



The TRELLIS™ Real-Time Infrastructure Optimization Platform

Backup and Restore Procedure for Microsoft® Windows®

Technical Bulletin

For Historical Use



For Historical Use

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

This document supports versions up to and including release 4.0.2.

Emerson, Emerson Network Power and the Emerson Network Power logo are trademarks or service marks of Emerson Electric Co. Avocent, the Avocent logo, *Trellis* and the *Trellis* logo are trademarks or service marks of Avocent Corporation. All other marks are the property of their respective owners. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2016 Avocent Corporation. All rights reserved.

TABLE OF CONTENTS

Overview	1
Platform Database Backup and Restore	3
Cold Backup	3
Back machine files and folder	3
Front machine files and folders	6
Cold Restore	7
License Server Reset and Reinstall	8
Reissue a License After the License Server Reset	9
Database Backup and Recovery Tool	11
Incremental Backups	11
Oracle® Database Configuration	11
Host server file backup	12
Tool Configuration	12
Fast Recovery Area Size	12
Fast Recovery Area Location	13
Modify Backup Schedule	13
Reports	14
Restore Database	15
Database Threshold Notification	15
Avocent® Universal Management Gateway Appliance Backup and Restore	17
MSS Engine Manual Backup Process	17
MSS Engine Automated Backup Process	18
Appliance and MSS Engine Restore Process	19
MSS Engine Restore	19

For Historical Use

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 Microsoft® Windows® commands, can perform the back up and restore procedures. If you are restoring to a new system, the operating system (OS) and the *Trellis*™ platform 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.

For Historical Use

For Historical Use

Platform Database Backup and Restore

Cold Backup

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

To create a cold backup:

1. As administrator, on the front and back machines, enter the following at the command prompt to stop the machine:

```
C:\u01\trellis\trellis.bat stop
```

2. On the front machine, enter the following to stop the Node Manager service:

```
sc stop "Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)"
```

3. On the back machine, enter the following to stop the database:

```
sc stop "OracleServiceORCL"
```

4. Enter the following to stop the Emerson-license server on the back machine:

```
sc stop "ServedLicenseInterface"
```

-or-

Run *Services.msc*, navigate to the Served License Interface Service and stop the service.

5. After the backup completes, enter the following to reboot the operating system servers for the back and front machines:

```
sc start "Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)"
```

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

6. On the back machine, enter **C:\u01\trellis\trellis.bat start** to start the platform.
7. On the front machine, enter **C:\u01\trellis\trellis.bat start** to start the platform.

Back machine files and folder

As administrator, back up and restore the following directories and files from the back machine. Because systems may have different configurations, test each instance.

NOTE: The following list is a guideline.

Back Machine Files and Directories

Directories	Files
C:\u01	C:\users\Administrator\TrellisConfiguration.zip
C:\u02	C:\users\Administrator\Trelliscript.zip
C:\u03	N/A

Directories	Files
C:\bea	N/A
C:\users\Administrator\oracle	N/A
C:\Program Files\Oracle	N/A
C:\Program Files\EmersonNetworkPower	N/A

To export registry files:

1. Select *Run* and enter **regedit** to open the Windows registry.
2. Export the following platform-related entries to create a separate .reg file for each export.
 - HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ServedLicenseInterface
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\beasvc
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle.orcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle11
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleDBConsoleorcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\OracleDBConsoleorcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleJobSchedulerORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleMTSRecoveryService
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleOraDb11g_home1TNSListener
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleOraDb11g_home1ClrAgent
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleVssWriterORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_asinst_1
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle Services for MTS
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleServiceORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle.VSSWriter.Oracle
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\beasvc
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleDBConsoleorcl

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle11
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleOraDb11g_home1ClrAgent
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleOraDb11g_home1TNSListener
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleJobSchedulerORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleMTSRecoveryService
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_asinst_1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleServiceORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleVssWriterORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SCM
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle.orcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle Services for MTS
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle.VSSWriter.ORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\beasvc
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_CURRENT_USER\Software\JavaSoft
- HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBCINST.INI\Oracle in OraDb11g_home1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle.orcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle11
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleOraDb11g_home1ClrAgent
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleOraDb11g_home1TNSListener
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleJobSchedulerORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleMTSRecoveryService
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_asinst_1

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle Services for MTS
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleVssWriterORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle.VSSWriter.ORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleServiceORCL

Front machine files and folders

As administrator, back up and restore the following directories and files from the front machine. Because systems may have different configurations, test each instance.

NOTE: The Robocopy or xcopy command line tool can be used when replicating files.

Front Machine Files and Directories

Directories	Files
C:\u01	C:\users\Administrator\TrellisConfiguration.zip
C:\u02	C:\users\Administrator\TrellisScript.zip
C:\u03	N/A
C:\bea	N/A
C:\users\Administrator\oracle	N/A
C:\Program Files\Oracle	N/A

The Administrator role must first be assigned ownership of the password in order to copy the command to a remote backup destination.

To set the Administrator as the owner of the jmxremote.password file:

1. As administrator, navigate to `C:\u02\domains\<Trellis domain>\config` and execute the following command:
takeown /f C:\u02\domains\<Trellis domain>\config\jmxremote.password
2. Wait for the response SUCCESS: The file (or folder): "C:\u02\domains\<Trellis domain>\config\jmxremote.password" now owned by user "HSV-STR-20207\Administrator."
3. After `C:\u02\domains\<Trellis domain>\config`, execute the following command to grant the administrator access to the jmxremote.password file:
icacls C:\u02\domains\<Trellis domain>\config\jmxremote.password /grant administrator:F
4. Wait for one of the following responses:
 - Processed file: C:\u02\domains\<Trellis domain>\config\jmxremote.password
 - Successfully processed 1 files; Failed processing 0 files
5. Copy the C:\U02 directory to the remote backup location.

To export the registry files:

6. Select *Run* and enter **regedit** to open the Windows registry.
7. Export the following platform-related entries to create a separate .reg file for each export.

- HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\beasvc
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle WebLogic NodeManager
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_osbproxy01
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_ui01
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_osbproxy01
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_ui01
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_osbproxy01
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_ui01

NOTE: If you get a permission error when copying the c:\u02\domains\\config\jmxremote.password file, make sure the file has administration privileges and re-copy the file. After copying the file remove all the privileges.

Cold Restore

The new instance configuration is a replica of the original failed instance. Changing the IP addresses, hosts names or other configurations is 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 administrator, provision the front and back machines using the appropriate Windows® OS version with all pre-requisites.
2. Configure the front and back machines with pre-installation steps as a replica of the original systems.
3. On the back machine, restore all the files and folders mentioned in [Cold Backup](#) on page 3.
4. On the front machine, restore all the files and folders mentioned in [Cold Backup](#) on page 3.
 - a. As administrator, execute the following command to set the SYSTEM as the owner of the jmxremote.password file:


```
icacls "C:\u02\domains\\config\jmxremote.password" /setowner "SYSTEM" /T /C
```
 - b. Wait for one of the following responses:
 - Processed file: jmxremote.password

- Successfully processed 1 files; Failed processing 0 files
- c. Execute the following command to revoke the administrator access to the jmxremote.password file:
C:\u02\domains
- 5. For restoring/importing the registry entries, double-click each exported registry and click Yes for the corresponding information on the front and back machines.
- 6. Reset the license server. See [License Server Reset and Reinstall](#) on page 8.
- 7. As an administrator user on the back machine, enter the following to start the database:
c:\u01\trellis>sqlplus / as sysdba
SQL> startup
- 8. As administrator on the back machine, enter **\u01\trellis\trellis start** to start the platform.
- 9. As **oracle** on the front machine, enter **\u01\trellis\trellis** to start the platform.
- 10. If the front machine fails when starting, proceed as follows:
 - a. Remove all users and permissions from the **c:\u02\domains\ file.**
 - b. On a Windows machine, create the **ora_dba** group and assign administrator user to the group to start the oracleORCL service.
 - c. Enter **C:\u01\trellis>trellis start** to start the back machine.

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 administrator, log in to the back machine.
3. In Windows®, go to services and verify the license services are running.
4. If the services are not running, run **tsreset_svr.exe** to start the *Served License Interface* service.
5. From the command prompt, reset the license server in the **C:\Program Files\EmersonNetworkPower\ServedLicenseInterface** folder.
6. If the license server reset fails, follow the steps to reinstall the license server.

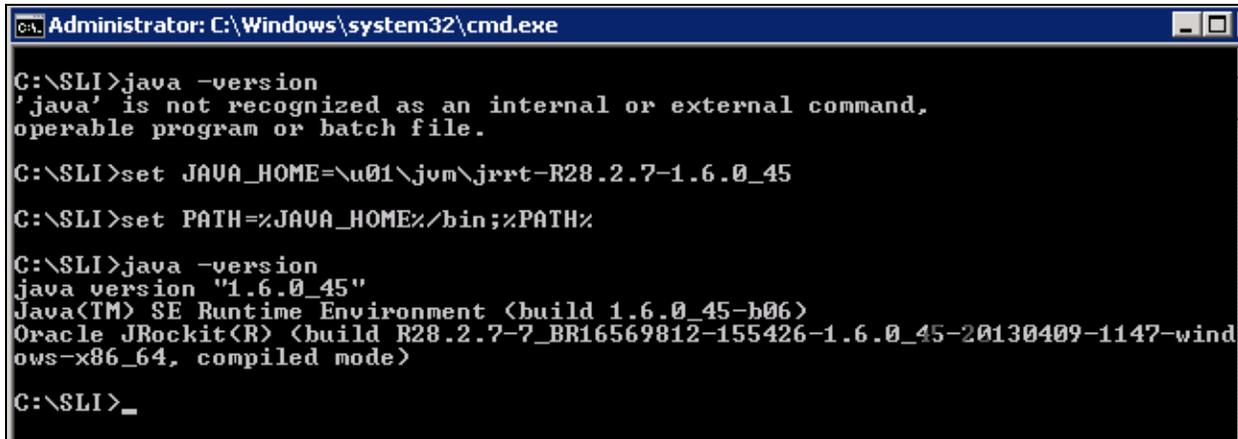
NOTE: If the license server reset is unsuccessful you must reinstall the license server.

To reinstall the license server:

1. As administrator, go to the services and stop the Served License Interface service.
2. Create a directory on your C drive called **C:\SLI** and copy the license server **sli_windows_install64-1_0_1_50.exe** installer file to the back machine.
3. At a DOS prompt, go to the SLI directory and enter the following to set the correct Java version:

- a. **set JAVA_HOME=\u01\jvm\jdk1.7.0_85**
 - b. **set PATH=%JAVA_HOME%/bin;%PATH%**
4. Enter **java -version** to verify the Java version. See the following screen.

Java Version Screen



```

Administrator: C:\Windows\system32\cmd.exe
C:\SLI>java -version
'java' is not recognized as an internal or external command,
operable program or batch file.
C:\SLI>set JAVA_HOME=\u01\jvm\jrrt-R28.2.7-1.6.0_45
C:\SLI>set PATH=%JAVA_HOME%/bin;%PATH%
C:\SLI>java -version
java version "1.6.0_45"
Java(TM) SE Runtime Environment (build 1.6.0_45-b06)
Oracle JRockit(R) (build R28.2.7-7_BR16569812-155426-1.6.0_45-20130409-1147-wind
ows-x86_64, compiled mode)
C:\SLI>_

```

5. From the DOS command prompt, in the SLI directory, run **slf_windows_install64-1_0_1_50.exe**.
-or-
Double-click the *SLI.exe* file to install the license server.
6. From the Windows services, verify the Served License Interface service is running.
-or-
If the service is not running, start it.

Reissue a License 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 administrator, generate the Request XML file from the following directory and save it to the request directory on the C drive. The following is an example of the command:
Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface):
Serveractivationui -activate a1a7-94e9-22a5-4867-8204 -quantity 10 -gen c:\requests\reqActivate_052302.xml
2. After the request.xml file is generated for all the files, send it to Technical Support. After you receive the Response XML files, save them to the response directory on C Drive.
3. Process the response files. For example,
Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface)
Serveractivationui -process c:\responses\response.xml
4. After the command is complete, the following message is displayed:

File activate_response.xml successfully processed

Refresh license client cache

Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface

lmutil lmreread

5. After the command is complete, the following message is displayed:

lmutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved.

lmreread successful

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 **serveractivationui.exe -showlocal** from C:\Program Files\EmersonNetworkPower\ServedLicenseInterface directory to verify the license is available through the license server.

For Historical Use

Database Backup and Recovery Tool

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

- 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 that are used in the 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, the database backup and recovery tool 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	This database mode enables archiving of the online redo log.
Online redo log	This log includes two or more online redo log files that record all changes made to the 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 `c:\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 the Windows administrator user that installed *Trellis*™ platform, log in to the database host server.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.
4. Enter option **1** RMAN Configuration, then option **1** Enable RMAN and press **Enter** to enable the RMAN tool.
5. Accept the default FRA location and press *Enter* or enter a new location.
6. 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, the control file, archived redo log files and 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 the 23355M by three. In this example, your FRA size is 70065M (x 3).

To change the FRA size:

1. As the Windows administrator user that installed the *Trellis*™ platform, log in to the database host server.

2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.
4. Enter option **1** RMAN Configuration, then option **2** Modify FRA Settings in the Configuration Menu and press **Enter**.
5. Enter the FRA 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 the Windows administrator user that installed the *Trellis™* platform, log in to the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.
4. Enter option **1** RMAN Configuration, then option **2** Modify FRA Settings and press **Enter**.
5. 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:

```
Trellis RMAN Backup Schedule
=====
Started backups on: 29-10-2014 00:00:00 America/New_York
Back up intervals (in hours): 24
Next 5 backup starts are:
29-10-2014 00:00:00 America/New_York
30-10-2014 00:00:00 America/New_York
31-10-2014 00:00:00 America/New_York
01-11-2014 00:00:00 America/New_York
02-11-2014 00:00:00 America/New_York
Modifying the backup interval may require re-evaluating the FRA size
=====
New Interval (hours, default: 24): █
```

1. As the Windows administrator user that installed the *Trellis*™ platform, log in to the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.
4. Enter option **1** RMAN Configuration, then option **3** Modify Backup Schedule and press **Enter**.
5. Enter the new interval in hours.

```
New Interval (hours, default: 24): 20
dd-MM-yyyy HH:mm:ss z
default: 29-10-2014 00:00:00 America/New_York):
█
```

6. Enter the starting date and time in the format **DD-MM-YYYY HH:MM:SS**.

```
New Interval (hours, default: 24): 20
dd-MM-yyyy HH:mm:ss z
default: 29-10-2014 00:00:00 America/New_York):
29-10-2014 14:14:00
New Scheduled Start date is: 2014-10-29T14:14-04:00[America/New_York]
New Interval (hours) is: 20
Next five run date are:
2014-10-29T14:14-04:00[America/New_York]
2014-10-30T10:14-04:00[America/New_York]
2014-10-31T06:14-04:00[America/New_York]
2014-11-01T02:14-04:00[America/New_York]
2014-11-01T22:14-04:00[America/New_York]
Is this correct (Type : YES to accept, NO to abort): █
```

7. 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 the Windows administrator user that installed the *Trellis*™ platform, log in to the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.

4. Enter option **1** RMAN Configuration, then option **4** Reports and press **Enter**.
5. Enter option **1** Data files status to view a report about the health of the database files.
6. Press any key to return to the Reports Menu.
7. Enter option **2** Backup History.
8. 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 the Windows administrator user that installed the *Trellis*[™] platform, log in to the database host server.
5. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
6. At the prompt, enter **c:\u01\trellis\configure**.
7. Enter option **1** RMAN Configuration, then option **5** Restore Database.
8. 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 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 **rmnotificationX**, where X is a number between 0 and 9.

NOTE: You must add each user in sequential order starting with rnotification0. For example, rnotification0 must be added before rnotification1, rnotification1 must be added before rnotification2 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.

For Historical Use

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. As **admin**, open an **ssh** connection into the appliance.
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 into the appliance.
2. Select option **2** in the login 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. To test the automatic login from appliance to backup location, enter **ssh <backup_user>@<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 make sure 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 in to the appliance.
2. Select option **2** in the log in 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 in to the appliance folder:
`/var/home` for MSS engines lower than version 3.0
`/mss-db/tmpdir` for MSS engines 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 `/var/home/` folder for the MSS engine version 3.0 or lower and `/mss-db/tmpdir/` for MSS engine version 3.0 and higher.
8. Make sure there are no error messages during the extraction. The folder structure in `db_backup_TODAY` appears 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.

For Historical Use

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. For additional assistance, visit www.avocent.com/support.

Avocent Community Support Site

To search product knowledge content, visit community.emerson.com/networkpower/support/avocent.

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.

For Historical Use