *Trellis*™ Real-Time Infrastructure Optimization Platform and the Avocent® Universal Management Gateway appliance may require a backup to restore a current or new system. An administrator, who has experience with Red Hat® Linux® commands, can perform the back up and restore procedures. If you are restoring to a new system, the operating system and the *Trellis*™ platform software version must be the same as the existing system. The same internal files and directories will exist in both systems after the restoration is complete.

NOTE: This document describes how to back up and restore the *Trellis*™ platform software, version 3.4 and higher.

The following tools can be used to back up and restore the system database:

- The *Trellis*™ platform database cold backup and restore procedure enables you to create backups of all of the *Trellis*™ platform and the operating system files in order to restore all of the platform contents on a new server.
- The *Trellis*™ platform database backup and recovery tool - RMAN provides a continuous incremental hot backup of the database, a backup of all schemas, including *Trellis*™ platform users, and allows a database restore to a point in time.

Platform Database Backup and Restore

Cold Backup

The cold backup process enables you to create backups of all of the *Trellis*™ platform and the Red Hat® operating system files in order to restore the platform onto a new server.

To create a cold backup:

1. As **oracle**, enter the following to stop the platform on the front and back machines:

   /etc/init.d/Trellis stop

2. On the front and back machines, find and kill the process ID servicing port 5556 to stop the Node Manager service.

   a. Enter **netstat -anp|grep 5556** to find the process ID servicing port 5556.

   b. Enter **kill -1 <process id>** to re-execute the **netstat -anp|grep 5556** command and check if the process ID still exists.

   c. If the process ID still exists, execute the command **kill -9 <process id>.**

3. As **root**, enter the following to stop the Oracle database on the back machine.

   /etc/init.d/oracle stop

4. As **root**, enter the following to stop the emerson-license server on the back machine.

   /etc/init.d/emerson_licenseserver stop

5. Using the following list of files and folders, create a backup of the back machine. This list should be used as a guideline as configurations may differ for each system. It is recommended that the list is tested for each instance. The directories and files starting from /usr, /var and /etc are copied as root and restored as root. The directories starting from /home and /u* are copied as oracle and restored as oracle user.

Back Machine Files and Directories

Directories	Files	Symbolic Links (To Be Re-created)	Configuration
/home/oracle	/etc/rsyslog.conf	/usr/sbin/rcemerson_licenseserver to /etc/init.d/emerson_licenseserver	Syslog Configuration
/usr/lib/licenseserver	/etc/logrotate.d/Trellis	/usr/sbin/rcemerson_sliserver to /etc/init.d/emerson_sliserver	oracle user crontab
/var/log/Trellis	/etc/xinetd.d/nodemanager	/etc/rc5.d/S50emerson_licenseserver to /etc/init.d/emerson_licenseserver	root user crontab
/etc/rc.d/init.d/functions	/etc/sudoers	/etc/rc5.d/S99oracle to /etc/init.d/oracle	n/a
/u01	/var/spool/cron/root	/etc/rc3.d/S50emerson_licenseserver to /etc/init.d/emerson_licenseserver	n/a
/u02	/var/spool/cron/oracle	/etc/rc3.d/S99oracle to /etc/init.d/oracle	n/a

Directories	Files	Symbolic Links (To Be Re-created)	Configuration
/u03	/etc/oraInst.loc	/etc/rc3.d/K99oracle to /etc/init.d/oracle	n/a
/u05	/etc/rc.d/init.d/emerson_ licenseserver	n/a	n/a
/u99	/etc/rc.d/init.d/oracle	n/a	n/a
	/etc/sysconfig/Trellis	n/a	n/a
	/usr/sbin/rcemerson_ licenseserver	n/a	n/a
	/etc/hosts	n/a	n/a
	/etc/passwd	n/a	n/a
	/etc/shadow	n/a	n/a
	/etc/group	n/a	n/a
	/etc/oratab	n/a	n/a
	/etc/rc.d/init.d/Trellis	n/a	n/a
	/etc/ssh/sshd_config	n/a	n/a
	/etc/oratab	n/a	n/a
	/etc/init.d/Trellis	n/a	n/a

6. Using the following list of files and folders, create a backup of the front machine. This list should be used as a guideline as systems may have different configurations. It is recommended that the list be tested for each instance. The directories and files started from /usr, /var and /etc are copied as root user and restored as root user. The directories started from /home and /u* are copied as oracle and restored as oracle user.

Front Machine Files and Directories

Directories	Files	Configuration
/home/oracle	/etc/xinetd.d/nodemanager	/etc/rsyslog.conf
/u01	/etc/sudoers	/etc/logrotate.d/Trellis
/u02	/var/spool/cron/root	/etc/ssh/sshd_config
/u03	/var/spool/cron/oracle	oracle user crontab
/u05	/etc/rc.d/init.d/Trellis	root user crontab

Directories	Files	Configuration
/u99	/etc/sysconfig/Trellis	n/a
	/etc/hosts	n/a
	/etc/passwd	n/a
	/etc/shadow	n/a
	/etc/group	n/a
	/etc/init.d/Trellis	n/a

7. When the backup is complete, restart the operating system as **root**.

NOTE: The License Server, Node Manager and Oracle database services are automatically started with the operating system.

8. As **oracle**, enter **/etc/init.d/trellis start** to start the platform on the back machine.
9. As **oracle**, enter **/etc/init.d/trellis start** to start the platform on the front machine.

Cold Restore

The new instance configuration is a replica of the original failed instance. Changing the IP addresses, hostnames or other configurations are not supported.

WARNING: The *Trellis*™ platform must be re-licensed after a restore. Contact Technical Support for assistance.

To restore from a cold backup:

1. As **oracle**, provision the front and back machines using the kickstart files.
2. Configure the front and back machines as a replica of the original system.
3. On the back machine, restore all the back machine files and folders mentioned in Cold Backup on page 3.

NOTE: Use the root user to create the symbolic links.

4. On the front machine, restore all the front machine files and folders mentioned in Cold Backup on page 3.
5. Reset the license server using the following License Reset procedure.
6. On the back machine, as **root**, enter **/etc/init.d/oracle start** to start the database.
7. On the back machine, as **oracle**, enter **/etc/init.d/trellis start** to start the platform.
8. On the front machine, as **oracle**, enter **/etc/init.d/trellis start** to start the platform.

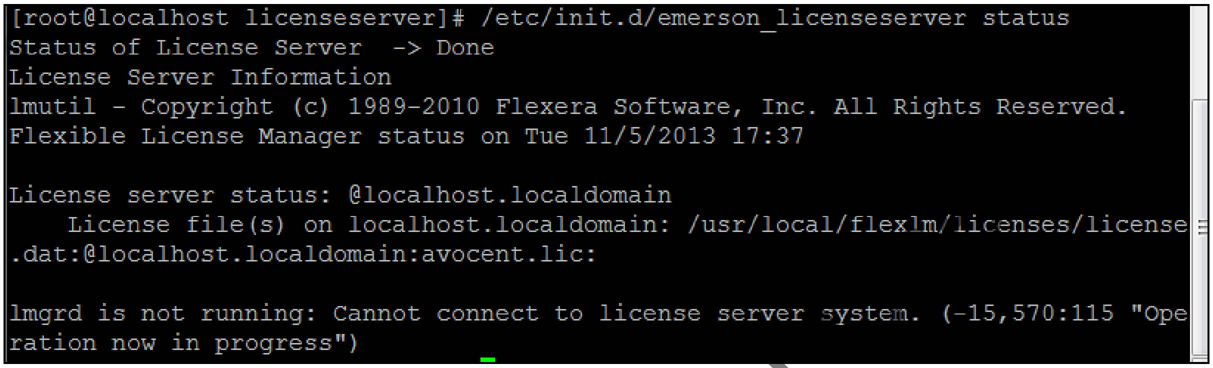
License Server Reset and Reinstall

After the restore is complete, the operating system license server detects the copy and breaks the trust store.

To reset the license server:

1. Before proceeding, ensure the platform software is not running.
2. As **sliuser** (created during the initial SLI installation), log in to the back machine.
3. Enter **cd /usr/lib/licenseserver**.
4. Enter **/etc/init.d/emerson_licenseserver status** to verify the license server is running. If the command returns the following, the server is not running.

Example of Server Reset Failure



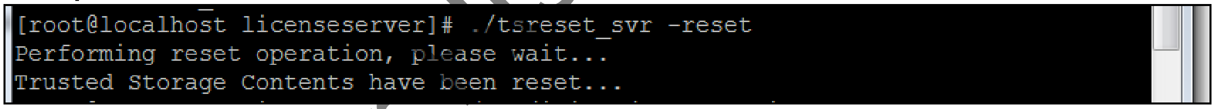
```
[root@localhost licenseserver]# /etc/init.d/emerson_licenseserver status
Status of License Server  -> Done
License Server Information
lmutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved.
Flexible License Manager status on Tue 11/5/2013 17:37

License server status: @localhost.localdomain
    License file(s) on localhost.localdomain: /usr/local/flexlm/licenses/license
.dat:@localhost.localdomain:avocent.lic:

lmgrd is not running: Cannot connect to license server system. (-15,570:115 "Ope
ration now in progress")
```

5. Enter **/etc/init.d/emerson_licenseserver start** to start the license server.
6. Enter **./tsreset_svr –reset from /usr/lib/licenseserver**, to reset the license server.
7. If the license server reset fails, follow the steps to reinstall the license server.

   -or-

   Repeat the steps as the **oracle** user.

Example of a Successful Reset



```
[root@localhost licenseserver]# ./tsreset_svr -reset
Performing reset operation, please wait...
Trusted Storage Contents have been reset...
```

NOTE: If the license server reset is unsuccessful, you must reinstall the license server.

To reinstall the license server:

1. As **root**, enter **/etc/init.d/emerson_licenseserver stop** to stop the license server.
2. Enter the following to /tmp on the back machine.

   cd /tmp to copy the license server installer file sli_install-1.0.1.50
3. Enter **chmod +x sli_install-1.0.1.50** to make the file executable.
4. Enter **./sli_install-1.0.1.50** to run the file. This starts the installation process into the **/usr/lib/licenseserver** folder.
5. Enter **/etc/init.d/emerson_licenseserver start** to start the license server.

License Reissue After the License Server Reset

After the license server is reset, the previous license is returned and a new license is issued. This process can take 30 minutes or more to complete.

NOTE: All licensing activation tasks are completed on the back machine.

To reissue a license:

1. As **root**, log in to the back machine.
2. Copy the script provided by Technical Support, to the back machine.
3. Using a tool, such as dos2unix, verify the script is UNIX compliant. For example:

   ```
   dos2unix ABC7A-T5PNQ-UPDXP-AWZCY_OfflineActivationScript.sh
   ```

4. Run the script following the instructions listed in the header comments of the file and email the produced request.xml files to Technical Support.
5. After Technical Support modifies the files and returns them, run the same script with the **-process**flag and follow the instructions in the header comments.

NOTE: The licenses are returned during normal business hours. A 10-day emergency license can be provided and should be replaced with an official license within the 10 days.

6. After the system is licensed, enter **/etc/init.d/emerson_licenseserver status** to verify the license is available through the license server. The command return output should be similar to the following:

```
/etc/init.d/emerson_licenseserver status
Status of License Server -> Done
License Server Information
lmutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved.
Flexible License Manager status on Tue 7/23/2013 05:00
License server status: 27000@Trellis-back-PS01
License file(s) on Trellis-back-PS01: /usr/lib/licenseserver/avocent.lic:
Trellis-back-PS01: license server UP (MASTER) v11.9
Vendor daemon status (on Trellis-back-PS01):
avocent: UP v11.9
Feature usage info:
Users of CHANGEPLANNER: (Total of 2 licenses issued; Total of 0 licenses in use)
Users of COOLINGSYSTEMSMANAGER: (Total of 1 license issued; Total of 0 licenses in
use)
Users of ENERGYINSIGHT: (Total of 2 licenses issued; Total of 0 licenses in use)
Users of INVENTORYMANAGER: (Total of 2 licenses issued; Total of 0 licenses in use)
Users of PLATFORMCPUCOUNT: (Total of 16 licenses issued; Total of 0 licenses in use)
Users of PLATFORMSERVICES: (Total of 2 licenses issued; Total of 0 licenses in use)
Users of POWERSYSTEMSMANAGER: (Total of 1 license issued; Total of 0 licenses in use)
Users of SITEMANAGER: (Total of 2 licenses issued; Total of 0 licenses in use)
Users of TIERONEDEVICE: (Total of 40000 licenses issued; Total of 4818 licenses in use)
"TIERONEDEVICE" v2.0, vendor: avocent
floating license
root Trellis-back-PS01 /dev/tty (v2.0) (Trellis™-back-PS01/27000 101), start Wed 5/22 9:55,
4818 licenses
Users of TIERTHREEDEVICE: (Total of 1200 licenses issued; Total of 2 licenses in use)
"TIERTHREEDEVICE" v2.0, vendor: avocent
floating license
root Trellis-back-PS01 /dev/tty (v2.0) (Trellis-back-PS01/27000 301), start Mon 5/27 5:10, 2
licenses
Users of TIERTWODEVICE: (Total of 10000 licenses issued; Total of 91 licenses in use)
"TIERTWODEVICE" v2.0, vendor: avocent
floating license
root Trellis-back-PS01 /dev/tty (v2.0) (Trellis-back-PS01/27000 201), start Wed 5/22 9:55, 91
licenses
```

Database Backup and Recovery Tool

An administrator can use the *Trellis*™ platform database backup and recovery tool to perform the following:

- Set up the database to perform online incremental backups
- Modify the backup retention policy
- Change the Fast Recovery Area size
- Change the location of the Fast Recovery Area
- Change the database backup job schedule
- Report the status of the recovery manager incremental backups
- Restore the database to a point in time within the retention policy

The following table defines the most common terms used in this document.

Common Terms

Term	Description
Fast Recovery Area (FRA)	Provides a centralized disk location for backup and recovery files. All of the files needed to completely recover a database are stored in the FRA.
Recovery Manager (RMAN)	Primary utility for the physical backup and recovery of an Oracle database.
Block Change Tracking (BCT)	When enabled on a database, the database backup and recovery manager uses a tracking file to identify changed blocks for incremental backups. Using this file avoids the tool having to scan every block in the data file.
DB_RECOVERY_FILE_DEST	Backups are stored in this fully qualified path.
Archive log mode	Database mode enables archiving of the online redo log.
Online redo log	Includes two or more online redo log files that record all changes made to Oracle database data and control files.

Incremental Backups

The *Trellis*™ platform provides a command line interface tool to protect the data in your Oracle database. The tool enables database incremental backups without server downtime. Each incremental backup contains the database blocks that have changed since the previous backup. The incremental backups are saved for recovery, based on the days set in your retention policy.

Oracle® Database Configuration

The database must be configured before the backup and recovery tool can be used. The platform installer configures the database and dependencies.

The following pre-configuration is applied by the installer:

- The *Trellis*™ database is in archive log mode.
- The default location c:\u03\backup is configured for the FRA.
- BCT is enabled.

Host server file backup

The backup and recovery tool depends on a host server backup of the file system. The file system backup must be able to recover and restore the operating system to a working state. After the operating system is restored, the tool can restore the latest database backup.

Tool Configuration

The database backup and recovery tool, RMAN, is installed automatically on the database server in the **/u01/trellis** directory. The factory default setting for tool functionality is disabled. After the RMAN tool is enabled, you can configure the default values for the Fast Recovery Area location and size, enable Block Change Tracking and schedule the daily backup job.

To configure the tool:

1. As **oracle**, log in to the database host server.
2. At the prompt, execute **/u01/trellis/configure.sh**.
3. Enter option **1** RMAN Configuration, then option **1** Enable RMAN and press **Enter** to enable the RMAN tool.
4. Accept the default FRA location and press **Enter** or enter a new location.
5. Enter **YES** to enable the RMAN tool, execute the first database backup and schedule the backup to the default value at midnight. Full backups of the database include: the complete contents of all data files of the database, the control file, archived redo log files and the server parameter file. With these files, you can perform a complete recovery.

NOTE: The default backups run daily at midnight.

Fast Recovery Area Size

The FRA stores the backups and other critical files. With database size fluctuations, retention policy changes and the increase of backups, the space allocated to the FRA must be adjusted. As you approach the limit, a notification is sent to the platform administrator until the issue is resolved. If you exceed the allocated space, the database ceases to function.

The FRA should be large enough for copies of the data files, control files, online redo log files and archived redo log files, which are needed to recover the database. The copies of these backup files are kept based on the retention policy.

The FRA needs to be sized for your environment. FRA size is calculated based on your database size and usage. For a new installation of the *Trellis*™ platform, the default/recommended minimum is 23355M. To calculate your FRA size, multiply 23355M by three. In this example, your FRA size is 70065M (x 3).

To change the FRA size:

1. As **oracle**, log in to the database host server.
2. Execute **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration to open the Configuration Menu.
3. Select option **2** Modify FRA Settings and press **Enter**.
4. Enter the Fast Recovery Area size and press **Enter**.

Fast Recovery Area Location

The new FRA Location directory should exist prior to setting a new location. Before setting a new FRA location, review the following:

- Place the FRA on a separate disk from your database files to prevent losing your files if a media failure occurs.
- The permanent files and transient files can be left in the previous FRA location.
- The database deletes transient files from the previous FRA location as they become eligible for deletion.

To change the FRA location:

1. As **oracle**, log in to the database host server.
2. Execute **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration to open the Configuration Menu.
3. Select option **2** Modify FRA Settings and press **Enter**.
4. Enter the default FRA size and the new location, then press **Enter**.

Modify Backup Schedule

By default, the start date/time schedule for a backup is daily at midnight. After this, the backup runs on a fixed configurable interval based on this date. The RMAN backup schedule displays the next five scheduled backups.

The start time and interval for the backups can be modified. With a small interval, the backup schedule is more frequent and may require re-evaluating the FRA size. When modifying the backup interval, enter a value between 1 and 99 hours. The value should be less than the retention policy. For example, if the retention policy is one day, use an interval between 1 and 24 hours.

To modify the backup schedule:

1. As **oracle**, log in to the database host server.
2. At the prompt, enter **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration to open the Configuration Menu.
3. Select option **3** Modify Backup Schedule and press **Enter**.
4. Enter the new interval in hours.
5. Enter the starting date and time in the format **DD-MM-YYYY HH:MM:SS**.
6. Enter **YES** to accept the new values.

Reports

Backup reports contain summary and detailed information about previous backup jobs run by the tool. They also include information about the health of the database files.

To view database backup and recovery reports:

1. As **oracle**, log in to the database host server.
2. At the prompt enter **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration to open the Configuration Menu.
3. Enter option **4** Reports and press **Enter**.

4. Enter option **1** Data files status to view a report about the health of the database files.
5. Press any key to return to the Reports Menu.
6. Enter option **2** Backup History.
7. Enter a filename to save the report in a file in your current directory.

Restore Database

The restore database feature allows you to restore the database from a previous backup to a point in time. All current data in the database is overwritten with the backup files for the given date.

To restore the database:

1. Stop the front machine.
2. Stop the back machine.
3. If necessary, restore the operating system files from an operating system backup.
4. As **oracle**, log in to the database host server.
5. At the prompt enter **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration to open the Configuration Menu.
6. Enter option **5** Restore Database.
7. The tool presents a range of available dates to restore the database backups. Enter a date in the DD/MM/YYYY HH:MM:SS format and press **Enter**.

NOTE: If you are outside the range of the available backups, the nearest date is automatically selected.

Database Threshold Notification

A notification is sent when the available space in the database is less than 15%. A critical alert is sent when reclaimable space is less than 3%. To warn the platform administrator of this condition, an entry is added to the Event Viewer of the *Trellis*™ platform scheduler. The database continues to consume space in the flash recovery area until there is no reclaimable space left.

The platform runs a disk space check in the FRA every 15 minutes, updates the Alarm and Event Viewer and sends an email to notify the administrator and RMAN tool users.

To view a notification task:

From the Quick Launch menu in the platform software, select *Scheduler*, and in the Scheduled Tasks window, verify the task for the email notification alarm.

To add users to receive a notification alert:

From the Administration menu in the platform software, select *User* and add a new user with the name **rmannotificationX**, where X is a number between 0 and 9.

NOTE: You must add each user in sequential order starting with rmannotification0. For example, rmannotification0 must be added before rmannotification1, rmannotification1 must be added before rmannotification2 and so on.

FRA files are auto managed. When available space is low, Oracle automatically deletes files that are out of the retention policy. If no files are eligible for automatic deletion, the following steps are required:

- Increase the FRA size.
- Move backups from the FRA to tertiary storage.

Avocent® Universal Management Gateway Appliance Backup and Restore

The Avocent® Universal Management Gateway appliance is a central part of monitoring in the *Trellis*™ platform. The appliance includes the MSS Engine which is responsible for the data monitoring configuration and monitored data. Both the appliance basic configuration and the MSS Engine need to be backed up. The appliance backup contains appliance configurations, such as network settings, but does not contain MSS Engine data. For instructions to back up and restore the appliance firmware, see the Avocent® Universal Management Gateway Appliance Installer/User Guide.

MSS Engine Manual Backup Process

To manually back up the MSS engine:

1. Open an **ssh** connection into the appliance as **admin**.
2. Select option **2** in the login menu to drop to the shell.
3. Enter **sh /mss/engine/version.sh** to identify the MSS Engine version.
4. Enter **cd /mss/engine/bin** to navigate to the /mss/engine/bin directory.
5. Enter **./mss-run BackUp_Restore.sh backup** to perform the backup. The backup time varies depending on the size of the MSS Engine database.
6. After the backup is complete, verify the MSS Engine files have been backed up and enter the following commands:

   For MSS engine versions lower than 3.0:

   cd /var/home

   ll ./db_backup_TODAY/

   For MSS engine version 3.0 and higher:

   cd /mss-db/tmpdir

   ll ./db_backup_TODAY/
7. Verify the directory db_backup_TODAY has been created with all of the files associated with the MSS Engine backup. The directory should look like the following sample:

```
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 conf
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 elementlibrary
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 mssengine
-rw-r--r-- 1 admin admin 1933121 Oct 17 12:24 mssengine_backup.gz
```

8. Enter **tar -zcvf ./db_backup_TODAY.tar.gz ./db_backup_TODAY/** to tar zip the folder.
9. Enter **md5sum ./db_backup_TODAY.tar.gz > ./db_backup_TODAY.tar.gz.md5** to create an md5sum of the tar.gz file and save the output.
10. Enter the following commands to back up the file and the md5 sum file to a backup location:

    scp db_backup_TODAY.tar.gz oracle@<backup_server>:<backup_location><appliance Name>_<Date>

scp db_backup_TODAY.tar.gz.md5 oracle@<backup_server>:<backup_location><appliance Name>_<Date>

MSS Engine Automated Backup Process

A script can be created and copied to the appliance to automatically run a backup. A cronjob runs daily, creates a backup for the MSS Engine and then copies the backup to a backup location. Sample contents of an MSSbackup.sh file:

```
cd /mss/engine/bin
./mss-run BackUp_Restore.sh backup
cd /mss-db/tmpdir
tar -zcvf ./db_backup_TODAY.tar.gz ./db_backup_TODAY/
md5sum ./db_backup_TODAY.tar.gz > ./db_backup_TODAY.tar.gz.md5
/usr/bin/scp -r ./db_backup_TODAY.tar.gz oracle@<backup_server>:<backup_location>/db_
backup_TODAY.` date +%F`.tar.gz
/usr/bin/scp -r ./db_backup_TODAY.tar.gz.md5 oracle@<backup_server>:<backup_
location>/db_backup_TODAY.` date +%F`.tar.gz.md5
```

To set up an automated backup:

1. As **admin**, open an **ssh** connection in to the appliance.
2. Select option **2** in the log in menu to drop to the shell.
3. Enter **ssh-keygen –t rsa** to generate ssh keys for the admin user.
4. Transfer the public key to the backup server location to the backup user.
   a. Enter **scp <backupuser>@<backup_location>:.ssh/authorized_keys ~/.ssh** to copy the original authorized_keys to the appliance.
   b. Enter **cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys** to append the new key to authorized_keys.
   c. Enter **~/.ssh/authorized_keys <backup_user>@<backup_location>:~/.ssh/authorized_keys** to copy the authorized_keys back to the server.
5. As the **root** user, **ssh** to the backup location server and create the backup folder. Enter **backend # mkdir <backup location>**.
6. Change the ownership of the folder to the backup user.
7. Enter **ssh <backup_user>@<backup_location>:~/** to test the automatic log in from the appliance to the backup location.
8. Edit or create the **mssbackup.sh** file and ensure that the last line points to the correct server and appropriate location.
9. As **admin**, use **scp** to copy the file into the **/var/home** folder of the appliance.
10. Navigate to **/var/home** and make the script executable. Enter **chmod +x ./mssbackup.sh**
11. From the ssh console session to the appliance, set up a cronjob using **crontab -e** to copy the backup file to the back machine every X minutes.

    Sample cronjob for 1:05 AM:

```
# Minute Hour Day of Month Month Day of Week Command
# (0-59) (0-23) (1-31) (1-12 or Jan-Dec) (0-6 or Sun-Sat)
5 1 * * * /var/home/mssbackup.sh
```

Appliance and MSS Engine Restore Process

In the case of a disaster, the failed appliance is replaced by a new appliance. The appliance should be restored from a full backup to ensure that the new appliance has the same configurations, firmware and patch level. After the appliance is restored, the MSS engine is restored. Restoring the MSS engine ensures the appliance has the same monitoring configuration and settings as the failed appliance. Any SSL certificates required for communication with the *Trellis*™ platform are also restored.

To restore the appliance:

1. From a laptop or similar system, set up an FTP server and verify the appliance backup image is available.
2. Connect the appliance to the FTP server.
3. Using a keyboard and mouse, open the console to the appliance.
4. Reboot the appliance.
5. On the boot prompt, select **nboot recovery**.
6. Enter the following commands to configure the appliance:

   ifconfig eth0 up

   ifconfig eth0 <Appliance IP> netmask <NETMASK>
7. If required, enter **route add default gateway <GATEWAY IP>** to define the gateway.
8. Enter the following commands to start the netboot process.
   a. If there is no user on the FTP server, enter the **nboot ftp://<FTP IP>/<Location and filename of the img file>** command.
   b. Enter the username and password of the FTP server using the **nboot ftp://<FTPusername>:<FTP Password>@<FTP IP>/<Location and filename of the img file>** command. No special characters are allowed.
9. Press **Enter** and wait approximately 45 minutes. During the process the appliance will download the image from the FTP server, recreates the required partitions and boot menus, then the appliance reboots to complete the process.

MSS Engine Restore

The MSS Engine can only be restored to the same version as the backup. Before the backup can be restored, the file must first be extracted.

To restore the MSS Engine:

1. As **admin**, open an **ssh** connection into the appliance .
2. Select option **2** in the login menu to drop to the shell.
3. Navigate to the directory for the backup file. For MSS engine versions lower than 3.0, enter **cd /var/home**

-or-

For MSS engine versions higher than 3.0, enter **cd /mss-db/tmpdir**.

-or-

Enter **mkdir –p /mss-db/tmpdir** to create the directory if it does not exist.

4. Enter **rm –rf ./db_backup_TODAY/** to remove the folder ./db_backup_TODAY/, if it exists. Be sure you are in the correct folder.
5. Using **scp**, copy the latest mss-engine backup file and md5 sum file into the appliance folder:

   /var/home for MSS engine version lower than 3.0

   /mss-db/tmpdir for MSS engine version 3.0 and higher.
6. Enter **md5sum ./<backup file name>** and **cat ./<backup file name>.md5** to confirm both outputs match.
7. Enter **tar –zxvf ./<backupfile name>** to extract the files. The db_backup_TODAY folder should now exist under the folder /var/home/ for MSS engine version lower than 3.0 and **/mss-db/tmpdir/** for MSS engine version 3.0 and higher.
8. Make sure there are no error messages during the extraction and the folder structure in db_backup_ TODAY looks as follows:

```
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 conf
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 elementlibrary
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 mssengine
-rw-r--r-- 1 admin admin 1933121 Oct 17 12:24 mssengine_backup.gz
```

9. If the folder structure does not contain the same folders and files, navigate to */mss/engine/bin* and enter **./mss-run BackUp_Restore.sh restore** to restore the MSS Engine. The restore time will depend on the size of the MSS Engine database.
10. When the restore is complete, enter **/mss/engine/MSScont.sh status** and verify the Oracle® Complex Event Processing, MSS engine, MSS ELF, MSS Exporter and MSS node processes are running.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), delivers software, hardware and services that maximize availability, capacity and efficiency for data centers, healthcare and industrial facilities. A trusted industry leader in smart infrastructure technologies, Emerson Network Power provides innovative data center infrastructure management solutions that bridge the gap between IT and facility management and deliver efficiency and uncompromised availability regardless of capacity demands. Our solutions are supported globally by local Emerson Network Power service technicians. Learn more about Emerson Network Power products and services at **www.EmersonNetworkPower.com**.