Dell OpenManage Network Manager Version 6.2
Service Pack 2

Installation Guide

Notes and Cautions

A NOTE indicates important information that helps you make better use of your computer.

A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

2016-9

Rev. A01

Contents

1

Sizing Overview

System requirements vary depending on how you use Dell OpenManage Network Manager.

System Basics

Optimally, base the minimum configuration of your system on expected peak load. Typically a configuration running all elements of a system on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your real system needs may be higher.

CAUTION:
Hostnames can be any length, but the initial eight characters in the names of all hosts used as servers with this application must be unique in the network.

See Best Practices: Single Server Hardware on page 14, and Suggested Hardware for High Availability Installations on page 20 for more specifics about hardware.

Best practice, and advice about how to prevent problems, is in the “Pre-flight Checklist” in the *User Guide*.

Supported Operating System Versions

Disable firewall products during initial installation and testing. If you are upgrading, take a look at Compatible Operating Systems / Databases / Browsers on page 105. The following are recommended operating system versions:

Microsoft Windows—This application supports most Windows operating systems from Windows XP forward, with their latest service packs, with the exception of Windows 2003. The supported operating systems are: Windows XP (Pro) SP3 or later, Windows Vista (Business or Ultimate), Windows Server 2008, Enterprise Edition, 64-bit, Windows 7 (Business or better), and Windows 2012. To install on Windows 2012, right-click the win_install.exe file (not the shortcut, but the file in `Disk1\instdata` directory), and select the Compatibility tab.

Check *Run this program in compatibility mode for ...* then select either Windows 7 or Vista. Do likewise if you must uninstall (find the uninstall program and run it in compatibility mode). Command line installations are supported without any compatibility issues.

NOTE:

Windows Terminal Server is not supported. The installer becomes non-responsive with Data Execution Prevention enabled. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server.

Also: You must disable User Access Control (UAC) if you are installing on Vista or Windows Server 2008. Right click the user icon when you open the start menu to do this.

Also: Installer may halt when pre-existing bash sessions or cmd sessions left are open. Close all such sessions.

Finally: In Vista, you must either to disable User Account Control or run application server as service. Another option is to run as administrator on startappserver. In Vista, right click the startappserver icon and select run as administrator.

CAUTION:

To manage Windows systems—in single server deployments, you must install this application on a Windows host. In distributed deployments, a mediation server installed on Windows must communicate to managed Windows systems.

Linux—This application supports 64-bit Red Hat (Enterprise versions 6.2 and 6.4) Linux. Also supported: 64-bit CentOS 6.2 and 6.4. See the 32-bit Linux Libraries section below for some additional requirements. See the *User Guide* for Linux installation best practices.

VMware—Dell OpenManage Network Manager supports the above operating systems on VMware virtual machines. We test Dell OpenManage Network Manager primarily on Windows 2008R2 and Redhat/CentOS on virtual machines. The hardware and software requirements for virtual machines are the same as discussed in Best Practices: Single Server Hardware on page 14 and Suggested Hardware for High Availability Installations on page 20 with the caveat that hardware with a virtual machine must have enough capacity for its own requirements in addition to the virtual machine itself.

CAUTION:

The Dell OpenManage Network Manager installer does not validate operating systems, so it allows installation on unsupported operating systems.

Troubleshooting:

Upon Login, if you see the message "Credentials are needed to access this application," add `oware.appserver.ip=[application server IP address]` to `/oware/synergy/tomcat-XXX/webapps/ROOT/WEB-INF/class/portal-ext.properties`.

32-bit Linux Libraries

For Linux installations, you must identify the appropriate package containing 32-bit `libtcl8.4.so` (for the example below: `tcl-8.4.13-3.fc6.i386.rpm` for Red Hat).

NOTE:

Do not use any x86_x64 rpms; these would not install the 32-bit libraries.

Any 32-bit tcl rpm that is of version 8.4 and provides `libtcl8.4.so` works. You can download them from Sourceforge: http://sourceforge.net.

Download these, then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect
/opt/dorado/oware3rd/expect/linux/bin/expect
[someone@RHEL5-64bit ~]$ ldd /opt/dorado/oware3rd/expect/linux/bin/expect
        linux-gate.so.1 =>  (0xffffe000)
        libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/
  libexpect5.38.so (0xf7fd2000)
        libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000)
        libdl.so.2 => /lib/libdl.so.2 (0x0033e000)
        libm.so.6 => /lib/libm.so.6 (0x00315000)
        libutil.so.1 => /lib/libutil.so.1 (0x00b8d000)
        libc.so.6 => /lib/libc.so.6 (0x001ba000)
        /lib/ld-linux.so.2 (0x0019d000)
```

Make sure that `libtcl8.4.so` maps to `/lib/libtcl8.4.so`

An Alternative for Red Hat Linux

1. Copy /usr/lib/libtcl8.4.so from a 32-bit RH system to /usr/local/lib/32bit on your 64-bit RedHat system
2. As root, execute: ln –s /usr/local/lib/32bit/libtcl8.4.so /usr/lib/libtcl8.4.so

Supported Protocols

The following are supported protocols:

- TCP/IP
- SNMP
- HTTP
- UDP Multicast

- CIDR

Installing Perl

If you install Perl to take advantage of this application's use of Perl Scripting capabilities, you must install it on the path on the application server and mediation server host. Note that in versions 6.1 and later Perl comes installed (with Cygwin). See Upgrading Perl in Dell OpenManage Network Manager 6.1 on page 14 for one caveat.

Make sure your system has Perl installed on both the application and mediation server hosts. You must verify the executable is on the system path. If you install it after you install Dell OpenManage Network Manager, best practice is to reboot that host to ensure the path recognition.

NOTE:

We recommend Perl version 5.10 or later (however not 5.16). You must the Perl module Net::Telnet. Running `perldoc [package name]` (for example `perldoc Net::Telnet`) lets you know whether your system has the relevant package.

This application does not package Perl. If you want to use the Perl scripting features, you must make sure your system has Perl installed. You can find information about Perl at www.perl.com. Follow the downloads link to find the recommended distribution for your specific platform.

One of the recommended Perl packages is from ActiveState which can be found at: www.activestate.com/activeperl/

Upgrading Perl in Dell OpenManage Network Manager 6.1

Perl v. 5.14 deprecates the `switch` module. This version is installed with the Cygwin update for Windows in Dell OpenManage Network Manager 6.1 and later. After this update if you still have `switch` cases/ scripts using `switch` statements, then you must install `switch.pm` manually.

To install `switch.pm`, copy that file into the following directories under Cygwin:

```
[installation root]\oware3rd\cygwin\lib\perl5\vendor_perl\5.14
[installation root]\oware3rd\cygwin\lib\perl5\5.14
```

You can use the `switch.pm` file from an older Perl installation or look online for it.

Best Practices: Single Server Hardware

The following describes hardware and sizing configuration for common Dell OpenManage Network Manager deployments in both real and virtual machines. Before any deployment, best practice is to review and understand the different deployment options and requirements. Consider future growth of the network when estimating hardware sizes. You can often expand modern systems running Dell OpenManage Network Manager by adding more RAM to the host server(s). Selecting expandable hardware may also be critical to future growth. For ease of management, deployments

selection best practice is to use the fewest possible servers. Standalone (single server) deployments offer the simplest and easiest management solution. When you require high availability (HA), you can configure a deployment with as few as two servers.

Minimum Hardware

The minimum hardware specification describes the least of what Dell OpenManage Network Manager needs. In such minimum installations, traffic flowing from the network to Dell OpenManage Network Manager may exceed the capacity of the hardware. When estimating the size of a deployment, it is important to understand the applications configurations in the target environment. For example, the most resource-intensive, demanding applications are typically Traffic Flow Analyzer (TFA), Event Management and Performance Monitoring.

REQUIRED Minimum hardware—8GB RAM[5], dual core CPU, 2.8GHz or better, 200 GB 7200 RPM Disk.

Supports:

- Standalone installations (Single Server) are supported when you use high-resource demand applications minimally.
- Distributed installation of a single component server like application server only, Mediation server only, database server only or web server only.

RECOMMENDED Minimum hardware: 10GB RAM, four-core (or more) CPU (2.8GHz or better), 400 GB 10,000 RPM Disk

Supports:

- Standalone installations

CAUTION:

The above assumes you have dedicated a host to Dell OpenManage Network Manager alone. Other applications may compete for ports or other resources and can impair the system's performance.

Sizing for Standalone Installations

The following are suggested sizing guidelines for your Dell OpenManage Network Manager system.[1]

Max. Managed Devices[2]	64-bit Operating System: Disks / RAM / Hardware	Max. Concurrent Users	Performance Monitor Max. Targets[3]	Max. Traffic Flow Exporters[3]	Installation Changes to Heap Memory Settings
25	8GB[5] RAM, single disk, consumer level PC	5	2500	5	Use defaults: (3GB application server heap, 512M database, 2G Synergy Web Server[4])
50	10 GB RAM, single disk, consumer level PC	8	5000	5	3-6 GB application server heap, 512M database buffer, 2G Synergy Web Server
100	12 GB RAM, single disk, consumer level PC	10	10000	10	4-7GB application server heap, 1GB database buffer, 3GB Synergy Web Server
175 - 250	14GB RAM, single disk, business level PC	15	25000	25	4-9 GB application server heap, 1GB database buffer, 3GB Synergy Web Server
300 - 500	16GB RAM, single disk, business level PC	25	50000	50	5-10GB application server heap, 2GB database buffer, 3GB Synergy Web Server
1000	18 GB RAM, multi-disk, server level PC	50	100000	100	8-12GB application server heap, 3GB database buffer, 5GB Synergy Web Server
2000	32GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	100	200000	100	10-14GB application server heap, 8GB database buffer, 8GB Synergy Web Server

Max. Managed Devices[2]	64-bit Operating System: Disks / RAM / Hardware	Max. Concurrent Users	Performance Monitor Max. Targets[3]	Max. Traffic Flow Exporters[3]	Installation Changes to Heap Memory Settings
2500	40GB RAM, multidisk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	125	250000	125	12-16GB application server heap, 10GB database buffer, 12GB Synergy Web Server
3000	48GB RAM, multidisk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	150	400000	150	14-16GB application server heap, 12GB database buffer, 12GB Synergy Web Server
5000	64 GB RAM, multidisk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	175	600000	200	20-24GB application server heap, 16GB database buffer, 16GB Synergy Web Server
7500	80 GB RAM, multidisk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	200	850000	250	28-32GB application server heap, 20GB database buffer, 20GB Synergy Web Server

Max. Managed Devices[2]	64-bit Operating System: Disks / RAM / Hardware	Max. Concurrent Users	Performance Monitor Max. Targets[3]	Max. Traffic Flow Exporters[3]	Installation Changes to Heap Memory Settings
10000	128GB RAM, multidisk, server level PC. Recommend fast disk	225	1000000	300	38-44GB application server heap, 24GB database buffer, 24GB Synergy Web Server

[1] Servers are assumed to have at least four cores (2.8GHz or better) and are no more than four years old. As memory and usage increases, the number of CPU cores needs to increase. Dual core CPUs can work for the most basic installations, but such configurations are not recommended.

[2] Each device mentioned here is equivalent to a L2 or L3 switch with a total of 48 interfaces per device being monitored. For each device not being monitored for 48 interfaces, you can add another 50 devices to the overall inventory for ICMP-only monitoring. Maximum monitor targets assumes a 5 minute or longer polling interval. It assumes each monitor is polling the default number of attributes or less.

[3] Application Constraints are most relevant to Traffic Flow Analysis, Performance Management, and Event Management. Refer to the performance monitor Section of the user guide to best practices. In general, no single monitor should exceed 10000 targets. This is primarily for performance reasons. Actual physical hardware and monitor configuration will determine your system capacity for targets and overall system performance.

The Maximum Exporters assumes your Traffic Flow configuration does not exceed the capacity of the physical hard drive(s). refer to the Performance section of the Traffic Flow chapter.

Traffic Flow Analysis ratings map to constant throughput divided by sample rate, as in bandwidth / sample rate. 20G / 2000 is easier to manage than 20G / 1000. 20G / 1 is a thousand times more demanding than 20G / 1000. Best practice is to avoid such high sample rates. The bandwidth the hardware your Dell OpenManage Network Manager installation can support is dramatically lower in such cases. Best

practice is to sample a maximum of one traffic flow for every 1000 (1:1000). Higher sampling rates degrade database performance and increase network traffic without adding any significant statistical information.

Performance Management can support 600 inserts per second using a single disk (SSD) Drive. 1 insert = 1 monitored attribute. Expect better performance as you add more drives (and worse performance with slower drives).

Event Management can support a sustained 1200 traps /sec using a single (SSD) drive. Expect better performance as you add more drives (and worse performance with slower drives).

CAUTION:

Java JVM problems can generate over 10GB of thread dump in case of a memory error. To solve the problem of such files filling up your hard drive, delete the `*.hprof` files in the `/oware/jboss-5.1/bin` directory to free up the disk space. You can also clean out `temp` directories. Finally, ensure your hardware has enough RAM for the tasks it has been assigned. The Server Statistics portlet displays performance information.

[4] Concurrent users determine the amount of RAM required for the web server. You can reduce the web server heap setting can if your system has fewer concurrent users.

[5] Although not recommended, 6 GB of RAM may be enough for systems with up to two users that are not using Traffic Flow Analysis or Performance Monitoring. In such cases, adjust installation/settings to 1 GB Synergy web server rather than the 2 GB default.

If the network you manage exceeds the parameters outlined above, or your system is balky and unresponsive because, for one example, it monitors more devices than your hardware can handle, consult your sales representative about upgrading to a more robust or multi-server version of Dell OpenManage Network Manager. Also, see the *User Guide* for more about tuning monitor performance. You can also monitor the application server itself. See the *User Guide* for specifics.

Suggested Hardware for High Availability Installations

The following describes hardware examples for High Availability installations. We base these suggestions on average Dell OpenManage Network Manager use on your managed network. These suggestions include an indication for, Number of Users, Number of devices managed, Traffic Flow Analysis (TFA), Performance Management (PM) and Event Management (EM) as the most demanding elements

High Availability installations consist of separate servers for separate functions within Dell OpenManage Network Manager. Web Server (WS) + Application Server (AS), Mediation Server (MS) and Database server (DB) are on separate hosts. The RAM, CPU and hard drive (HD) sizes for these are indicated below. All CPUs and/or cores should be 2.8GHz or faster.

Dell OpenManage Network Manager Use	**Application Server (AS) + Web Server (WS)**			**Mediation Server (MS)**			**Database Server (DB)**			**Memory Allocation (Changes to default heap settings)**			
	RAM (GB)	CPU	HD (GB)	RAM (GB)	CPU	HD (GB)	RAM (GB)	CPU	HD	WS (GB)	AS (GB)	MS (GB)	DB (GB)
10 users 500 devices TFA [1] PM[4] EM[5]	8	Dual Core	100	4	Dual Core	40	4	Dual Core	1x 100 GB 7200RPM	2	3	3	3
50 users 1000 Devices TFA [2] PM[4] EM[5]	16	Quad Core	100	6	Dual Core	60	8	Quad Core	2x100GB 10K RPM RAID 0 or better striping or SSD	6	6	4	6
150 users 5000 Devices TFA[3] PM[4] EM[5]	32 +	8 core	100	6	5 x Dual Core [6]	100	16 +	8 core	High Perf Disk Array 4 x 100GB 10K RPM or better. RAID 0 or better or SSD	14	14	4	14

Dell OpenManage Network Manager Use	Application Server (AS) + Web Server (WS)			Mediation Server (MS)			Database Server (DB)			MemoryAllocation (Changes to default heap settings)			
150 users 10000 Devices TFA[3] PM[4] EM[5]	64+	8 Core	200	32	4 Core	200	32	8 Core	High Perf Disk Array8x100GB 10K RPM or better. RAID 0 or better or SSD	20	20	6	20

[1] <2Mbs Internet egress and a 1:1000 sample rate.

[2] <10Gbs Internet egress and a 1:1000 sample rate

[3] <200 Gbs Internet egress and a 1:1000 sample rate.

[4] PM can support 600 inserts per second using a single disk (SSD) Drive. 1 insert = 1 monitored attribute. Expect better performance as you add more drives (and worse performance with slower drives).

[5] EM can support a sustained 1200 traps /sec using a single (SSD) drive. Expect better performance as you add more drives (and worse performance with slower drives).

[6] Mediation recommendations assume managing <1000 devices per host.

For sizing recommendations about larger installations than this chart covers, contact your sales representative.

Calculating Memory Requirements

One way to calculate Dell OpenManage Network Manager memory requirements is the following formula:

500M + active users * 80M = RAM needed.

Please remember that the concurrent users value is typically far less than the number of total users. Most users do not use active web server operations constantly. Most will not even be logged in.

MySQL Server Configuration File Examples

The `my.cnf` files optimize MySQL installations for the database size you configure at installation time. Refer to the *User Guide* for more suggestions about re/sizing your MySQL database, as well as starting, stopping and performance tuning it.

Several my.cnf files and example `*.ini` files (`my-small.ini`, `my-large.ini`, and so on) accompany standard installations, but the origin of the configuration on Linux is `/opt/dorado/oware3rd/mysql/[version number]/my.cnf`, and on Windows is `\oware3rd\mysql\[version number]\my.cnf` so be sure to alter that file if you are optimizing MySql. The following are examples of `my.cnf` files for the configurations described above:

- 6GB example (default):
- 8GB example:
- 12GB example:
- 16GB example:
- 32GB example:

CAUTION:
Some Linux distributions have MySQLinstalled by default. Remove any previous MySQL installation, and make sure to remove or rename the `my.cnf` file for that previous installation. If it is on the path, it can interfere with the correct operation of Dell OpenManage Network Manager.

See the *User Guide* for additional advice about `my.cnf` configuration.

6GB example (default):

```
# The MySQL server
[mysqld]
port=3306
#socket=MySQL
skip-locking
set-variable    = connect_timeout=10
set-variable    = key_buffer=384M
set-variable    = max_allowed_packet=32M
set-variable    = table_cache=1024
set-variable    = sort_buffer=2M
set-variable    = record_buffer=2M
set-variable    = thread_cache=8
# Try number of CPU's*2 for thread_concurrency
set-variable    = thread_concurrency=8
set-variable    = myisam_sort_buffer_size=64M
server-id       = 1
transaction-isolation = READ-COMMITTED

# Uncomment the following if you want to log updates
#log-bin
innodb_locks_unsafe_for_binlog=1

set-variable = innodb_mirrored_log_groups=1
set-variable = innodb_log_files_in_group=3
```

```
set-variable = innodb_log_file_size=256M
set-variable = innodb_log_buffer_size=8M
innodb_flush_log_at_trx_commit=1
innodb_log_archive=0
set-variable = innodb_buffer_pool_size=512M
set-variable = innodb_additional_mem_pool_size=20M
set-variable = innodb_file_io_threads=4
set-variable = innodb_lock_wait_timeout=30
```

8GB example:

```
# The MySQL server
[mysqld]
port=3306
#socket=MySQL
skip-locking
query_cache_type=1
#caches often used queries.  32-512M, depending on how big the commonly
   cached queries need to be, limit per and overall size
query_cache_limit=12M
query_cache_size=128M
set-variable    = connect_timeout=10
#This is for myISAM tables, not needed for appserver
set-variable    = key_buffer=384M
set-variable    = max_allowed_packet=32M
set-variable    = table_cache=1024
set-variable    = sort_buffer=2M
set-variable    = record_buffer=2M
set-variable    = thread_cache=8
# Try number of CPU's*2 for thread_concurrency
set-variable    = thread_concurrency=8
set-variable    = myisam_sort_buffer_size=64M
server-id       = 1
transaction-isolation = READ-COMMITTED

# Uncomment the following if you want to log updates
#log-bin
```

```
innodb_locks_unsafe_for_binlog=1


set-variable = innodb_buffer_pool_size=1024M
#larger sizes help with write intensive workloads and large data sets, but
   usually not needed above 512M
set-variable = innodb_log_file_size=256M
#set high enough for 1 second worth of operations; maybe 1% of total (8M
   for 8G, 16 for 16, etc)
set-variable = innodb_log_buffer_size=8M
#default of 1 is slow.  2 uses the OS cache so only lose data on OS crash
   (power outage, etc).  MUCH FASTER.
innodb_flush_log_at_trx_commit=2
innodb_thread_concurrency=8
#Increase based on number of concurrent users; assume each user hits about
   100 tables and uses 1 thread (plus app overhead; 6 for overhead plus 1
   per user)
table_cache=1024
thread_cache=16


set-variable = innodb_mirrored_log_groups=1
set-variable = innodb_log_files_in_group=3
innodb_log_archive=0
# set a smidge high each step; doesn't make a huge difference
set-variable = innodb_additional_mem_pool_size=20M
set-variable = innodb_file_io_threads=4
set-variable = innodb_lock_wait_timeout=30
```

12GB example:

```
# The MySQL server
[mysqld]
port=3306
#socket=MySQL
skip-locking
query_cache_type=1
#caches often used queries.  32-512M, depending on how big the commonly
   cached queries need to be, limit per and overall size
query_cache_limit=12M
query_cache_size=256M
```

```
set-variable    = connect_timeout=10
#This is for myISAM tables, not needed for appserver
set-variable    = key_buffer=384M
set-variable    = max_allowed_packet=32M
set-variable    = table_cache=1024
set-variable    = sort_buffer=2M
set-variable    = record_buffer=2M
set-variable    = thread_cache=8
# Try number of CPU's*2 for thread_concurrency
set-variable    = thread_concurrency=8
set-variable    = myisam_sort_buffer_size=64M
server-id       = 1
transaction-isolation = READ-COMMITTED


# Uncomment the following if you want to log updates
#log-bin
innodb_locks_unsafe_for_binlog=1


set-variable = innodb_buffer_pool_size=2048M
#larger sizes help with write intensive workloads and large data sets, but
   usually not needed above 512M
set-variable = innodb_log_file_size=256M
#set high enough for 1 second worth of operations; maybe 1% of total (8M
   for 8G, 16 for 16, etc)
set-variable = innodb_log_buffer_size=12M
#default of 1 is slow.  2 uses the OS cache so only lose data on OS crash
   (power outage, etc).  MUCH FASTER.
innodb_flush_log_at_trx_commit=2
innodb_thread_concurrency=8
#Increase based on number of concurrent users; assume each user hits about
   100 tables and uses 1 thread (plus app overhead; 6 for overhead plus 1
   per user)
table_cache=1536
thread_cache=24


set-variable = innodb_mirrored_log_groups=1
set-variable = innodb_log_files_in_group=3
```

```
innodb_log_archive=0
# set a smidge high each step; doesn't make a huge difference
set-variable = innodb_additional_mem_pool_size=20M
set-variable = innodb_file_io_threads=4
set-variable = innodb_lock_wait_timeout=30
```

16GB example:

```
# The MySQL server
[mysqld]
port=3306
#socket=MySQL
skip-locking
query_cache_type=1
#caches often used queries.  32-512M, depending on how big the commonly
   cached queries need to be, limit per and overall size
query_cache_limit=12M
query_cache_size=256M
set-variable    = connect_timeout=10
#This is for myISAM tables, not needed for appserver
set-variable    = key_buffer=384M
set-variable    = max_allowed_packet=32M
set-variable    = table_cache=1024
set-variable    = sort_buffer=2M
set-variable    = record_buffer=2M
set-variable    = thread_cache=8
# Try number of CPU's*2 for thread_concurrency
set-variable    = thread_concurrency=8
set-variable    = myisam_sort_buffer_size=64M
server-id       = 1
transaction-isolation = READ-COMMITTED

# Uncomment the following if you want to log updates
#log-bin
innodb_locks_unsafe_for_binlog=1

set-variable = innodb_buffer_pool_size=3072M
```

```
#larger sizes help with write intensive workloads and large data sets, but
   usually not needed above 512M

set-variable = innodb_log_file_size=256M

#set high enough for 1 second worth of operations; maybe 1% of total (8M
   for 8G, 16 for 16, etc)

set-variable = innodb_log_buffer_size=16M

#default of 1 is slow.  2 uses the OS cache so only lose data on OS crash
   (power outage, etc).  MUCH FASTER.

innodb_flush_log_at_trx_commit=2

innodb_thread_concurrency=8

#Increase based on number of concurrent users; assume each user hits about
   100 tables and uses 1 thread (plus app overhead; 6 for overhead plus 1
   per user)

table_cache=2048

thread_cache=64


set-variable = innodb_mirrored_log_groups=1

set-variable = innodb_log_files_in_group=3

innodb_log_archive=0

# set a smidge high each step; doesn't make a huge difference

set-variable = innodb_additional_mem_pool_size=20M

set-variable = innodb_file_io_threads=4

set-variable = innodb_lock_wait_timeout=30
```

32GB example:

```
# The MySQL server

[mysqld]

port=3306

#socket=MySQL

skip-locking

query_cache_type=1

#caches often used queries.  32-512M, depending on how big the commonly
   cached queries need to be, limit per and overall size

query_cache_limit=12M

query_cache_size=512M

set-variable    = connect_timeout=10

#This is for myISAM tables, not needed for appserver

set-variable    = key_buffer=384M
```

```
set-variable    = max_allowed_packet=32M
set-variable    = table_cache=1024
set-variable    = sort_buffer=2M
set-variable    = record_buffer=2M
set-variable    = thread_cache=8
# Try number of CPU's*2 for thread_concurrency
set-variable    = thread_concurrency=8
set-variable    = myisam_sort_buffer_size=64M
server-id       = 1
transaction-isolation = READ-COMMITTED


# Uncomment the following if you want to log updates
#log-bin
innodb_locks_unsafe_for_binlog=1


set-variable = innodb_buffer_pool_size=6144M
#larger sizes help with write intensive workloads and large data sets, but
   usually not needed above 512M
set-variable = innodb_log_file_size=372M
#set high enough for 1 second worth of operations; maybe 1% of total (8M
   for 8G, 16 for 16, etc)
set-variable = innodb_log_buffer_size=32M
#default of 1 is slow.  2 uses the OS cache so only lose data on OS crash
   (power outage, etc).  MUCH FASTER.
innodb_flush_log_at_trx_commit=2
innodb_thread_concurrency=16
#Increase based on number of concurrent users; assume each user hits about
   100 tables and uses 1 thread (plus app overhead; 6 for overhead plus 1
   per user)
table_cache=10240
thread_cache=128


set-variable = innodb_mirrored_log_groups=1
set-variable = innodb_log_files_in_group=3
innodb_log_archive=0
# set a smidge high each step; doesn't make a huge difference
set-variable = innodb_additional_mem_pool_size=20M
```

```
set-variable = innodb_file_io_threads=4
set-variable = innodb_lock_wait_timeout=30
```

NOTICE

Best practice is to archive the modified database sizing file somewhere safe. Upgrading or patching your installation may overwrite your settings, and you can simply copy the archived file to the correct location to recover any configuration you have made if that occurs.

Oracle Version Support

This software supports Oracle 9i (9.2.0.5) up to Oracle 12c R1.

NOTE:

This application does not support Oracle 8i or 7.3.3 in this and later releases.

If you use Oracle 9i, Oracle recommends using 9.2.0.5 or above. For High Availability installations, we recommend using Oracle 10g RAC, or later.

If you use Oracle 12c, this application does not support multitenant feature.

This application does not include Oracle JDBC drivers.

You must set the environment variable `ORACLE_HOME` to a valid path for the local Oracle installation. The application expects that home directory to contain `bin` and `jdbc` subdirectories.

Oracle Databases

Oracle databases are recommended for highly available installations. See Chapter 7, Oracle Database Management for more.

Trap Processing Speeds

The following describes event processing speeds for the mediation service, the portion of this application that communicates directly with the devices under management, and the application server, which receives events from the mediation service, processes them, and formats them so that a client can view them. The nominal sustainable rate and a burst rate are two variations on these performance numbers. The sustainable rate is what is expected during normal operation.

This application typically does not lose traps as they come in. It can handle the burst rate, but only for a short period falls behind and events are backed up. This is standard behavior for Event Monitoring systems.

Application server inserts event data into the database, updates alarm states in the database, executes propagation logic, and executes any necessary automation. Besides handling incoming events, application server also handles client requests from event or alarm views and these result in database queries.

NOTE:

The performance of the database significantly effects event processing.

Mediation is a service. Without a separate mediation server, this service is running in the application server. The mediation service correlates events against the inventory model, applies event filtering, and determines what actions, if any, should execute for an event. When events come into the system, from any protocol, they queue for processing by mediation. At regular intervals, mediation submits processed events to the application server for more processing against the database. The remaining queued events wait while the current batch is being committed.

The application immediately converts SNMP traps into events and then queues them for mediation. It handles syslog differently, spooling all messages on disk first and then discarding or escalating them to event status. By default, all syslog messages are escalated. Handling a large volume of events may involve some analysis of the events coming in and modifications to event definitions and processing rules.

A separate mediation server commits more resources to receiving, filtering and converting incoming data. Off loading mediation services to a separate mediation server will also free up resources on the application server to do more alarm correlation and propagation. A dedicated southbound interface can also be configured to increase reliability at high rates.

The numbers here reflect both SNMP traps as well as Syslog messages. Syslog messages can be received at a higher rate without loss and are inspected very quickly, but escalated syslog messages must still go through general event processing and correlation.

Event type				
	SNMP		Syslog	
Service	**Sustained (traps/s)**	**Burst (traps/s)**	**Sustained (msgs/s)**	**Burst (msgs/s)**
Mediation	200	4000	200	20,000
Application	120	2000	120	10,000

NOTICE

Sustained counts reflect the number of events that pass through correlation and filtering. For example, 10,000 syslog messages may yield only 50 escalated events. Here, the sustained rate for syslog is low because we are assuming all messages are escalated. Higher volumes require more configuration to detect and ignore unwanted traps or messages at the mediation layer.

Swap Files and Services

Best practice is to set the swap file for Windows to at least 1536M (larger is better), with its minimum and maximum being set to the same value to avoid resizing and fragmentation of the swap file. Ideally, it would be on its own partition or drive, separate from the OS or database.

Also, best practice is to look at what else is running on the box, including third party software *and* Windows services (`services.msc`). Stop unnecessary services and reset their startup type to manual.

For example:

If netbios is enabled over TCP/IP, it should be disabled in the *Advanced TCP/IP properties* (*WINS* tab) for each connection, and the netbios, netbt, netbios helper and browser services should be stopped and disabled. The netbios and netbt services are not visible from the services control panel applet, but can be stopped using `net stop netbios, net stop netbt`.

Client Password

The first time users log in to a client, they are prompted by the interface to change their password. The default login is *admin*, and the default password is blank (no text).

NOTE:

The password is encrypted in the database.

CORBA Integration

Dorado recommends/uses Web services for integration between this application and an existing CORBA platform/environment. The majority of CORBA ORB vendors currently support Web services/SOAP messaging.

Setting Up FTP / TFTP

Install FTP and TFTP server pairs on the same machine, if your operating system does not come with one. (Open source examples: Filezilla, TFTPD64.) Both FTP and TFTP servers must share temporary file directories, with adequate permissions to read, write and delete any files transmitted.

Once you install these servers, use the *Common Setup Tasks* or *File Servers* portlets to enter the address and login information for the server(s).

While this application provides an internal FTP/TFTP server, best practice is to use that internal FTP/TFTP server only for testing. Installing an FTP and TFTP server as services on Windows hosts, and using the included Linux FTP / TFTP daemons is essential in production applications.

Consult FTP Servers on Linux on page 32 for additional information about setting up the internal FTP / TFTP servers (daemons) on that operating system.File Management does not always require the TFTP Server, but some devices require it to transfer files. On the other hand, the FTP server is always required.

FTP Servers on Linux

The internal file server does not work on these operating systems. The following sections describe how to use their alternatives to that file server. Installation of FTP, TFTP, SFTP and SCP depends on having the server correctly configured on Linux.

The following installation instructions describe how to do this:

CAUTION:
The banner files for external ftp servers should not contain FTP codes or words like "timeout" and "unknown host."

Refer to the operating system documentation for details about these, or if your operating system is not specifically mentioned below.

Operating System Settings

1 Edit /etc/ftpd/ftpaccess, adding the following line:

```
defumask 000
```

2 Execute inetconv

```
# inetconv
```

3 Verify the service is enabled

```
# svcs | grep tftp
    online         10:52:15 svc:/network/tftp/udp6:default
```

FTP

The following describers steps to set up FTP (and later TFTP) on Linux:

1 Create the user / password combination you want to use with the FTP server. For example: `ftp-user1`.

2 Confirm if FTP is installed by typing the following in a shell:

```
rpm -q vsftpd
```

The following is an example response (your version may differ):

```
vsftpd-2.0.5-10.el5.
```

If vsftpd is not installed, install it.

3 Modify the `vsftpd.conf` file which is in `/etc/vsftpd`

a. Become root.

a Edit `vsftpd.conf` file with a text editor.

b Uncomment the line `#listen = YES`

c Change `umask = 000` (must be at least `011`)

d Make sure `chroot_list_enable=YES` (and is not commented), and identify the `chroot_list_file` and location, making sure that line is not commented either.

e Save `vsftpd.conf`

f Create `chroot_list` in the selected location (default: `/opt/etc/vsftpd`), and enter the authorized user (here: `ftp-user1`).

NOTE:

The user must already be a system user with a valid password. You must also be able to find /home/ with that user's home directory beneath it.

g If necessary, run: `/sbin/service vsftpd stop`. It stops any running vsftpd.

h Run this to restart the FTP process: `/sbin/service vsftpd start`

i Confirm the FTP process is running `netstat -a | grep ftp`

TFTP

If you need TFTP to communicate with your managed resources, follow these steps to install and configure it.

1 Confirm TFTP is installed by running this command in a shell:

```
rpm -q tftp-server
```

The following is an example response (your version may differ)

```
tftp-server-0.42-3.1
```

If TFTP-server is not installed, install it.

2 Start TFTP with the following shell commands, once you are logged in as superuser:

```
/sbin/chkconfig --level 345 xinetd.d on
/sbin/chkconfig --level 345 tftp on
```

3 Modify the following line in the `tftp` file in `/etc/xientd.d/` to look as follows:

```
server_args = -u ftp-user1 -s /home/ftp-user1
```

(This sets the same directory for ftp & tftp)

4 Change `disable=yes to disable = no`

5 Save the file, then restart `xinetd` by going to System > Administration > Server settings > Services, and enter the root password. Select `xinetd` and click *Restart* (or click *Stop*, then click *Start)*.

6 Run the following in a shell to verify TFTP is running: `netstat -a | grep tftp`. A response should indicate such a process is running.

NOTE:

The test files in the ftp user's home must have at least -rw-rw-rw (666) permissions for Dell OpenManage Network Manager's server test to be successful.

Ports Used

For more information about the Ports and Flows, and how to set up firewall access, refer to the *User Guide*.

2

Installation Overview and Prerequisites

The installation process installs the application, including its foundation class software. (Oware provides the foundation classes for these applications.) You must have administrative privileges on your host to properly complete the installation of this application. For hardware requirements, and other prerequisites, consult the sections following System Basics on page 11.

This application is incompatible with any other software using the standard SNMP ports (162, for example), or other raw sockets. Either stop the conflicting application before you install this one, or stop this one whenever you want to use the alternative. You may have to reboot to close conflicted sockets. To stop this application, you must close the client *and* stop the Application Server (see Stopping Servers on page 103).

NOTICE

Upgrading from a previous installation is automated, but best practice is to back up the existing system first to ensure data preservation. Some packages may have an install wizard option to back up the database before upgrading.

Quick Start

The typical sequence of events, including installation is the following:

Install the software—See Installing the Application on page 49 for details.

Discover Network Devices—See *User Guide* for detailed instructions, or right-click to create or use a profile in the *Discovery* portlet and enter the IP addresses you want to discover. You may also have to enter SNMP and Telnet login/password combinations to fully discover equipment. Once you have discovered equipment, you can manage it.

Begin Managing your network

You can also administer your application, setting up users, and equipment access passwords, and groups for both users and equipment, as you begin to use it.

Benign Errors

The `HeapDumpOnOutOfMemoryError` is not an error, and is not logged at ERROR level. This is a Java VM option which enables creating a heap dump when the VM encounters and OutOfMemoryError. This dump may be useful to help diagnose memory issues.

The `SOAP Service Manager: Unable to read 'DeployedServices.ds: assuming fresh start` warning appears the first time you run SOAP. The file it refers to does not exist and is then created for the first time. This is just a warning, not really an error.

Basic Network Considerations

This application communicates with devices over a network. In fact, you must be connected to a network for Application Server to start successfully. Firewalls, or programs using the same ports on the same machine where this application is installed can interfere with its ability to communicate with devices. See Ports Used in the *User Guide*.

Your network may have barriers to communication with this software that are outside the scope of these instructions. Consult with your network administrator to ensure this application has access to the devices you want to manage with the Protocols described below.

NOTICE

One simple way to check connectivity with a device is to open a command shell with Start > Run `cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected devices.

Consult the *User Guide*'s Troubleshooting chapter for additional information about how to troubleshoot this application.

Name Resolution

This application requires resolution of equipment names, whether by host files or domain name system (DNS). If your network does not have DNS, you can also assign hostnames in `%windir%\system32\drivers\etc\hosts` on Windows. You must assign a hostname in addition to an IP address in that file. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

CAUTION:

This software does not support installation to anything but the local file system. Avoid installing to shared drives.

Protocols

This application uses the following protocols: TCP/IP, SNMP, HTTP, UDP Multicast. You can bypass multicast, if it is disabled on your network. To allow a client to connect without multicast, add the following property to the client's `owareapps\installprops\lib\installed.properties` file.

```
oware.application.servers[Host1 IP address], [Host2 IP address]...
```

Fixed IP Address

Dell OpenManage Network Manager includes a web server, among other things, and so must be installed to a host with a fixed IP address. For demonstration purposes, you can rely on dynamic IP address assignment (DHCP) with a long lease, but this is not recommended for production installations. See Using Load Balancers (Proxy) on page 46.

Windows Prerequisites

This application requires a temp directory on the host where it is being installed. If the install launcher cannot extract a Java Virtual Machine (JVM), then it cannot run. The launcher extracts a JVM to a temp directory and then starts the installer main using this temp JVM.

Windows typically has a temp directory, `WINDOWS\temp`. Installation expects that TEMP or TMP environment variable exists and points to this temp directory (check in a command shell with `cd %TEMP%` or `cd %TMP%`).

You can also execute the `win_install.exe` installation from a command line to override temp directory locations with this command line:

```
win_install.exe -is:tempdir c:\mytemp
```

Although it is not always necessary, during installation or uninstallation a suggested option is to disable any virus protection software, and any other running application. Some applications have additional services (like Norton Unerase) that prevent correct installation on some systems. Stop these in Services in Control Panel's Administrative Tools.

This application cannot co-exist with other installations of Cygwin on the same Windows computer. Do not install it where Cygwin is already installed, either separately or as part of another application. If Cygwin is already installed, remove it before installing this application.

If they are present, turn off Microsoft Windows SNMP Services and Traps.

Linux Prerequisites

If you are installing on Linux, you must log in as a non-root user. Linux installation prompts you to run some additional scripts as root during the installation process.

CAUTION:
Do not log in as root and su to a non-root user. Make sure your login automation does not do this either. This causes problems, particularly with upgrades.

When installing to Linux, ensure you are installing as a user with the correct permissions, and are in the correct group. You must configure the installation directory so this user and group have all permissions (770, at least). You may install without any universal ("world") permissions. However, you must create a home directory for the installing user.

NOTE:

All files created during installation respect a umask of 007. All files from [operating system].jar are 770. Files from ocpinstall -x are set for 660. Bin scripts from ocpinstall -x are 770.

Best practice is to install as the user designated as DBA. If necessary, create the appropriate user and login as this user for running the install program. The installing user must have create privileges for the target directory. By default, this directory is `/opt/dorado`.

CAUTION:
Linux sometimes installs a MySQL database with the operating system. Before you install this application, remove any MySQL if it exists on your Linux machine. Make sure to remove or rename the my.cnf file for that previous installation. If it is on the path, it can interfere with the correct operation of Dell OpenManage Network Manager. See MySQL Server Configuration File Examples on page 21 for more about configuring MySql.

NOTE:

To set the environment correctly for command line functions, after installation, type `oware` (or `. /etc/.dsienv` in Linux—[dot][space]/etc/[dot]dsienv) before running the specified command.
Also: This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on) but the installer will only install shortcuts for CDE.

Best Practices: Linux

- This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on).
- Most Linux installations include lib-apr for Tomcat. This application requires it, so if you have customized your Linux host(s) to omit it, put it back.
- Make sure any third party firewall or Linux's IP Tables firewall is off or allows traffic on the ports needed for your installation. See the Ports Used section of the User Guide for specifics.
- Install your Linux distribution (example: CentOS) on the server, choosing Basic Server when prompted to select software. CentOS should be the only repository selected. Choose Customize Later to decline further customizing the installation.

- Xvfb must be running to have a web client work correctly. This is automated when application server starts automatically. You can manually start this process with root access using the following:

  ```
  [root@test X11]Xvfb :623 -screen 0 1152x900x8 2>/dev/null &
  ```

  Confirm xvfb is running as follows:

  ```
  >ps -ef | grep Xvfb
  root 25991 21329 0 16:28 tty2 00:00:00 Xvfb :623 -screen 0 1152x900x8 qa
     26398 26053 0 16:31 pts/3 00:00:00 grep Xvfb
  ```

  (The path may differ from this example.)

- If you are installing with an Oracle database, do not set the Oracle in Dell OpenManage Network Manager to user redcell.

Create a User and Prepare for Installation

1 Add your IP and hostname to `/etc/hosts`. For example (for host `Test.localdomain`):

```
10.18.0.241 Test Test.localdomain
```

Also: verify that `/etc/hosts` points to new name-use the cat command and you should see output with the correct IP Address / hostname pair(s).

```
[qa@Test Desktop]$ cat /etc/hosts
10.18.0.241 Test Test.localdomain
```

Remember: Dell OpenManage Network Manager requires a fixed IP address for its host.

2 Login as `root`, create a new user with a home directory, set the password and add the user to the proper group. Here are examples of the commands for this. configuring user `test`:

```
useradd -m test
passwd abcxyz
usermod -aG wheel test
```

The wheel user group allows password-less `sudo`.

The wheel user group allows password-less `sudo`.

CAUTION:
If you are installing with an Oracle database, do not make the user for Oracle redcell.

3 Copy the installation files to the system.

4 After unzipping the installation files, copy the folder with source files as a subdirectory of a directory (for example: /home/test) on the hard disk of the server. Set permissions on the installation directory:

```
chown -R test /home/test
chmod -R 777 /home/test/install_path
```

5 Make sure the installation script has permission to execute:

```
chmod +x /home/test/install_path/linux_install.sh
```

6 Create the target installation directory structure and set permissions. Assuming test is the installing user, the following are examples, not defaults:

```
mkdir /dell
mkdir /dell/openmanage
mkdir /dell/openmanage/networkmanager
chown -R test /dell
chmod -R 777 /dell
```

7 Disable Firewall with System > Administration > Firewall, or disable the firewall, and configure the network interface card with a static IP address from a command shell with the following command(s):

```
setup
```

You may be prompted to enter the root password; the password dialog may also appear behind the Firewall Configuration Startup dialog.

8 In some Linux distributions, by default the Network Interface Card (NIC) is not active during boot, configure it to be active and reboot:

```
nano /etc/sysconfig/networking/devices/ifcfg-eth0
```

Change ONBOOT = no to ONBOOT = yes

9 Disable SELINUX. Turn this off in `/etc/selinux/config`. Change

```
SELINUX=disabled.
```

This and the previous step typically requires a reboot to take effect.

10 So...from a command line, type `reboot`.

11 Once reboot is complete, login as `root` update the system:

```
yum update -y
```

12 Linux (CentOS particularly) sometimes installs MySQL libraries by default, this interferes with Dell OpenManage Network Manager since it installs its own MySQL version. Remove mysql-libs from the system:

```
yum remove mysql-libs -y
```

Dell OpenManage Network Manager needs C + + compatibility libraries installed

```
yum install compat-libstdc++-33.x86_64 -y
```

...and install 32-bit compatibility libraries (for MySQL). (See 32-bit Linux Libraries on page 54)

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

...and reboot:

```
reboot
```

Alternatively, do these steps in the Syst

em > Administration > Add/Remove Software user interface.

13 If you have not already done so, configure file handle maximums. Open `/etc/security/limits.conf` and ensure the following are at minimum 65535:

```
test soft nofile 65536 test hard
nofile 65536 test soft nproc 65536
test hard nproc 65536
```

Here, `test` is the installing user login.

Set these limits higher for more heavily used systems. You can also check/set file handles temporarily using the `ulimit -H/Sn` command. For example:

```
$ ulimit -Hn
$ ulimit -Sn
```

CAUTION:
If you enter ulimit - a in a shell, open files should NOT be 1024, and User Processes should NOT be 1024. These are defaults that must be changed. If you do not have enough file handles, an error appears saying not enough threads are available for the application.

14 Restart Linux. (`reboot`)

32-bit Linux Libraries

For 64 bit installations, you must identify the appropriate package containing 32-bit libtcl8.4.so (for the example below: tcl-8.4.13- 3.fc6.i386.rpm for Red Hat).

Do not use any x86_x64 rpms; these would not install the 32-bit libraries. Any 32-bit tcl rpm that is of version 8.4 and provides libtcl8.4.so works. You can download them from Sourceforge: http://sourceforge.net. Download these, then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect /opt/dorado/oware3rd/expect/linux/bin/expect
[someone@RHEL5-64bit ~]$ ldd /opt/dorado/oware3rd/expect/linux/bin/ expect
linux-gate.so.1 => (0xffffe000)
libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/ libexpect5.38.so (0xf7fd2000)
libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000) libdl.so.2 => /lib/libdl.so.2 (0x0033e000) libm.so.6 => /lib/libm.so.6 (0x00315000) libutil.so.1 => /lib/libutil.so.1 (0x00b8d000) libc.so.6 => /lib/libc.so.6 (0x001ba000) /lib/ld-linux.so.2 (0x0019d000)
```

Make sure that libtcl8.4.so maps to /lib/libtcl8.4.so

An Alternative for Red Hat Linux

1. Copy `/usr/lib/libtcl8.4.so` from a 32-bit RH system to `/usr/local/lib/32bit` on your 64-bit Red Hat system
2. As root, execute: `ln -s /usr/local/lib/32bit/libtcl8.4.so /usr/lib/libtcl8.4.so`

System Capacity

System requirements for each element of your system vary depending how you use it. The numbers in this guide are suggestions only, not definitive recommendations.

You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of the application on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your system requirements may be much higher. See System Basics on page 11 for more specific hardware recommendations.

Paths

Paths in this document are often written as Linux represents them, with foreslashes (/) rather than Windows/DOS backslashes (\). The shell command `oware` makes any shell subsequently emulate a bash shell. That means either foreslash or backslash can accurately represent path separators as they may appear, depending on whether the `oware` command has set the environment to bash emulation. Most shell commands for this application are available in Windows/DOS equivalents structured to call the emulator, then a bash script. If you have difficulty using a command line script in Windows/DOS, then try it after you have run `oware` or `. ./etc/.dsienv`.

NOTICE

Run command line scripts with -? to see their parameters.

CAUTION:

Do not install to paths with spaces in their names.

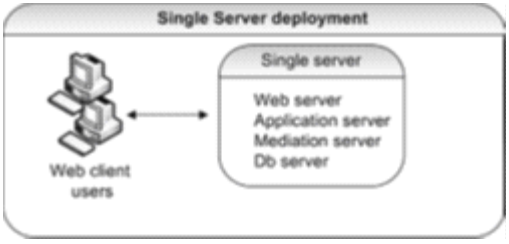
Installation Types

This application supports many installation and configuration options to fit the network environment it manages. Because several products (and later optional addons) can use the following features, best practice is to consider them when designing your installation and its capacities. In other words, design your application's installation using features that support its role in your network.

The following outlines the basic types of installation available with this application. See System Basics on page 11 for hardware recommendations based on your system load.

Single-Server Edition (Standalone)

An ideal solution for smaller network environments recommended only for the most limited deployments. A single host can be Web Server, Application Server, Mediation Server, and Database Server..



This is a typical configuration for small environments, with a limited number of managed network devices. It includes these features:

- Supports five clients.
- Does not support registering multiple domains in the web client.
- Does not support database replication (upgrade to HA edition to get this feature)
- Does not support application/mediation server failover available (upgrade to the HA edition to get this feature)

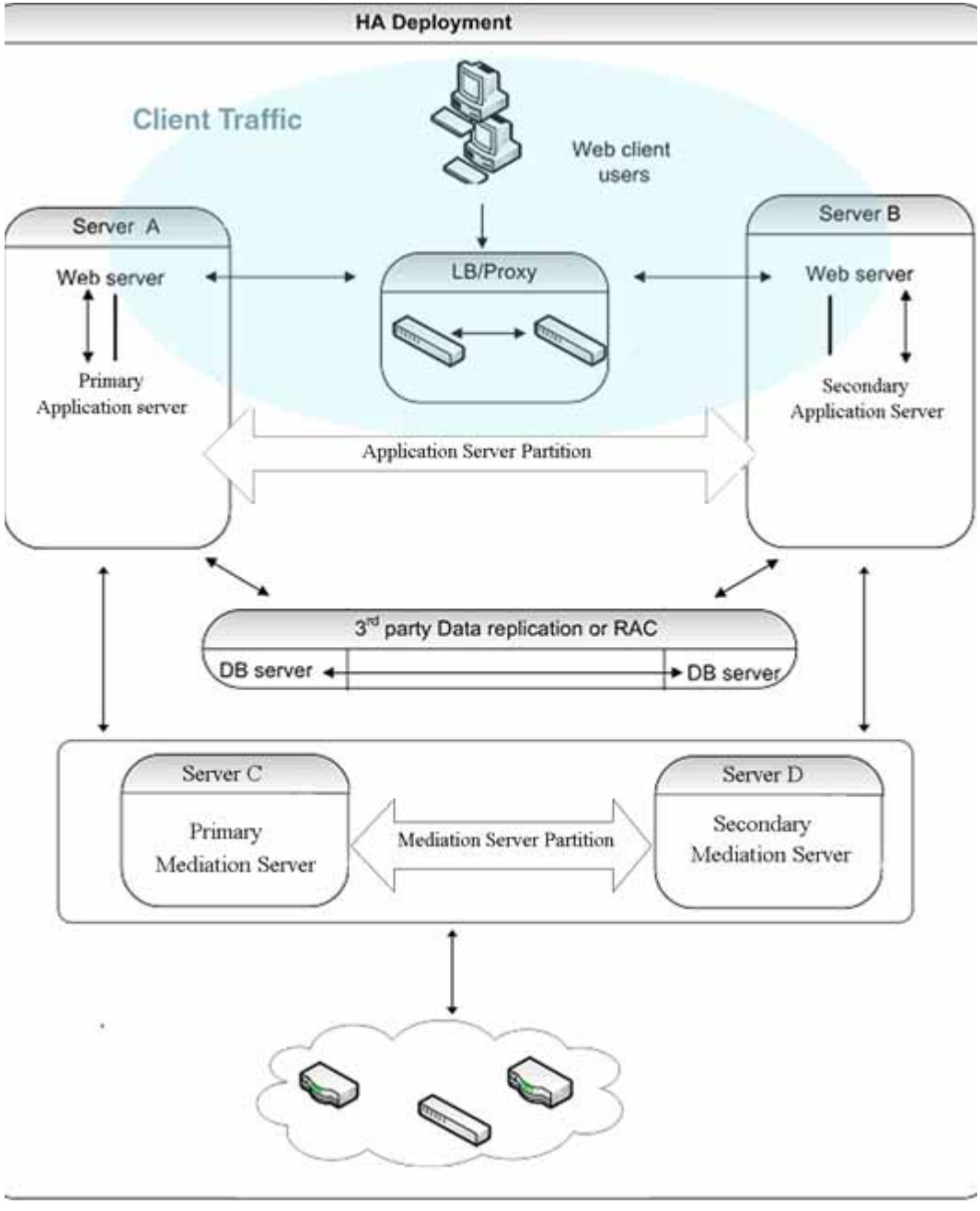
CAUTION:

Even in single server installations, best practice is to ensure that your database, whether embedded (MySQL) or Oracle, resides on a separate disk, not just a separate disk partition.

Also: The host where you install this application must be on a network.

High Availability Edition

The High Availability (HA) capability makes the Application Server highly available and load balanced. Normally used in carrier-class or very large deployments.


HA Deployment
Client Traffic
Web client users
Server A
Web server
Primary Application server
LB/Proxy
Server B
Web server
Secondary Application Server
Application Server Partition
3rd party Data replication or RAC
DB server
DB server
Server C
Primary Mediation Server
Mediation Server Partition
Server D
Secondary Mediation Server

In this edition, primary and secondary paired mediation servers use configurable heartbeats to monitor each others status. If the secondary mediation server detects that the primary is down, it will take over. The Application Server also monitors the mediation server and will generate an event/alarm if the primary mediation server goes down. Configurable trap buffers reduce trap loss during failover.

Primary and secondary Application Servers also use configurable heartbeats to monitor each others status. If the primary fails, the secondary will take over and will also generate an event/alarm. Clients and mediation servers identify applications servers by partition name. The name is the same for the primary and secondary Application Server, so the failover is transparent to the clients and mediation servers.

Paired load-balancers / proxy servers direct web users to an available web server, and distribute web server traffic to an available application server.

If you want to extend this to the database, Oracle Real Application Clusters (RAC) handle database replication, synchronization and failover. Application Servers identify Oracle by Service Name which is the same for all Oracle hosts, so failover between Oracle hosts is transparent to this application.

You can also have a form of HA at the application level with transaction management. For example:

HA installations support the following:

- Application Server clustering
- Mediation server failover
- Supports Database replication (must have Oracle Parallel Server, Oracle's Real Application Cluster [RAC] or equivalent, database).

When you are installing a high availability system, installation includes a setup screen for the Config Server (the primary server). The multicast address is configured automatically.

The following are some HA installation considerations.

- HA does not require DNS entries for all servers.
- Servers (Application or Mediation) in HA need to share the following piece of information:
- **Partition Name** - Some unique string for this HA, begins with a letter. You can configure this name one of several ways:
  - Installation wizard
  - Command line: - typical for testing
  - installed.properties - the command line overrides this property file.
  - pmstartup.dat - settings used by automatic server startup (i.e., Windows Service)

Dell OpenManage Network Manager High Availability (HA) consists of the following installations:

- 2 Application and Web Servers
- 2 Mediation Servers
- 2 Database Servers (Oracle RAC or MySQL Replication)

You can also configure Oracle database installations for failover (see Oracle Failover on page 244).

Application Servers and Web Portals

By selecting Application Server and Web Portal installation option during the installation process, you can install Dell Open Manage Network Manager's Application and web server on a separate machine.

As in most installations, and as is essential for HA installations, you must select a partition name, whether the server starts automatically on host startup, the heap size, database type and location (host and port).The default heap size for the web server is 2G, but you can configure a larger heap to support more clients. The default port is 8080. See the User Guide for information about installing with SSL.

.Web server starts automatically once installation is complete. In Windows, right-click the Apache Web server icon to Configure it (heap size, for example), Start and Stop this service. See Starting the Application on page 63 for complete instructions, including Linux.

Mediation Servers

For reliability, paired Mediation servers can fail over when they transmit SNMP traps and/or Network Element-initiated Syslog Messaging to Application Server(s). Both Mediation Servers must be in the same partition.

Each server has a primary and a secondary role, and uses keep-alives heartbeats to verify the other Mediation server's operational state. Based on the operational state, only one Mediation server (the primary) forwards messages to the Application Server(s) for processing.

Database Servers

Like the Application Server, you can deploy the Database Server in a fault tolerant configuration to eliminate data lost during a system failure and to ensure data integrity. This configuration typically uses MySQL Replication or Oracle RAC. You can cluster the Oracle database servers.

Using Load Balancers (Proxy)

Deployments where many users access the system concurrently may require a Load Balancer, also known as a Proxy, to manage traffic to multiple Web Servers. If one web server is overloaded or un-responsive, the Load Balancer directs users to a responsive Web server. Single-server installations do not require a Load Balancer.

With the proper configuration the same load balancer can serve both web server and application server.

Dell OpenManage Network Manager's web server(s) is (are) between application servers and clients. To add high availability-like capabilities a web served application system, you may use an open-source load balancer like HAProxy either between the web servers and application servers, or between clients and web server. For high availability (HA) installations, systems typically use pairs of load balancers. Dell OpenManage Network Manager needs at least one load balancer pair to distribute loads among webservers. The load balancer IP is what clients connect to. If webserver and appserver are on same machines, all web servers can point to 127.0.0.1 to use their own local appserver. If webserver and appserver are on different machines, they must have another load balancer pair to distribute loads among appservers. All web servers then point to the appserver load balancer IP

Load Balancer recommended hardware (or equivalent)

Configure your minimum hardware based on the expected number of connection per second:

- Less than 10000 connection/ sec 1 GB RAM, 2GB HD, Atom processor
- Up to 20000 connections/sec 4 GB ram, 10GB HD, Core DUO processor.

Deployments vary based on application usage, system availability and redundancy needs.

Deployment recommendations depend on system sizing factors discussed in the Sizing section.

Refer to Best Practices: Single Server Hardware on page 16 for hardware recommendations

Mediation Server Subnets

For other Mediation server-initiated Dell OpenManage Network Manager functions like provisioning, configuration, backup, restoration, compliance monitoring, and so on, you can optionally assign Mediation servers to a management subnet on an installation screen.

When Dell OpenManage Network Manager initiates communication to a Network Element in the assigned subnet, the Application Server attempts to use the Mediation server for that subnet. Application Server(s) update their list of active Mediation servers every 15 seconds. When Dell OpenManage Network Manager needs to communicate to a device that is on a subnet without an assigned Mediation server, it uses the first Mediation server on the Active Mediation server list. If for some reason a device does not respond to a Mediation server, the Application Server try the next Mediation server on the Active list. During installation Accept or alter the subnet mask for this agent. By default the subnet mask is 255.255.255.0. This mask represents the portion of the network serviced by this agent.

If you want to change this subnet later, the `installed.properties` file (in `owareapps\installprops\lib\`) has a `oware.mediation.subnet.mask` property that you can re-make. You must then restart the mediation server.

Mediation request routing supports explicit configuration of device scope managed per mediation server partition.

Routing Behavior

Each mediation request made by the application is routed to a server for execution. The routing is based on the IP address of the device to be communicated with. The logic of this routing is as follows:

—Is the target IP already in a mediation server's device list?

yes - Is the same mediation server still available?

yes - Use the same agent

—If no agent yet determined

For each available mediation server...

For each `ip;mask` pair (default and additional config),

calculate network address from IP and mask

calculate network address from device IP and mask

Do they match?

yes - add mediation server to preferred agent list

Were any preferred agents found?

yes - use the least loaded agent from preferred list

add device IP to the agent's device list (use same server next time)

replicate agent device list within application server cluster

—If no agent yet determined

Is the local application server configured to do mediation?

yes - use the local server (not “sticky”)

no - execution of mediation request will fail

Compatibility with Previous Versions

The impact of the above behavior on previous mediation versions occurs only where no preferred mediation server is available. Before such behavior was available, the application made an arbitrary selection from any available mediation servers, possibly using the same server every time. Now, only the local application server can handle the request. If you have configured the application server to perform mediation (true by default), then the system should continue to execute these requests as it had in the past. If the application server is not configured to perform mediation, then requests may fail with `no mediation` errors instead of being routed to the wrong mediation server possibly resulting false `device not available` errors.

Configuration Options

By default, each mediation server has a single network mask established during installation. Each mediation server in a HA Pair should yield the same network address when the default mask is applied to the mediation server's IP address. Here is an example of a default mask setting on a mediation server:

```
oware.mediation.subnet.mask=255.255.255.0
```

In addition to the default mask, you can define additional routing configurations as application server properties. Each application server should have the same settings. You can add more IP Addresses and/or masks to the default configuration made locally on the mediation server for each mediation server partition. The property name is `com.dorado.mediation.routing` with a mediation partition name appended. Here is an example of routing requests for any device IP address starting with 10.10 to a mediation server named `foo-medPartition`:

```
com.dorado.mediation.routing.foo-medPartition=10.10.0.0;255.255.0.0
```

```
This appends Partition to the partition name. For example
  com.dorado.mediation.routing.rcellmedPartition=172.16.0.0;255.255.0.0
```

The syntax for routing configuration values is as follows:

```
ipAddress;mask[,ipAddress;mask]
```

Basically, you can add more IP and mask pairs as comma delimited values. If you omit the mask, then Dell OpenManage Network Manager assumes it is 255.255.255.255. If you omit the IP address, then Dell OpenManage Network Manager assumes the address is the mediation server's IP address. If an IP address or mask is not valid, a warning appears once in the application server log when the properties load. If one of several values for a single property is not valid, Dell OpenManage Network Manager still applies the other setting.

The application server itself performs mediation when no agents are available. This is required unless your deployment includes at least one mediation server. All application servers must have the same configuration. To disable mediation services on an application server after you have configured a distributed mediation server elsewhere, add the following property on the application server (preferably in `installed.properties`):

```
oware.appserver.mediation.setup=false
```

Installing the Application

Install on Windows

The following steps install the application with the installation wizard on Windows. You can also install with a command line; see "Command Line and Silent Installations" for more about those.

Single-Server Installation

Single-Server Installation Screens for Windows

The following lists the screens displayed during Dell OpenManage Network Manager Single-Server installation on Windows:

- **Instruction:** this dialog displays the OMNM version and it also reminds you to shut down other running software (this may include anti-virus software).
- **Software Requirements**: this dialog displays the minimum system requirements and it also provides the link to OMNM user guide.
- **License Agreement:** This dialog displays the Dell Software License Agreement. You must accept the terms of the License Agreement to proceed.
- **Choose Install Folder:** This dialog screen lets you select the directory where the application installs. If you want to install to a different directory, type the path or click Choose to select another in a directory browser.
- **Network Interfaces:** If you are installing the software on a machine with multiple network interface cards, installation prompts you to select one IP address for the system you are installing. Also: Windows 2008 may not support the installer finding the host's IP Address. In such cases, a screen appears where you can enter the IP address and Partition Name for your installation.
- **Heap Settings:** This dialog let you specify memory settings for the application server and Web server. Refer to Memory Tuning (Heap & Portal) in the User Guide for more about setting heap size.
- **MySQL Setup:** This dialog requests a data path, an initial size and maximum size. A blank maximum allows growth without limits.
- **Possible Port Conflicts:** This dialog appears when the installer detects port conflicts. This typically occurs when other application(s) reside on the same server is using the port(s).To determine the source of the port conflict and remove the application, please refer to Ports Used section in the User Guide. Best practice is to install on a dedicated server platform.
- **Pre-Installation Summary:** This lists the installation summary. Please review and click Install.
- **Install Completed Successfully:** This dialog indicated Del OpenManage Network Manager has been successfully installed. Click Done to finish.

Install Dell OpenManage Network Manager

1. Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.
2. If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with `@. Also:` You must extract any compressed (zipped) installation source before executing the installation. Do not modify the package folder structure in any way prior to installation.

3 Follow the instructions displayed in the installation screens to complete the installation process.

4 When application server and web server have completed their startup, open a browser to this URL: `[application server IP or hostname]:8080`

Single-Server Post Installation

- Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) can have a significantly impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the User Guide for details about tuning these policies.
- After you complete the installation, you may want to install Adobe Acrobat Reader. You can download a free copy from www.adobe.com. This application requires Acrobat to successfully print reports.
- Additional post-Dell OpenManage Network Manager installations can also include Perl and FTP/TFTP servers. See "Installing Perl" and "Setting Up FTP / TFTP" .
- See "Starting the Application" for instructions about running what you have just installed.

High Availability Installation

HA Installation Screens

The following lists the screens displayed during Dell OpenManage Network Manager High Availability (HA) installation on Windows:

- **Instruction:** this dialog displays the OMNM version and it also reminds you to shut down other running software (this may include anti-virus software).
- **Software Requirements:** this dialog displays the minimum system requirements and it also provides the link to OMNM user guide.
- **License Agreement:** This dialog displays the Dell Software License Agreement. You must accept the terms of the License Agreement to proceed.
- **Component Summary:** This dialog lists OMNM package and platform versions. It also lists the components version summary.
- **Choose Install Folder:** This dialog screen lets you select the directory where the application installs. The default directory is `C:\Program Files\Dell\OpenManage\Network Manager`. If you want to install to a different directory, type the path or click `Choose` to select another in a directory browser. The installer checks for directory permissions. See Create a User and Prepare for Installation section for more instructions on how to set permissions on target installation directory.

- **Network Interfaces:** If you are installing the software on a machine with multiple network interface cards, installation prompts you to select one IP address for the system you are installing. Also: Windows 2008 may not support the installer finding the host's IP Address. In such cases, a screen appears where you can enter the IP address and Partition Name for your installation.
- **Choose Install Set:** This dialog lets you select what server(s) to install. The available install sets are Application Server, Mediation Server, Database, and Custom.
- **Choose Shortcut Folder:** This dialog lets you select a directory where you would like to create product icons..
- **Partition Name/Auto Start:** This dialog requests a partition name for application servers in High Availability installation. The partition name for the application servers must be the same. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore. This dialog also provides the option to start the application server on startup.
- **Heap Settings:** This dialog lets you specify memory settings for the server(s) that you are installing. Refer to Memory Tuning (Heap & Portal) in the User Guide for more about setting heap size.
- **Cluster Configuration:** This dialog appearance may vary depending on the type of server you are installing. If you are installing an application server, this dialog requests a Config server IP; typically, this is the IP address of the primary application server that you install for your HA. If you are installing a mediation server, this dialog requests a Config server IP, which is the address of the primary mediation server. Similar to application partition name, the Config server IP entry must be the same for application/mediation servers.
- **Database Selection:** This dialog lets you select the database type for your installation. This will apply necessary client configuration for connectivity to the remote database. You can select either MySQL or Oracle and proceed to the next screen.
- **MySQL Setup:** This dialog appearance may vary depending on previous selections made. If the option selected was *Configure Client*, then MySQL Setup dialog requests for the IP address and port of an existing MySQL database server where the application servers will point to. If the option selected was *Install Server*, then MySQL Setup dialog requests for MySQL data path, initial and max size. The default path is /dell/openmanage/networkmanager/oware3rd/mysql. If a Max Size (MB) is specified, capacity will grow as needed up the max size, else capacity will grow as needed unless the disk is full.
- **Oracle Setup:** This dialog requests username, password, host, port, and SID of an existing oracle database server which the application servers will point to.
- **Possible Port Conflicts:** This dialog appears when the installer detects port conflicts. This typically occurs when other application(s) reside on the same server is using the port(s).To determine the source of the port conflict and remove the application, please refer to Ports Used section in the User Guide. Best practice is to install on a dedicated server platform.
- **Pre-Installation Summary:** This lists the installation summary. Please review and click Install.
- **Mediation Partition Name/Auto Start:** This dialog requests a partition name and subnet mask for mediation servers in High Availability installation. The partition name for the mediation servers must be the same. Partition names must start with a letter and consist of

letters, digits, minus sign and/or underscore. You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask or use unicast to point mediation servers directly to the application servers. This dialog also provides the option to start the mediation server on startup.

- **Application Server Partition Name:** This dialog requests an application server partition name. This name is used by mediation servers for locating an application server on the network and establishing a connection between mediation and application servers. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.
- **Start Server:** This dialog asks if you want to start the server now..
- **Install Completed Successfully:** This dialog indicated Dell OpenManage Network Manager has been successfully installed. Click Done to finish.

HA installation outline

1 Install Database servers

2 Install Primary Application + Web Server

3 Install secondary Application + Web server

4 Seed the Database

5 Install Primary Mediation Server

6 Install secondary Mediation server

7 Install License

8 Restart all Servers

9 Add Mediation Domain and Routing Entry

Install Database Severs

Dell OpenManage Network Manager High Availability supports MySQL replication and Oracle RAC database structures. For MySQL Replication and Oracle RAC setup, best practice is to employ a trained DBA to either assist or manage the installation.

If you prefer Oracle as the database type, please follow the guidelines and recommendations in **Oracle Database Management** section for installing and configuring the database.

If you prefer MySQL as database type, OMNM High Availability installer provides the option to install MySQL database on a separate host. Consider the following steps to install MySQL servers (master and slave) as part of your MySQL Replication setup.

Install MySQL as Separate Server

The following steps describe how to install MySQL as separate server:

1 Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.

2 If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with @. Also: You must extract any compressed (zipped) installation source before executing the installation. Do not modify the package folder structure in any way prior to installation.

3 Follow the instructions on the installation wizard.

4 Select only **Database** in the **Choose Install Set** dialog. Follow the rest of the instructions on the installation wizard

NOTE:

Once you have completed installation of two MySQL servers using OMNM installation wizard, follow the MySQL guidelines (https://dev.mysql.com/doc/refman/5.1/en/replication.html) to configure your MySQL Replication.

Install Primary Application Server and Web Server

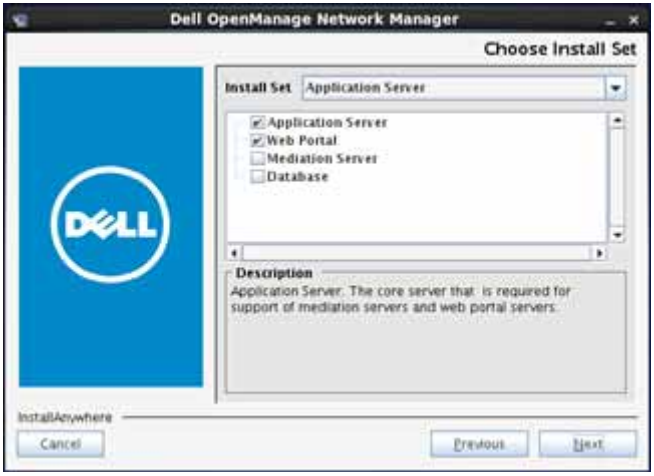
This section describes how to install Application and Web servers on the same host. For clarification on the installation screens, please review HA Installation Screens section.

1 Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.

2 If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with @. Also: You must extract any compressed (zipped) installation source before executing the installation.

3 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to HA Primary Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select both Application Server and Web Portal check-boxes.



- On the Partition Name/Auto Start dialog, enter a partition name for you application servers. This name must be the same for both primary and secondary server. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore. Select Auto Start if you want the server to auto-start on startup.

NOTE:

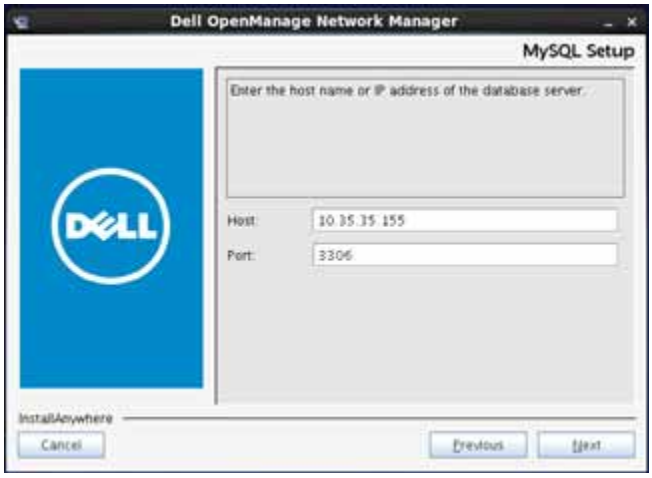
Recommend writing down this partition name for your secondary Application and Web server, and Mediation servers installations.

- On Cluster Configuration dialog, enter a **Config Server IP,** this is typically the address of this primary application server. Again this entry must be the same on both primary and secondary server.

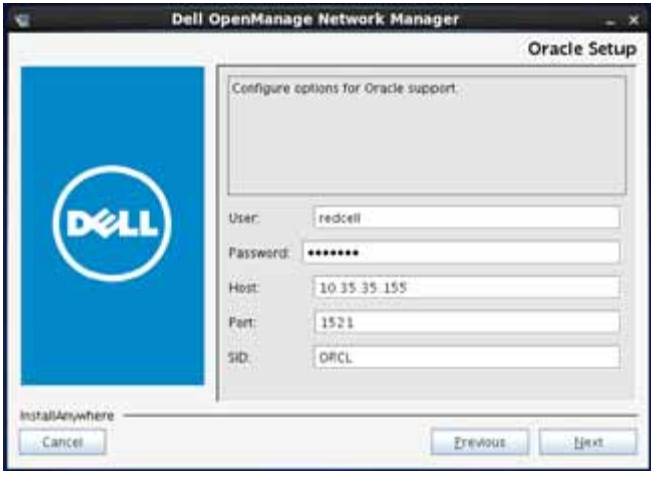
- On Database Selection dialog, select either MySQL or Oracle as database type.

- If you selected MySQL, the MySQL Setup dialog will request either the hostname/IP address and port number of the MySQL database server (See *Install Database Servers*

section for database installation) where your application and web server will be pointing to.



- If you selected Oracle, the Oracle Setup dialog requests the credentials of the Oracle RAC.



Install Secondary Application Server and Web Server

This section describes how to install Secondary Application and Web server. For clarification on the installation screens, please review HA Installation Screens section..

1 Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.

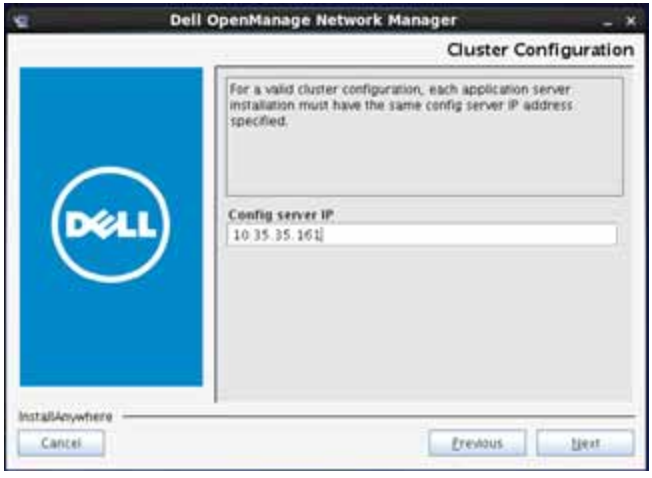
2 If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with @. Also: You must extract any compressed (zipped) installation source before executing the installation.

3 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select both Application Server and Web Server check-boxes.

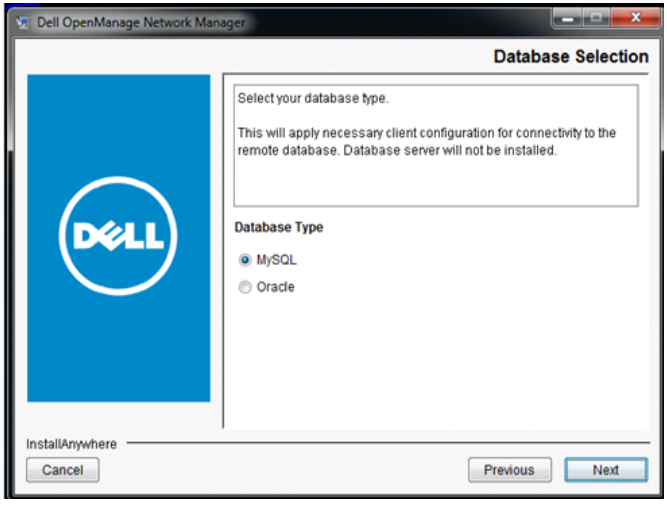
- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation

- On Cluster Configuration dialog, enter a **Config Server IP;** this is typically the address of this primary mediation server. Again this entry must be the same on both primary and secondary server.

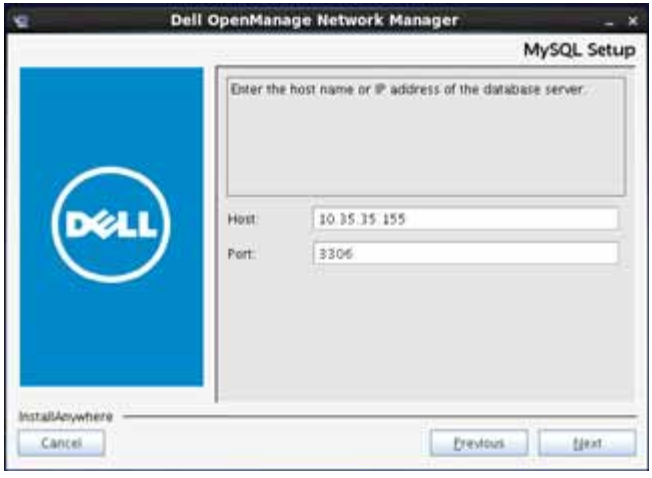


- On Database Selection dialog, select either MySQL or Oracle as database type. If you selected MySQL as database type for the Primary Application Server, then you must

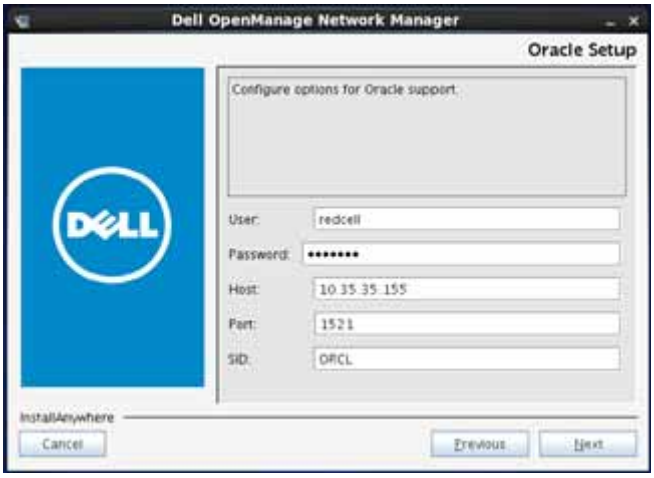
select MySQL as database type for this Secondary Application Server. The same rule applies if you selected Oracle.



- If you selected MySQL, the MySQL Setup dialog will request either the hostname/IP address and port number of the MySQL database server (See *Install Database* Servers section for database installation) where your application and web server will be pointing to.



- If you selected Oracle, the Oracle Setup dialog requests the credentials of the Oracle RAC.



Seed the Database

This section describes the process of creating the database schema and users for the OMNM application. Assuming that you have successfully completed the Application + Web server, MySQL Replication or Oracle RAC installation, please follow this guideline to complete the database seeding.

- If you selected Oracle as database type for this application, please skip the rest of this section and see *Oracle Database Management* chapter for steps to create database schema and user.
- For MySQL, from Command Prompt run the following commands on the primary Application server:
  - `Oware`
  - `pmstopall`
  - `loaddb -u root -w dorado`
  - `loaddb -u root -w dorado -s`
  - `dbpostinstall`
  - `pmstartall`

NOTE:

Test database connectivity with the command:

```
pingdb -u root -p dorado
```

The most likely reason that causes the seeding to fail is the invalid configurations in the installdirectory/owareapps/installprops/lib/installed.properties and installdirectory `/oware/synergy/tomcat-7.0.40/webapps/ROOT/WEB-INF/classes/portal-ext.properties.`

A correct configuration in the installed.properties file should have the three lines:

…….

com.dorado.bom_dbms.name=mysql

com.dorado.meta_database.name=//ipaddress:3306/owmetadb

com.dorado.jdbc.database_name.mysql=//ipaddress:3306/owbusdb

……..

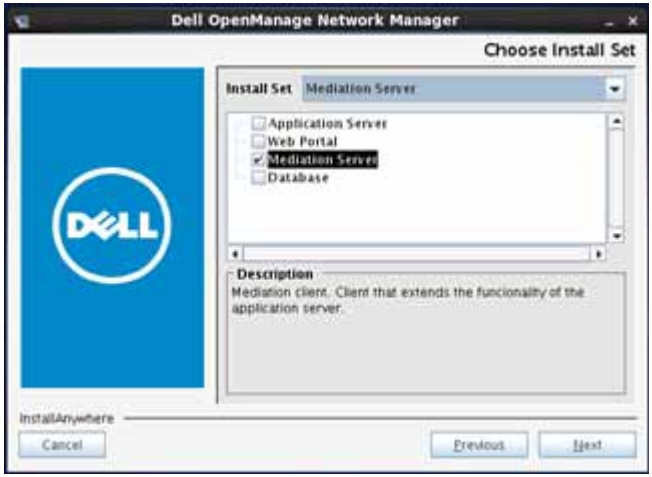
where ipaddress is the address or hostname of the database server.

And in the DATABASE OPTIONS portion of the portal-ext.properties file should list the correct IP address/hostname of the database server.

Install Primary Mediation Server

This section describes how to install Primary Mediation Server. For clarification on the installation screens, please review HA Installation Screens section.

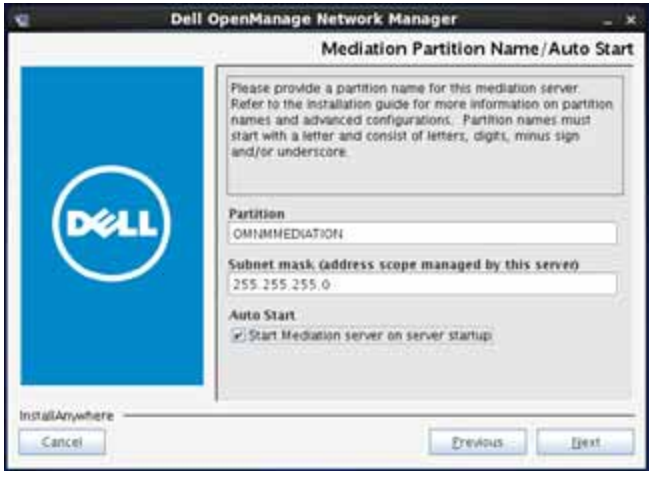
1. Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.
2. If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with @. Also: You must extract any compressed (zipped) installation source before executing the installation.
3. Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)
   - On the Choose Install Set dialog, select only Mediation Server checkbox.



- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation

- On Mediation Partition Name / Auto Start dialog, enter a Mediation Partition Name and Subnet Mask. The partition name must be the same for both primary and secondary mediation server. So whatever name you enter for the partition text field, you must enter the same name when you install the secondary Mediation server. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.

  You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask.



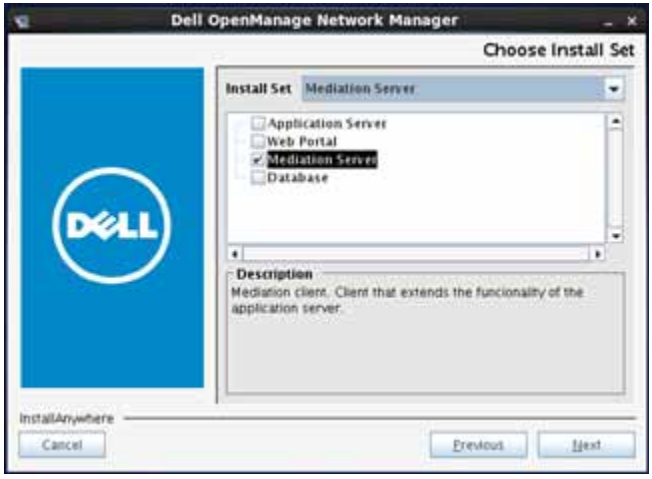
- On Cluster Configuration dialog, enter a **Config Server IP**; this is typically the address of this Primary Mediation server. Again this entry must be the same on both primary and secondary server.

Install Secondary Mediation Servers

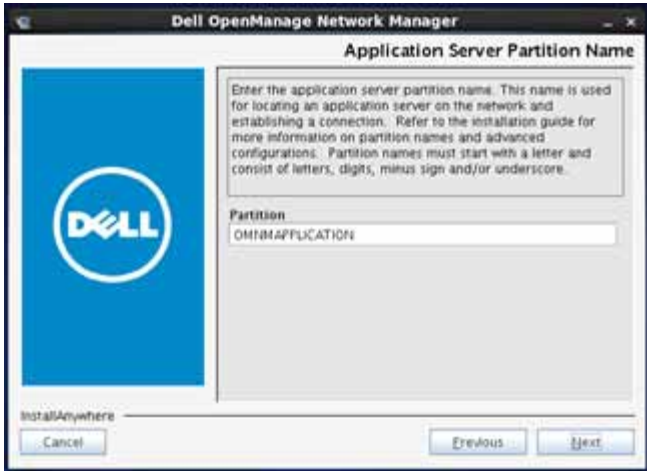
This section describes how to install Secondary Mediation server. For clarification on the installation screens, please review HA Installation Screens section.

1. Log in as a non-Administrator user with administrator's permissions (in the administrator group) on the Windows machine where you want to install the software.
2. If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager. Note: You cannot install from a directory whose name begins with @. Also: You must extract any compressed (zipped) installation source before executing the installation.
3. Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select only Mediation Server checkbox.

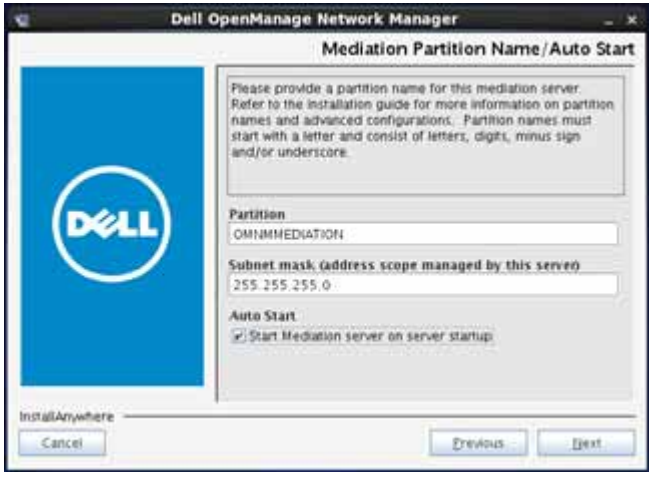


- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation..



- On Mediation Partition Name / Auto Start dialog, enter a Mediation Partition Name and Subnet Mask. The partition name must be the same for both primary and secondary mediation server. So whatever name you enter for the partition text field, you must enter the same name when you install the secondary Mediation server. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.

You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask.



- On Cluster Configuration dialog, enter a **Config Server IP**; this is typically the address of the Primary Mediation server. Again this entry must be the same on both primary and secondary server.

Install License

Dell OpenManage Network Manager High Availability requires license to be operational. Pllease see "Installing Licenses" to install HA license.

Restart All Servers

After you have completed the installation of all servers, you must restart all servers in the following order: Primary Application server > Web server (on same host as the Primary) > Secondary Application server > Web server (on same host as the Secondary) > Primary Mediation server > Secondary Mediation server.

Servers can also be restarted using the commands in Command Prompt:

To restart application server:

- Log into oware environment:

  `oware`
- Stop the server:

  `pmstopall`
- Wait for the server to stop completely (to view status of the server, use command `pmgetstatus`).
- Start the server:

  `pmstartall`
- Or If the Auto-Start is enabled, the appserver icon can be used to start the servers and web service.

Restart Web server (Right-click on Synergy Network Management icon and click Start service)

To restart Mediation server:

- Log into oware environment:

  `oware`
- Stop the server:

  `pmstopall`
- Wait for the server to stop completely (to view status of the server, use command `pmget-status`).
- Start the server:

  `pmstartall`

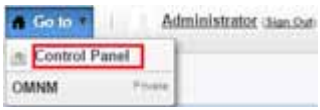
NOTE:

Servers may take up to 5 minutes to complete the initialization process and be ready.

Add Mediation Domain and Routing Entry to Discover Network Devices

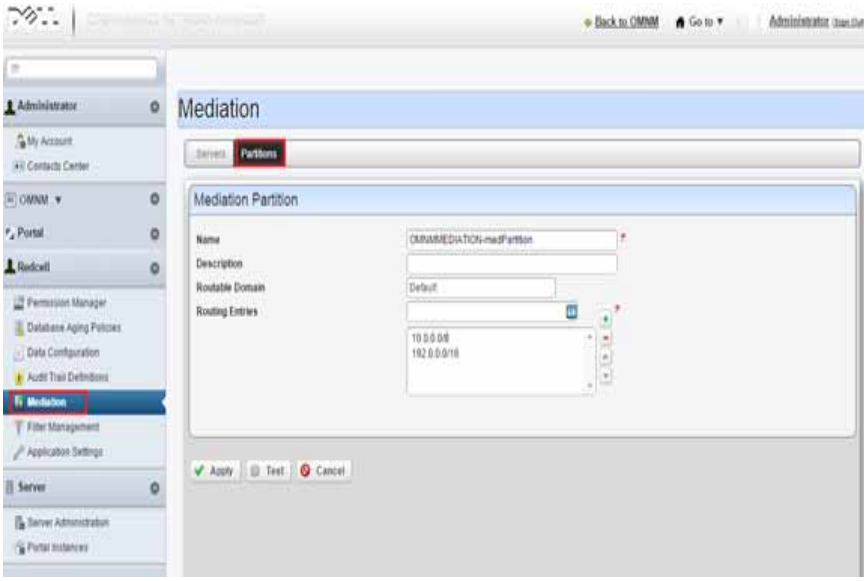
The routing entries determine which devices can use the mediation servers within the mediation domain. For example, you can specify individual subnets-10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16-or just add a 10.0.0.0/8, which covers all the 10.0.0.0 subnet. You can add or delete the routing entries without shutting down web or application servers. The mediation domain requires the -medPartition string appended at the end of the mediation domain name.

To add mediation domain and routing entries in Dell OpenManage Network Manager, go to `Control panel > Mediation > Partitions > Add Partition name and Routing Entries.`

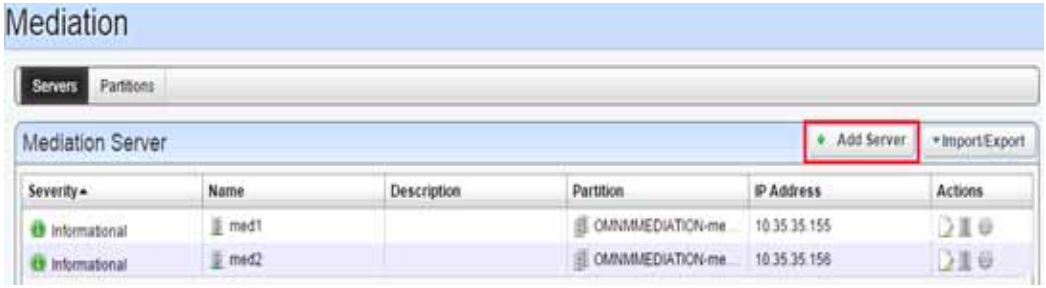


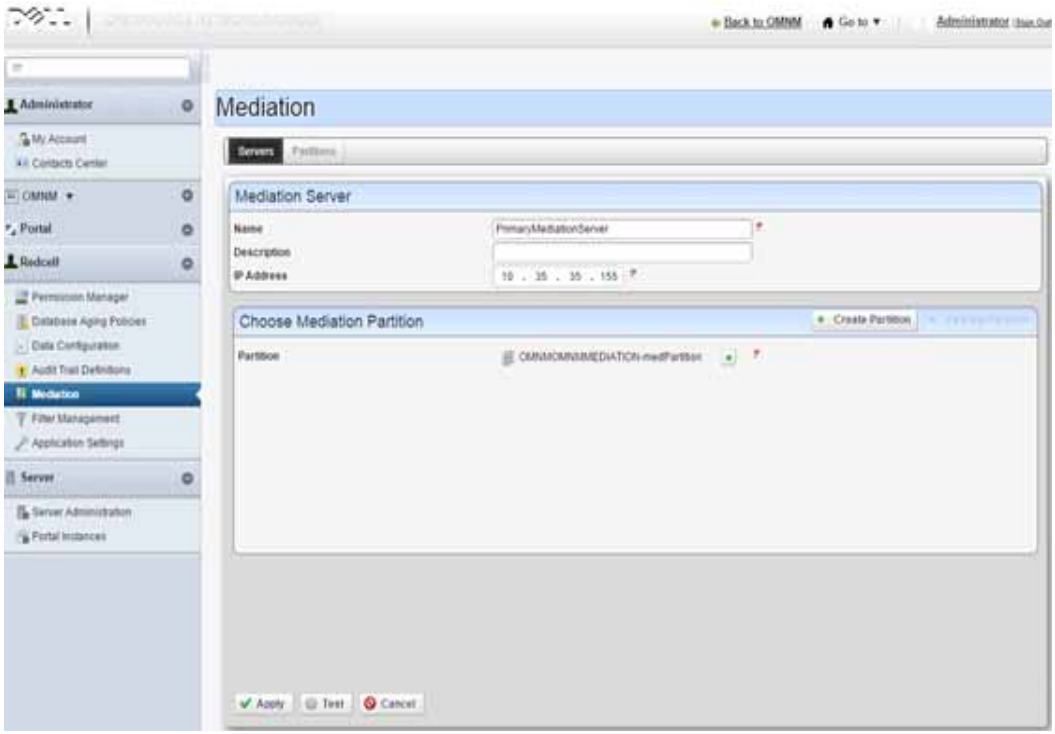
NOTE:

When specifying a mediation partition in Control Panel, add -medPartition at the end of mediation Partition name. For example if you specified your mediation partition as OMNMMEDIATION during installation, when adding partition name to control panel it needs to be OMNMMEDIATION -medPartition.



For testing purpose, add entries for the Primary Mediation server and Secondary Mediation server on the Servers tab select the mediation partition created and click Test. Result will indicate the connection status between the Application servers and the Mediation server. Click Apply to save.





Install on Linux

To run Dell OpenManage Network Manager in Linux, please follow guidelines in **Linux Prerequisites** section before proceed to the installation process. The following steps install the application with the installation wizard on Linux. You can also install with a command line; see Command Line and Silent Installations on page 58 for more about those.

Install Single-Server (Standalone)

This section describes the steps to install Dell OpenManage Network Manager as a Single-Server on Linux. Please review the guidelines in **Best Practices: Linux and Create a User and Prepare for Installation** sections before starting Dell OpenManage Network Manager installer.

Single-Server Installation Screens

The following lists the screens displayed during Dell OpenManage Network Manager Single-Server) installation on Linux:

- **Instruction:** this dialog displays the OMNM version and it also reminds you to shut down other running software (this may include anti-virus software).
- **Software Requirements:** this dialog displays the minimum system requirements and it also provides the link to OMNM user guide.
- **License Agreement:** This dialog displays the Dell Software License Agreement. You must accept the terms of the License Agreement to proceed.
- **Component Summary:** This dialog lists OMNM package and platform versions. It also lists the components version summary.
- **Linux Install Warning:** This dialog reminds you to follow the Linux configuration guidelines lists in the production documentation before installing the application.
- **Choose Install Folder:** This dialog screen lets you select the directory where the application installs. The default directory is /dell/openmanage/networkmanager. If you want to install to a different directory, type the path or click Choose to select another in a directory browser. The installer checks for directory permissions. See Create a User and Prepare for Installation in Linux Prerequisites section for more instructions on how to set permissions on target installation directory.
- **Network Interfaces:** If you are installing the software on a machine with multiple network interface cards, installation prompts you to select one IP address for the system you are installing. Also: Windows 2008 may not support the installer finding the host's IP Address. In such cases, a screen appears where you can enter the IP address and Partition Name for your installation.
- **Choose Install Set:** This dialog lets you select what server(s) to install. The available install sets are Application Server, Mediation Server, Database, and Custom.
- **Choose Link Folder:** This dialog lets you select the Link Folder where startup links reside. Typically this is the installing user's Home.
- **Heap Settings:** This dialog lets you specify memory settings for the server(s) that you are installing. Refer to Memory Tuning (Heap & Portal) in the User Guide for more about setting heap size.
- **Possible Port Conflicts:** This dialog appears when the installer detects port conflicts. This typically occurs when other application(s) reside on the same server is using the port(s).To determine the source of the port conflict and remove the application, please refer to Ports Used section in the User Guide. Best practice is to install on a dedicated server platform.
- **Pre-Installation Summary:** This lists the installation summary. Please review and click Install.

- **Root privileges required:** This dialog requests you to execute the setup.sh script located in the target install directory as root. This script records information in case you need technical assistance and installs some files as root. When you run the setup script, among other things, it automatically re-routes event/alarm traffic from port 162 to port 8162. Open a new shell, log in as root, and run the listed script on the dialog ($OWARE_USER_ROOT/install/root/setup.sh).
- **Install Completed Successfully:** This dialog indicated Del OpenManage Network Manager has been successfully installed. Click Done to finish.

Install Dell OpenManage Network Manager:

Review the guidelines in Best Practices: Linux and Create a User and Prepare for Installation sections before starting Dell OpenManage Network Manager installer.

1 You cannot install as `root` user, so, if necessary, log out as root and login as the user (here, `test`) created in the previous steps and run the installation script:

```
cd /home/test/install_path
./linux_install.sh
```

2 Now follow the instructions in the installation wizard or text, making sure to specify the configured target directory (in this example `/dell/openmanage/networkmanager`) as its installation root.

NOTE:

You may see benign errors during the root potion of the Linux installation. Installation always attempts to find the CW (current working directory). If another process deleted it, an error appears before the script runs. The error is benign and the script still runs, using a temp location controlled by the operating system.

3 When application server and web server have completed their startup, open a browser to this URL: `[application server IP or hostname]:8080`

Single-Server Post Installation

- Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) can have a significantly impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the User Guide for details about tuning these policies.
- After you complete the installation, you may want to install Adobe Acrobat Reader. You can download a free copy from www.adobe.com. This application requires Acrobat to successfully print reports.
- Additional post-Dell OpenManage Network Manager installations can also include Perl and FTP/TFTP servers. See Installing Perl on page 16 and Setting Up FTP / TFTP on page 31.
- See Starting the Application on page 60 for instructions about running what you have just installed.

Install High Availability (HA)

HA Installation Screens

The following lists the screens displayed during Dell OpenManage Network Manager High Availability (HA) installation on Linux:

- **Instruction:** this dialog displays the OMNM version and it also reminds you to shut down other running software (this may include anti-virus software).
- **Software Requirements:** this dialog displays the minimum system requirements and it also provides the link to OMNM user guide.
- **License Agreement:** This dialog displays the Dell Software License Agreement. You must accept the terms of the License Agreement to proceed.
- **Component Summary:** This dialog lists OMNM package and platform versions. It also lists the components version summary.
- **Linux Install Warning:** This dialog reminds you to follow the Linux configuration guidelines lists in the production documentation before installing the application.
- **Choose Install Folder:** This dialog screen lets you select the directory where the application installs. The default directory is /dell/openmanage/networkmanager. If you want to install to a different directory, type the path or click Choose to select another in a directory browser. The installer checks for directory permissions. See Create a User and Prepare for Installation section for more instructions on how to set permissions on target installation directory.
- **Network Interfaces:** If you are installing the software on a machine with multiple network interface cards, installation prompts you to select one IP address for the system you are installing. Also: Windows 2008 may not support the installer finding the host's IP Address. In such cases, a screen appears where you can enter the IP address and Partition Name for your installation.
- **Choose Install Set:** This dialog lets you select what server(s) to install. The available install sets are Application Server, Mediation Server, Database, and Custom.
- **Choose Link Folder:** This dialog lets you select the Link Folder where startup links reside. Typically this is the installing user's Home.
- **Partition Name/Auto Start:** This dialog requests a partition name for application servers in High Availability installation. The partition name for the application servers must be the same. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore. This dialog also provides the option to start the application server on startup.
- **Heap Settings:** This dialog lets you specify memory settings for the server(s) that you are installing. Refer to Memory Tuning (Heap & Portal) in the User Guide for more about setting heap size.
- **Cluster Configuration:** This dialog appearance may vary depending on the type of server you are installing. If you are installing an application server, this dialog requests a Config server IP; typically, this is the IP address of the primary application server that you install for your HA. If you are installing a mediation server, this dialog requests a Config server IP, which is the address of the primary mediation server. Similar to application partition name, the Config server IP entry must be the same for application/mediation servers.

- **Database Selection:** This dialog lets you select the database type for your installation. This will apply necessary client configuration for connectivity to the remote database. You can select either MySQL or Oracle and proceed to the next screen.
- **MySQL Setup:** This dialog appearance may vary depending on previous selections made. If the option selected was Configure Client, then MySQL Setup dialog requests for the IP address and port of an existing MySQL database server where the application servers will point to. If the option selected was Install Server, then MySQL Setup dialog requests for MySQL data path, initial and max size. The default path is /dell/openmanage/networkmanager/oware3rd/mysql. If a Max Size (MB) is specified, capacity will grow as needed up the max size, else capacity will grow as needed unless the disk is full.
- **Oracle Setup:** This dialog requests username, password, host, port, and SID of an existing oracle database server which the application servers will point to.
- **Possible Port Conflicts:** This dialog appears when the installer detects port conflicts. This typically occurs when other application(s) reside on the same server is using the port(s).To determine the source of the port conflict and remove the application, please refer to Ports Used section in the User Guide. Best practice is to install on a dedicated server platform.
- **Pre-Installation Summary:** This lists the installation summary. Please review and click Install.
- **Mediation Partition Name/Auto Start:** This dialog requests a partition name and subnet mask for mediation servers in High Availability installation. The partition name for the mediation servers must be the same. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore. You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask or use unicast to point mediation servers directly to the application servers. This dialog also provides the option to start the mediation server on startup.
- **Application Server Partition Name:** This dialog requests an application server partition name. This name is used by mediation servers for locating an application server on the network and establishing a connection between mediation and application servers. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.
- **Root privileges required:** This dialog requests you to execute the setup.sh script located in the target install directory as root. Log in as root and run the script to proceed with the installation.
- **Install Completed Successfully:** This dialog indicated Dell OpenManage Network Manager has been successfully installed. Click Done to finish.

HA installation outline

1 Install Database servers

2 Install Primary Application + Web Server

3 Install secondary Application + Web server

4 Seed the Database

5 Install Primary Mediation Server

6 Install secondary Mediation server

7 Install License

8 Restart all Servers

9 Add Mediation Domain and Routing Entry

Install Database Severs

Dell OpenManage Network Manager High Availability supports MySQL replication and Oracle RAC database structures. For MySQL Replication and Oracle RAC setup, best practice is to employ a trained DBA to either assist or manage the installation.

If you prefer Oracle as the database type, please follow the guidelines and recommendations in **Oracle Database Management** section for installing and configuring the database.

If you prefer MySQL as database type, OMNM High Availability installer provides the option to install MySQL database on a separate host. Consider the following steps to install MySQL servers (master and slave) as part of your MySQL Replication setup.

Install MySQL as Separate Server

The following steps describe how to install MySQL as separate server:

1 1Follow the guidelines in *Best Practices: Linux and Create a User and Prepare for Installation* sections before starting Dell OpenManage Network Manager Installer. Also review HA Installation Screens section for more details.

2 Log in as a non-root user (see *Create a User and Prepare for installation* sections) and run the installation script

3 Navigate to directory where linux_install.sh script resides and enter the following command to bring up the installation wizard:

```
./linux_install.sh
```

4 Follow the instructions on the installation wizard.

5 Select only **Database** in the **Choose Install Set** dialog. Follow the rest of the instructions on the installation wizard

NOTE:

Once you have completed installation of two MySQL servers using OMNM installation wizard, follow the MySQL guidelines (https://dev.mysql.com/doc/refman/5.1/en/replication.html) to configure your MySQL Replication.

Install Primary Application Server and Web Server

This section describes how to install Application and Web servers on the same host. It is important to follow the guidelines in *Best Practices: Linux and Create a User and Prepare for Installation* sections before starting Dell OpenManage Network Manager Installer. For clarification on the installation screens, please review *HA Installation Screens* section.

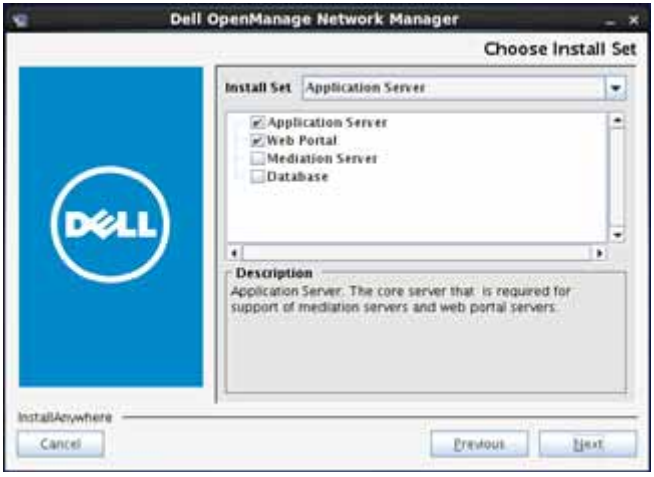
1 Log in as a non-root user (see *Create a User and Prepare for installation* sections) and run the installation script.

Navigate to directory where linux_install.sh script resides and enter the following command to bring up the installation wizard.

```
./linux_install.sh
```

2 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to HA Primary Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select both Application Server and Web Portal check-boxes.



- On the Partition Name/Auto Start dialog, enter a partition name for you application servers. This name must be the same for both primary and secondary server. Partition names

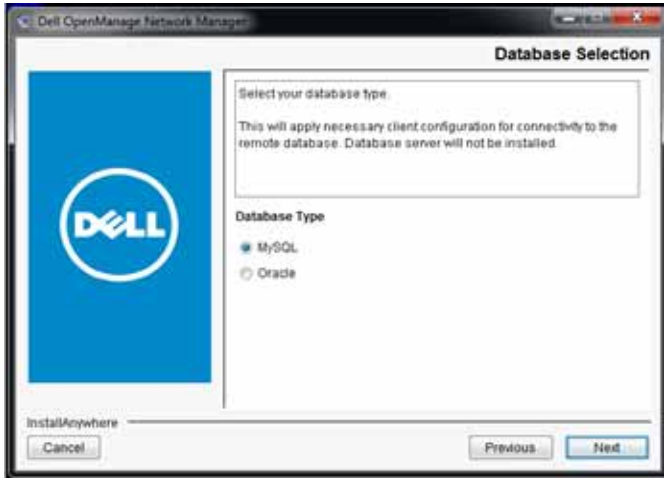
must start with a letter and consist of letters, digits, minus sign and/or underscore. Select Auto Start if you want the server to auto-start on startup.

NOTE:

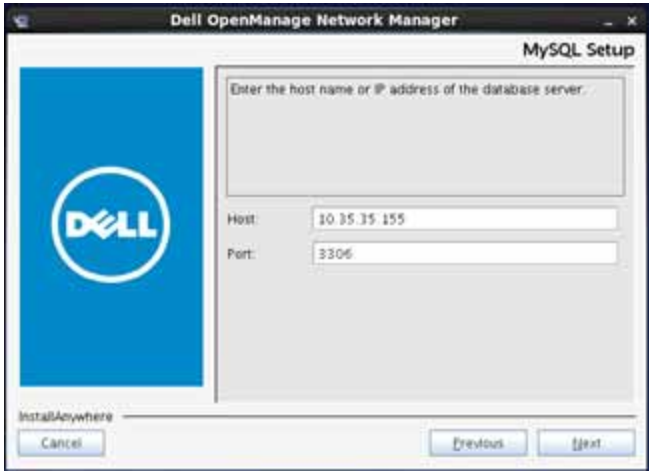
Recommend writing down this partition name for your secondary Application and Web server, and Mediation servers installations.

- On Cluster Configuration dialog, enter a **Config Server IP,** this is typically the address of this primary application server. Again this entry must be the same on both primary and secondary server.

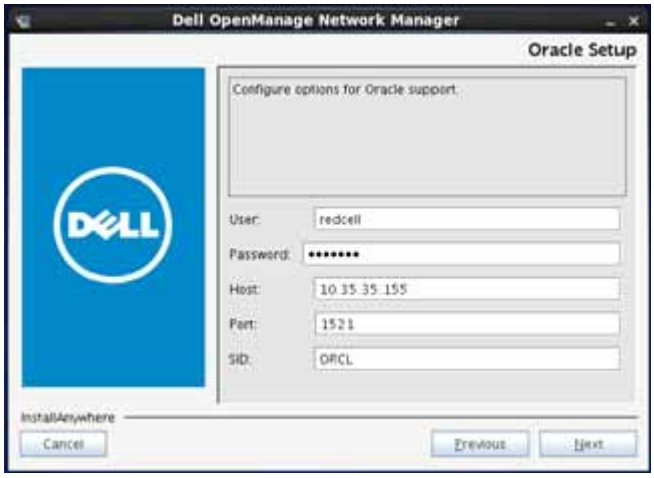
- On Database Selection dialog, select either MySQL or Oracle as database type.



- If you selected MySQL, the MySQL Setup dialog will request either the hostname/IP address and port number of the MySQL database server (See *Install Database Servers* section for database installation) where your application and web server will be pointing to.



- If you selected Oracle, the Oracle Setup dialog requests the credentials of the Oracle RAC.



Install Secondary Application Server and Web Server

This section describes how to install Secondary Application and Web server. Please Review the guidelines in *Best Practices: Linux and Create a User and Prepare for Installation* sections before starting Dell OpenManage Network Manager Installer. For clarification on the installation screens, please review *HA Installation Screens* section.

1 Log in as a non-root user (see *Create a User and Prepare for installation* sections) and run the installation script.

Navigate to directory where linux_install.sh script resides and enter the following command to bring up the installation wizard.

```
./linux_install.sh
```

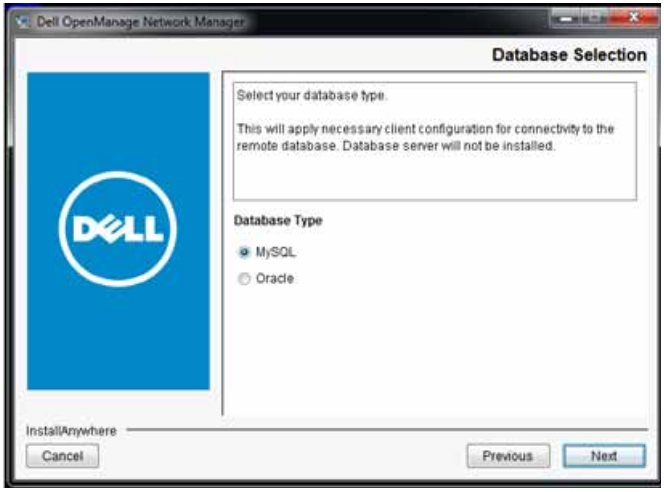
2 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select both Application Server and Web Portal check-boxes.

- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation

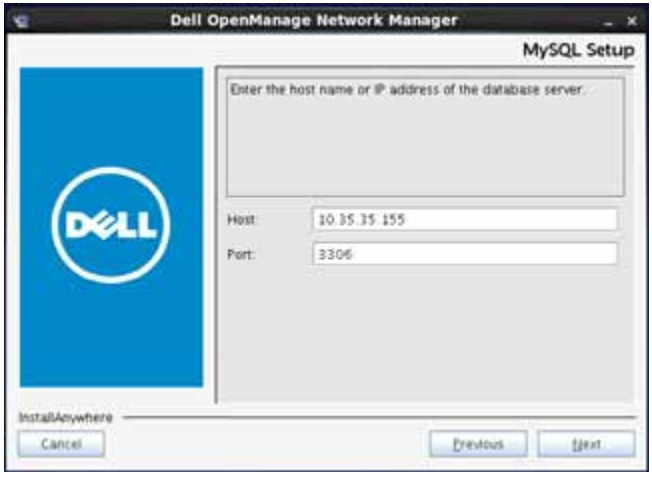
- On Cluster Configuration dialog, enter a **Config Server IP;** this is typically the address of this primary mediation server. Again this entry must be the same on both primary and secondary server.

- On Database Selection dialog, select either MySQL or Oracle as database type. If you selected MySQL as database type for the Primary Application Server, then you must select MySQL as database type for this Secondary Application Server. The same rule applies if you selected Oracle.

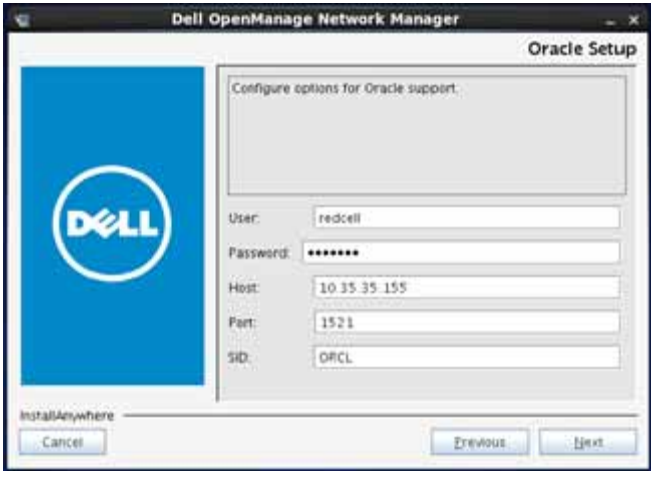


- If you selected MySQL, the MySQL Setup dialog will request either the hostname/IP address and port number of the MySQL database server (See Install Database Servers

section for database installation) where your application and web server will be pointing to.



- If you selected Oracle, the Oracle Setup dialog requests the credentials of the Oracle RAC.



Seed the Database

This section describes the process of creating the database schema and users for the OMNM application. Assuming that you have successfully completed the Application + Web server, MySQL Replication or Oracle RAC installation, please follow this guideline to complete the database seeding.

- If you selected Oracle as database type for this application, please skip the rest of this section and see *Oracle Database Management* chapter for steps to create database schema and user.
- For MySQL, run the following commands on the primary Application server:
  - Log in as `root` user:

    ```
    $ su
    ```
  - `#. /etc/.dsienv`
  - `#service oware stop`
  - `#service synergy stop`
  - `loaddb -u root -w dorado`
  - `loaddb -u root -w dorado -s`
  - `dbpostinstall`
  - `#service oware start`
  - `#service synergy start`

NOTE:

Test database connectivity with the command:

```
pingdb -u root -p dorado
```

The most likely reason that causes the seeding to fail is the invalid configurations in the installdirectory/owareapps/installprops/lib/installed.properties and installdirectory `/oware/synergy/tomcat-7.0.40/webapps/ROOT/WEB-INF/classes/portal-ext.properties.`

A correct configuration in the installed.properties file should have the three lines:

```
…….
com.dorado.bom_dbms.name=mysql
com.dorado.meta_database.name=//ipaddress:3306/owmetadb
com.dorado.jdbc.database_name.mysql=//ipaddress:3306/owbusdb
……..
```

where ipaddress is the address or hostname of the database server.

And in the DATABASE OPTIONS portion of the portal-ext.properties file should list the correct IP address/hostname of the database server.

Install Primary Mediation Server

This section describes how to install Primary Mediation Server. It is important to follow the guidelines in *Best Practices: Linux and Create a User and Prepare for Installation* sections before starting Dell OpenManage Network Manager Installer. For clarification on the installation screens, please review *HA Installation Screens* section.

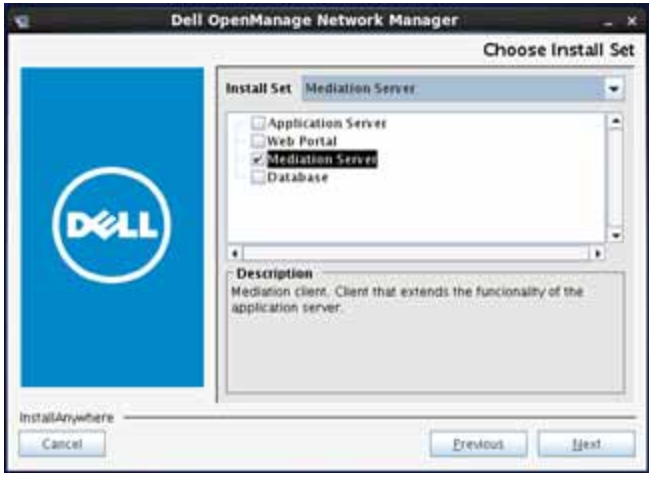
1 Log in as a non-root user (see *Create a User and Prepare for installation* sections) and run the installation script.

Navigate to directory where linux_install.sh script resides and enter the following command to bring up the installation wizard.

```
./linux_install.sh
```

2 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select only Mediation Server checkbox.

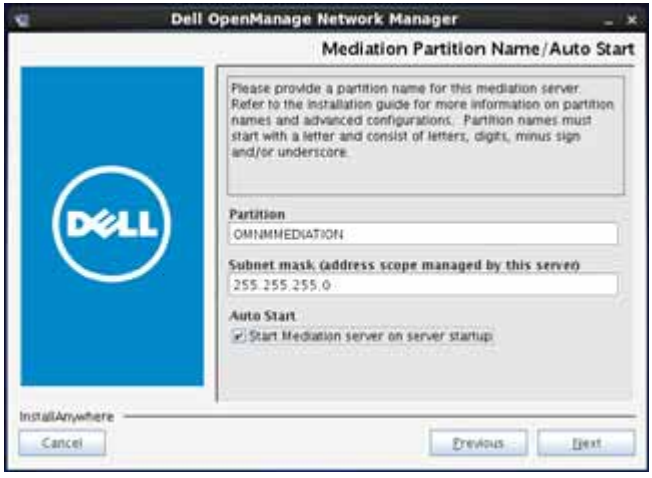


- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation

- On Mediation Partition Name / Auto Start dialog, enter a Mediation Partition Name and Subnet Mask. The partition name must be the same for both primary and secondary mediation server. So whatever name you enter for the partition text field, you must enter

the same name when you install the secondary Mediation server. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.

You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask.



- On Cluster Configuration dialog, enter a **Config Server IP**; this is typically the address of this Primary Mediation server. Again this entry must be the same on both primary and secondary server.

Install Secondary Mediation Servers

This section describes how to install Secondary Mediation Server. Please review the guidelines in *Best Practices: Linux and Create a User and Prepare for Installation* sections before starting Dell OpenManage Network Manager Installer. For clarification on the installation screens, please review *HA Installation Screens* section.

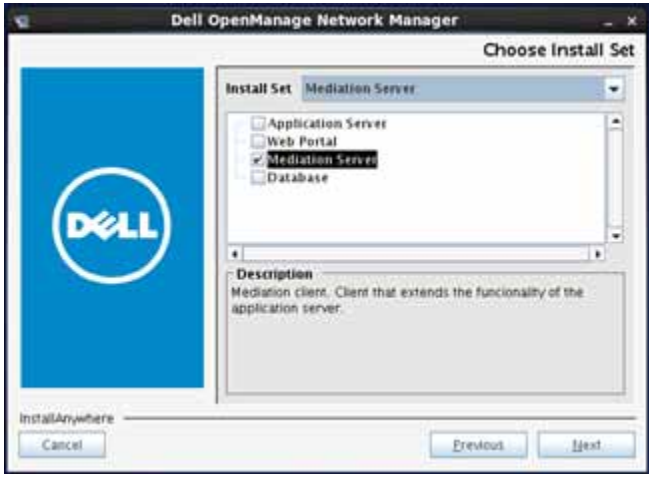
1 Log in as a non-root user (see *Create a User and Prepare for installation* sections) and run the installation script.

Navigate to directory where linux_install.sh script resides and enter the following command to bring up the installation wizard.

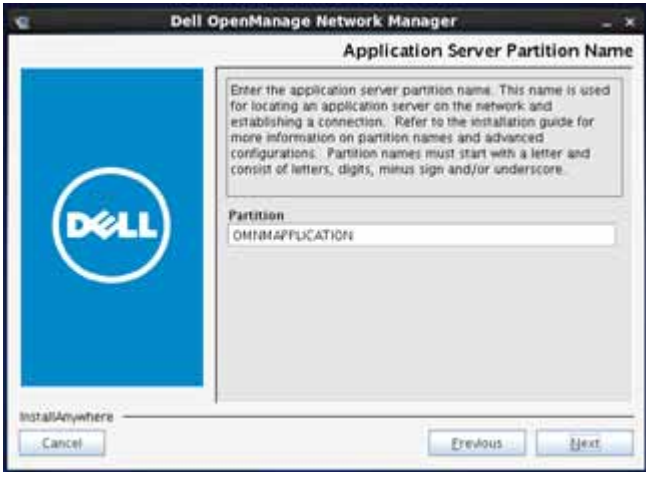
```
./linux_install.sh
```

2 Follow the instructions on the installation wizard. Some required inputs on HA installation dialogs are specific to Application and Web server installation. Please fill in accordingly following these instructions. (See *HA Installation Screens* section for more details.)

- On the Choose Install Set dialog, select only Mediation Server checkbox.

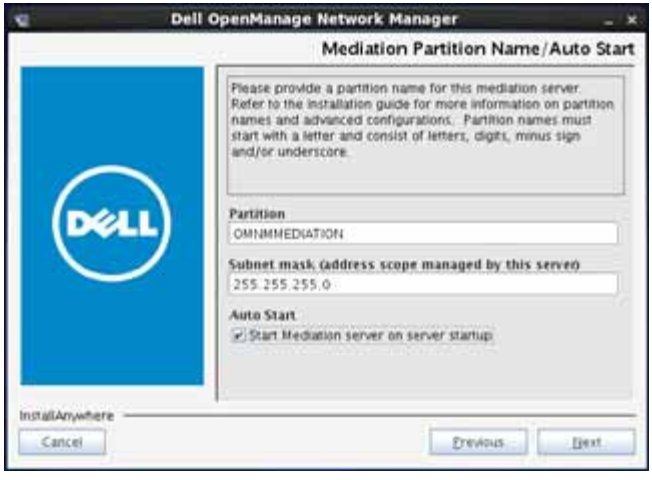


- On the Application Server Partition Name dialog, enter a partition name of the application servers. This is the same partition name that you entered during the Primary Application server installation..



- On Mediation Partition Name / Auto Start dialog, enter a Mediation Partition Name and Subnet Mask. The partition name must be the same for both primary and secondary mediation server. So whatever name you enter for the partition text field, you must enter the same name when you install the secondary Mediation server. Partition names must start with a letter and consist of letters, digits, minus sign and/or underscore.

  You can use the default subnet mask if mediation servers and application servers are all with in the /24 subnet. If they are different, then you must adjust the mediation subnet mask.



- On Cluster Configuration dialog, enter a **Config Server IP**; this is typically the address of the Primary Mediation server. Again this entry must be the same on both primary and secondary server.

Install License

Dell OpenManage Network Manager High Availability requires license to be operational. Pllease see "Installing Licenses" to install HA license.

Restart All Servers

After you have completed the installation of all servers, you must restart all servers in the following order: Primary Application server > Web server (on same host as the Primary) > Secondary Application server > Web server (on same host as the Secondary) > Primary Mediation server > Secondary Mediation server.

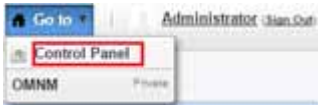
```
Log in as root user,
$ su
#. /etc/.dsienv
To restart Application server:
#service oware stop
#service oware start
To restart Web server:
#service synergy stop
#service synergy start
To restart Mediation server:
#service oware stop
```

```
#service oware start
```

Add Mediation Domain and Routing Entry to Discover Network Devices

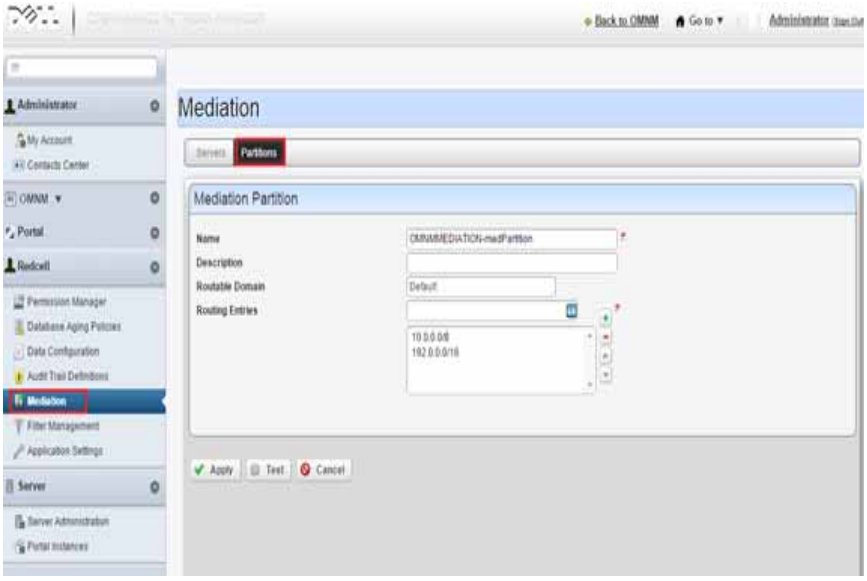
The routing entries determine which devices can use the mediation servers within the mediation domain. For example, you can specify individual subnets-10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16-or just add a 10.0.0.0/8, which covers all the 10.0.0.0 subnet. You can add or delete the routing entries without shutting down web or application servers. The mediation domain requires the -medPartition string appended at the end of the mediation domain name.

To add mediation domain and routing entries in Dell OpenManage Network Manager, go to `Control panel > Mediation > Partitions > Add Partition name and Routing Entries.`

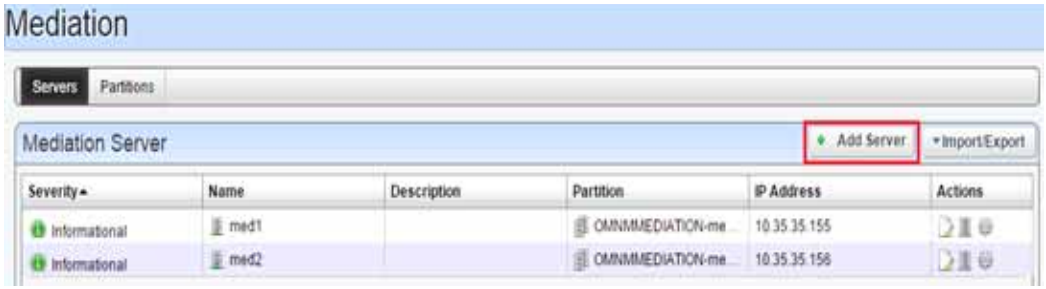


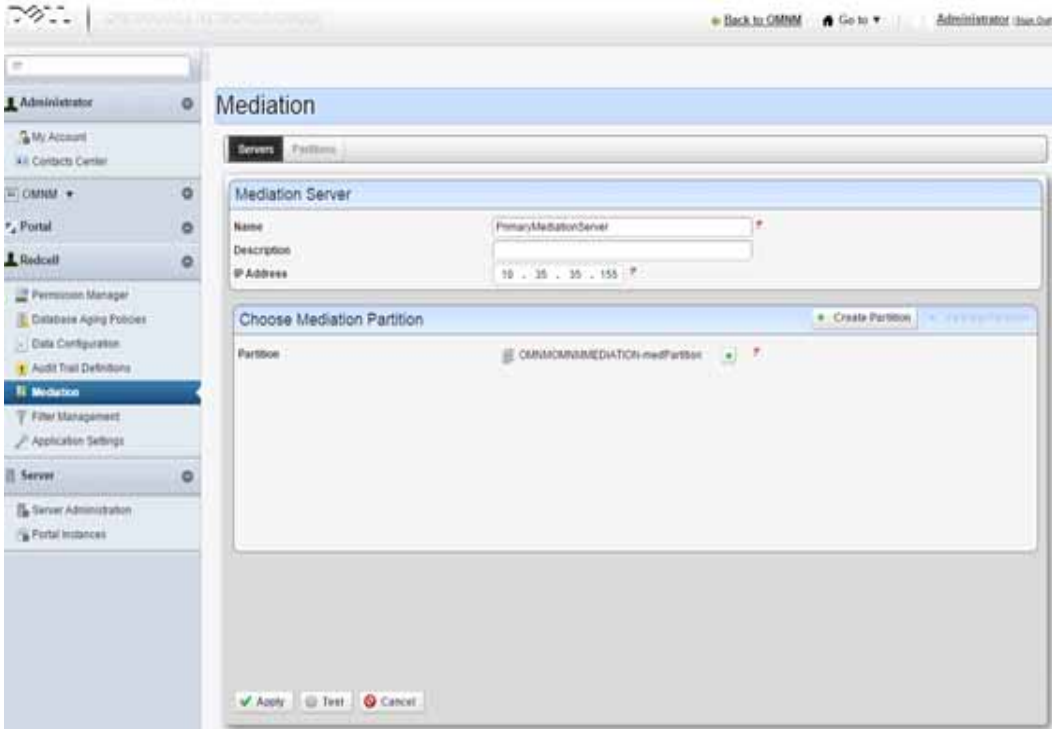
NOTE:

When specifying a mediation partition in Control Panel, add -medPartition at the end of mediation Partition name. For example if you specified your mediation partition as OMNMMEDIATION during installation, when adding partition name to control panel it needs to be OMNMMEDIATION -medPartition.



For testing purpose, add entries for the Primary Mediation server and Secondary Mediation server on the Servers tab select the mediation partition created and click Test. Result will indicate the connection status between the Application servers and the Mediation server. Click Apply to save.





How To:

Command Line and Silent Installations

You can execute the installation in console mode. Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type `back`. You may cancel this installation at any time by typing `quit`.Run one of the following in a shell to initiate console installation:

```
win_install.exe -i console
linux_install.sh -i console
```

These installations provide text alternatives for various features. For example:

```
===============================================================================
Choose Product Features
-----------------------
ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
   LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:
1- [X] Application Server
2- [X] Web Portal
3- [ ] Mediation Server
4- [X] Database
Please choose the Features to be installed by this installer.: 3
```

In such lists, the `[X]` indicates a selected feature. If you enter numbers on the `Please choose` line, this toggles the selection on or off. In the above example, the number 3 has toggled `3` so no `[X]` appears in that line, indicating this installation skips Mediation Server.

Silent Installation

Linux supports silent installation in which installer runs without any user interaction. A near-silent mode is also possible on Windows. Set installer and user-defined variables through a properties/ response file, as described below. You can collect the properties from a installation you wish to recreate.

To run a silent installation, follow these steps:

1. Create a response file—The installer automatically creates a sample properties file during a normal installation. Run installation and look for the file called `sample_installer.properties` in your install location root directory.
2. Execute the silent install—Copy the `sample_installer.properties` to the installer's directory. For example:

```
D:\installer\RCES\7.2\0.111\install\Disk1\InstData.
```

3 Rename `sample_installer.properties` file to just `installer.properties`.

4 To trigger a silent installer from the command line, type the following command:

```
installername -i silent
```

5 The `-i` argument means the installer automatically checks the directory in which it resides in for a file called `installer.properties` or `[installername].properties`.

Alternatively, you may also call a properties file from the command line:

```
installername -f properties file
```

You may use the direct or the relative path to the properties file. If you specify the properties file you must include the following property to trigger silent mode.

```
INSTALLER_UI=silent
```

MySQL Database

After installing a MySQL database to a separate host in console mode, you must run `loaddb`, `loaddb -s`, and then run `ocpinstall -s`, all from the application server installation console.

Installing Licenses

The Application Server, and other optional software, requires licenses. These should be installed by default, but if the license has expired, or if for any other reason your license is not available at startup the Application Server (or other application) shuts down and will not start.

You can install licenses for basic Application Server functionality, and for extended functionality for drivers and applications at any time. You can install these from the *License Management* in the Quick Navigation Portlet in the client. Select the license file in that screen (click the *Select File* button) on any client, and the Application Server stores the permissions to use that functionality in the database.

The license (`license.xml`) is typically in a directory below the installation shortcuts / links. To install the license without the benefit of a client (which does not start without a running Application Server), run the following commands in a shell before starting the server:

Windows

```
>oware
>licenseimporter c:\path\license.xml
```

Linux

```
>. /etc/.dsienv
>licenseimporter c:\path\license.xml
```

NOTE:

Most of the time, you must log out and re-log in for an imported license to take effect. On rare occasions, you must restart application server.

When the `licenseimporter` concludes its work, you should see:

```
importing.....done
```

The `c:\path` portion of this command line is an example. Correct it to wherever you have your license file (by default this is below installation directory on the CD or in `$OWARE_USER_ROOT`).

Starting the Application

In Windows, use the shortcuts in the *Start* button menu to start an Application Server or mediation server, and (after the Application Server has had time to start) the application itself. Right-clicking an Apache icon lets you start and stop the web server.

Start Linux applications after logging out, and logging back in either from the installed icon on the desktop, or from a command line. The following command lines all assume you run `oware` or `. /etc/.dsienv` before running them, to set the environment correctly. The commands:

```
startappserver
startmedserver
```

Both `stopappserver` and `startappserver` scripts may require username / passwords as parameters, if you have an installation that requires a password. To see the syntax of either of these scripts, append -? to them on a command line. Here is the help output from `stopappserver`:

```
~/:stopappserver -?
Usage(1):  stopappserver server_url [-u username] [-p password]
Usage(2):  stopappserver server_url password
example -  stopappserver localhost:1099 -u OWAdmin -p secret
example -  stopappserver localhost:1099 secret
If omitted, username will be assumed to be OWAdmin.
If omitted, password will be assumed to be blank.
If no arguments are provided, server_url will be assumed to be
   localhost:1099.
```

By default, these scripts assume the *OWAdmin* user and a blank password, so if you have changed the default password for OWAdmin, you must pass it to stopappserver.

Starting Linux Installations

The operating system prompts user `redcell` for the root password for the following command lines (no such prompt appears for root user):

Application Server

```
$service oware start
```

Portal Server

```
$service synergy start
```

In /etc/init.d, you can run the following:

```
#./oware start
#./synergy start
```

When you have autostart enabled, to start appserver and process monitor:

```
$startpm &
```

To stop appserver and process monitor

```
$stoppm
```

When process monitor is running, you can check the appserver status

```
$pmgetstatus
```

To stop the application server process only

```
$pmstopall
```

To start the appserver again when process monitor is already running:

```
$pmstartall
```

To open a web client, go to this URL: [host IP address]:8080.

NOTE:

You cannot run a separate mediation server and an Application Server on the same host. If no separate mediation servers are detected, the Application Server will act as a mediation server.

NOTICE

If a mediation server fails to start up with an ENetworkFailure, delete all files in the oware\temp directory manually to successfully start the mediation server.

If either application server or mediation server fails to start, particularly after an interruption in service, like a power failure, delete this directory's contents: oware\jboss*\server\oware\data

Web Services

Newer web services are disabled by default. Enable them by adding this line to $OWARE_USER_ROOT/owareapps/installprops/lib/installed.properties:

```
com.dorado.core.ws.disable=false
```

These are automatically available when dnc.ocp is installed. From version 7.0.0 forward, older non-Axis2 web services are disabled by default too. You can enable them by adding the following to $OWARE_USER_ROOT/owareapps/installprops/lib/installed.properties:

```
com.dorado.legacy.ws.enable=true
```

Disabling older web services enhances performance.

Application Password

The default user (admin) initially has the password admin. Application administrators can reset any passwords in the web portal's control panel Users and Organizations application. The database stores all passwords in encrypted form.

Starting Application Server

If you are installing mediation or Application Server(s), an option appears during installation to configure the server to autostart when the server boots. The final installation screen asks whether you want to start the application server, so you do not need to start the server immediately after installing it.

The startup sequence: Database server starts first, then Application server. Mediation server can start any time before or after this sequence, and waits for application server. See Stopping Servers on page 103 for instructions about stopping Application Server.

You can stop, start and monitor the autostarted Application Server service, with command lines (pmstopall, pmstartall, and pmgetstatus), or use a system tray tool for controlling Application Server in Windows. As always, run oware in Windows, or . /etc/.dsienv in Linux before running the command lines.

For security reasons, pmstopall has a security requirements similar to stopappserver. Here is a sample command line:

```
pmstopall <hostname>:1099 -u <username> -p <password>
```

Both -u and -p are optional parameters. If you omit username, the application assumes OWAdmin is the user. If you omit a password, the application assumes a blank password.

While you can always run the command-line script startappserver, a second Application Server on same ports fails. Also, the Windows *Start Application Server* shortcut does not appear in the *Start* menu when you elect autostart, assuming your installation offers that as an option.

If you select no autostart, then no autostart service installs, and you must manually start the Application Server either from the *Start* menu (in Windows), or from a command line with startappserver. (See Starting the Application on page 92)

If you want to install the service (daemon) after you have already installed the rest of the application, you must run the installprocman script from a command line. See Installing Server Manager on page 95 for details.

Autorun is useful for production server installations. However, if you do not elect this option, then you must manually start the Application Server and mediation server yourself (using the startappserver and startmedagent command lines or the item in the Windows *Start* button menu).

For Oracle/Windows installations with autostart selected for a server, the last step in the installation may prompt you about whether to start process monitor immediately. This potentially lets you defer appserver startup until the next reboot for the sake of Oracle.

NOTE:

Autostart takes some time for the initial load. You cannot see progress for the process unless you tail the server.log file.

Installing Server Manager

The `installprocman` script is in `$OWARE_USER_ROOT/oware/bin`. The script takes several parameters.

Usage:

```
-i       install service"
-r       remove service"
-d       set dependency on MySql service (-i only)"
-n Name  assign a custom display name (-i only)"
```

If you are installing the service on a host which houses both the MySQL database and application server you should execute the script with the -i and -d flags (`installprocman -i -d`).

If you are installing the service on a host which has only application server (MySQL is distributed to another host) the script should be executed with on the -i flag (`installprocman -i`).

The -n flag allows you to define a Custom display name for the service.

Installation of Process Monitor System Tray Icon

To ensure the Process Monitor System Tray icon appears each time the system is restarted simply add the `$OWARE_USER_ROOT/oware/bin/pmtray.exe` binary to the *all users* startup folder (`C:\Documents and Settings\All Users\Start Menu\Programs\Startup`).

Update pmstartup.dat

Finally, modify the `application.server.active=` property in `$OWARE_USER_ROOT/oware/lib/pmstartup.dat` and change the default value from `false` to `true`. Once complete, reboot the system and the application server automatically starts and the system tray icon automatically appears in the user's startup folder.

pmgetstatus

If you elect to autostart your Application Server, you can run the `pmgetstatus` script from a command line to see the status of Application Servers. If you run `oware` first in the shell where you run `pmgetstatus`, this script will automatically be on the path. Here is its usage (produced by typing the script name followed by `-?`):

```
Usage: pmgetstatus [-h <Server IP>] [-p <Server Port>] [-i <Iterations>
```

```
[-r <Refresh Rate>]]
Oware utility for reporting status on managed server processes. By default,
   the local host is queried for 1 iteration.
Options:
    -h <Server IP>      -- Server host IP. Defaults to local host
(127.0.0.1).
    -p <Server Port>    -- Process monitor command port.
                           Default loaded from
c:/work/oware/lib/pmstartup.dat
    -i <Iterations>     -- Number of times to repeat command, -1 is
infinite (requires Ctl-C).
    -r <Refresh Rate>   -- Refresh rate of iterative command in seconds.
Default is 5.
                           Requires -i option.
    -?                  -- Show this help.
```

Windows Server Monitor

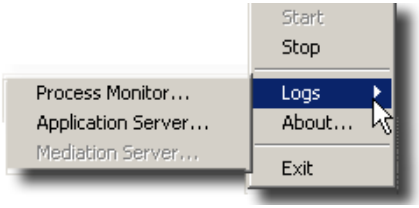
When you install your application as a service on Windows, you also install a server monitor. This monitor is a client to the server manager which controls starting and stopping of an application or mediation server.

Double click the tray icon to display the about panel. *OK* closes this dialog, but maintains the icon in the tray, while *Exit* ends the Server Manager (client and tray icon).

The tray icons themselves indicate the current service condition.

Icon	Status
	Offline (no status available, or not controlled by server manager)
	Running (initializing, or shutting down)
	Ready
	Stopped

You can also right-click the icon to see the client menu.



The logs item let you view logged items for Server Manager, Application Server or mediation server. You can *Start* or *Stop* the service(s) running on your host.

NOTICE

System changes can make the server monitor system tray icon disappear while the process is still running. If you cannot make your icon reappear, try running `pmtray -r` from a command line.

Web Server Parameters

When you install Dell OpenManage Network Manager, installation also includes an Apache Web server. Its monitor appears in the Windows tray, but you can also configure memory parameters for the web server in the `setenv.*` files under `oware/synergy/tomcat*/bin`.

For example:

Linux

```
-Xmx1024m -XX:MaxPermSize=256m
```

Windows

```
set "PORTAL_MAX_MEM=1024"
set "PORTAL_32BIT_MAX_MEM=768"
set "PORTAL_INIT_MEM=128"
```

Set only MAX_MEM and the INIT_MEM. Higher values permit better performance and more users, especially on 64bit machines. Do not change the other settings.

Best practice on a 64bit system: 2048 for the MAX_MEM and 256 for the INIT_MEM. If you have a lot of extra ram then specify more.

Any database parameters for Web server installation refer to the system's existing database.

NOTICE

The web server starts automatically with installation. If it does not, you can right-click the Synergy Network Management icon in Windows and select Start Service, or in Linux type the following in a shell: `/etc/init.d/synergy start` (or `stop`). In Linux systems, `startportal.sh` and `startportal.sh stop` accomplish the same thing, with additional checks.

Startup Properties

The values in `installed.properties` now set most properties for the process monitor to pass when starting a server. All command-line options for the `startappserver` script are now in `installed.properties` (see Overriding Properties on page 105 and Starting the Application on page 92). These are active for each execution of the server (even a mediation server) on the machine where the override exists. Command line arguments override these properties.

The following are properties you can set in `owareapps\installprops\lib\installed.properties` to configure servers:

- Default server partition name also used by client and mediation to locate a server
  `oware.client.partition.name=demo1`
- Default interface used by servers and direct access cut-thru sessions.
  `oware.local.ip.address=192.168.0.10 [for example]`

  The IP address also appears in database connection properties:

  `com.dorado.meta_database.name=//192.168.0.10:3306/owmetadb`

  `com.dorado.jdbc.database_name.mysql=//192.168.0.10:3306/owbusdb`

  To change the IP address, stop the server, set these properties to the new IP address and delete the content of the `oware/temp` directory. Then restart the server.

Web Portal Properties

If you do not use the ipaddresschange script, you will also have to change the IP address for the sake of the web portal. Change this in `portal-ext.properties` in `\oware\synergy\tomcat-7.0.40\webapps\ROOT\WEB-INF\classes`

Change property: `jdbc.default.url=jdbc:mysql://[IP address]/lportal?useUnicode\=true&characterEncoding\=UTF-8&useFastDateParsing\=false`

and

`oware.appserver.ip=[IP address]`

So these reflect the correct IP address, then restart the web service.

ipaddresschange

A simpler alternative to changing properties is to use the `ipaddresschange` script. If you were to install this application on a machine on one network, then move your machine to another network, the IP address from your original network remains hard-coded. You must change the application's IP address to reflect the new network for the software to function correctly. Here is how to do it, once you have connected the application server machine to the new network:

a. First, shut down the Oware Server Manager. Open a command shell (*Start* > *Run* `cmd`, in Windows) then type: `net stop "Oware Server Manager"` (including the quote marks)

a Next, find out what your new IP address is. To do this type `ipconfig` in the command shell you just opened, and make note of the IP Address that appears. You will need that number in a subsequent step.

b Type `oware` at the command line. This sets the environment.

c In the same shell, type `ipaddresschange -n [the IP address discovered in b]`

d Restart Oware Server Manager by typing: `net start "Oware Server Manager"` (including the quote marks). Also restart the web service.

Your machine should then be able to connect to other devices on this network and function correctly.

NOTE:

After the utility is done, if you are using Server Monitor, its Icon in the program tray has an x through it. You must either reboot or use Windows' Administrative facility stop the oware server manager service and restart it. **Also:** In certain packages, you may have to alter the properties mentioned in the Web Portal Properties mentioned above.

- Use only https for web services
  `oware.appserver.web.enable.https=false`
- Set to true when there is no graphics adaptor available for server
  `java.awt.headless=false`
- Primary cluster member (must be running for members to join)
  `oware.config.server=localhost`
- Cluster peer to peer multicast address
  `oware.cluster.multicast.address=226.10.20.30`
- Subnet mask for mediation device coverage
  `oware.mediation.subnet.mask=255.255.255.0`
- To change the default HTTP/HTTPS port numbers for web services, add the following properties to `owareapps/installprops/lib/installed.properties`:
  `oware.appserver.web.http.port=[default port number:80]`
  `oware.appserver.web.https.port=8443`

You may then change the port values for these property entries and restart the Application Server. Special setup (outside the scope of this document) is necessary to run a web server on port numbers lower than 1024 on many operating systems.

CAUTION:
Do not change the system time while the Application Server is running. If you must change the system time, shut down the server before the change, and restart it afterwards.

Proactive Runtime Management

To insure Dell OpenManage Network Manager continues to run smoothly long after you have installed it, best practice is to take the following precautions. For more about this, see Chapter 3, Troubleshooting Your Application.

- Make sure you configure database archiving policies (DAPs) to suit your system, particularly if you have device messaging (typically alarms and syslog) that threaten to fill your database.
- Occasionally check the Audit Trails to ensure DAPs are running properly.
- Configure your syslog and alarm events to only catch significant ones.
- Configure devices to suppress their own messages if these messages are unimportant.

Using Two Interfaces

While installation accommodates selecting between two interfaces, some rare occasions require communicating with both. When that occurs you must add the additional IP address, not selected during installation, to the application server's `tomcat-server.xml` listener so it can communicate with the webserver on the other IP. The following changes make this work:

Add to `/dorado/oware/synergy/conf/server-overrides.properties` on fresh installation:

```
oware.appserver.ip=192.197.95.2
```

(The address above is an example of IP address not selected during installation.)

Add to `/dorado/oware/jboss-5.1/owareconf/tomcat-server.xml` on fresh or update installation:

```
<Connector     scheme="http"
               address="192.197.95.2"
               port="@http.port.num@"
               maxThreads="150"
               minSpareThreads="5"
               maxSpareThreads="75"
               enableLookups="false"
               redirectPort="@https.port.num@"
               acceptCount="100"
```

```
connectionTimeout="20000"
disableUploadTimeout="true"
debug="0"/>
```

Updating an Existing Installation

Always consult the manuals and CD contents for upgrade instructions. Database changes may require a migration step to preserve your data when moving to a new version. A screen appears during this migration that lets you select the path for exported data to be processed. See Chapter 4, Upgrading / Patching from Previous Versions for the full story.

Best practice is to perform a complete backup of your system and database before attempting an upgrade. Provided you are dealing with the embedded MySQL database, some packages installs may prompt you to automatically back up the database. The wizard can also prompt you for a location. The filename is `backup.sql`.

NOTICE

If you are running either MySQL or Oracle as your database on a separate server, you must also run `dbpostinstall` on the (primary) application server before starting your system.

If you do an update installation, even if you elect not to rebuild the database, installation always re-seeds the system settings. If you have changed the default settings, you may want to export these before proceeding.

If you have a previously-installed version of the application on your computer and attempt to run the installation program an update installation dialog appears. It reminds you that setup can update previously installed features and, encourages you to make a database backup as part of the installation.

NOTE:

If you are upgrading File Management, you may have to update configuration file backups. Consult the File Management release notes for instructions about how to do this.

After files install, select whether you want the installation program to rebuild the database content, otherwise, the application keeps the existing one. The installation wizard begins copying the needed files.

If your installation fails, see `setup.log`, `db_setup.log` or `app_setup.log` in the destination directory for the installation for messages that may help fix the failure. (See Chapter 3, Troubleshooting Your Application for more advice about logs).

NOTE:

Servers should not be running during updates and uninstallation. Just before file transfers a screen appears, saying "Checking for active servers." This only checks with the server manager and would not detect a server started manually. If one is running, then you are warned to stop it with an option to test further.

Cancelling the Installation

Once the installer finishes transferring files, the application is installed; you cannot cancel installation. Short of killing the installer process, you cannot cancel database initialization or component installation and seeding. The installer considers this portion of its work system configuration and not application installation so it cannot stop unless you kill the process. If you do manage to abort the install after file transfer completes (after the "creating uninstaller" message goes away), then you must run the uninstaller to remove the software.

CAUTION:

Cancellation is *not* recommended. You may strand processes that you must then manually shut down. Some directories and files would be left behind after the automatic rollback that occurs when cancelling an install.

Uninstalling

You can uninstall the software by using Windows' control panel's *Add/Remove programs* feature (or with `Uninstall Redcell\Uninstall Redcell.exe`), or by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/linux_uninstall
```

or

```
$OWARE_USER_ROOT/_uninst/sol_uninstall.sh
```

or for console mode, run...

```
 OWARE_USER_ROOT/_uninst/linux_uninstall -i console
```

or

```
OWARE_USER_ROOT/_uninst/sol_uninstall.sh -i console
```

NOTE:

If you uninstall in a shell rather than using the graphic uninstaller, uninstaller cannot uninstall its own directory. This produces some errors you can safely ignore in a console uninstallation. Use `cd /opt` and then `rm -rf [installation target directory]` to do final cleanup.

In graphic uninstallation, as in installation, click *Next* to continue through the screens as they appear. One such screen appears listing what you want to uninstall. Confirm that you want to remove all the listed installed components. You can optionally delete all the applications' files and directories (complete removal).

CAUTION:

Uninstallation on MySql servers may delete the database and any application directories. The applications' directories also contains any installed application components and device drivers.

The option to delete directories is primarily to support application developers having to uninstall and re-install the basic application platform without losing component files (like device drivers) on disk that were not part of the installation.

Deletion is recommended, but not required. It removes files created after installation; temp files, database files, cache files, and files extracted from OCP/DDP files. Overall, it is the best way to get a clean uninstallation.

NOTICE

You can back up your `oware/lib/*.properties` files or overrides before uninstalling if you want to preserve them. An alternative is overriding properties See Overriding Properties on page 105 for more information.

When the software has been completely uninstalled on Windows, if prompted, you must reboot your computer to complete deletion of any locked files. Best practice is to reboot right away.

Uninstalling removes all installed files and files created by using the installed system (that it has permission to delete). It does *not* remove directories that were not created by this application's installation or runtime. User-created directories in the product's directory path remain after product removal.

NOTE:

Uninstaller may freeze on hosts with inadequate resources. **Also:** The uninstaller deletes uninstall.exe, if you press the cancel button. After the canceling uninstallation, several directories and files remaining on disk that require manually deletion to completely uninstall.

Stopping Servers

To stop the Application Server, you can either use the Application Server tray icon in Windows (see Starting Application Server on page 94), or stop the server from a command line. The command line to stop a server is `pmstopall`.

If you have not automated server startup, then you can use the `stopappserver` and `stopmedserver` scripts to stop these servers, even remotely. Here is the syntax:

```
stopappserver <hostname>:1099 -u <username> -p <password>
stopmedserver <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

CAUTION:

Using Ctrl+C in the application server shell may stop the application server, but processes can linger which you must stop manually before you can successfully restart application server. One example occurs when the application server shell displays ".... FAILED TO LISTEN ON TRAP PORT 162 .... "during startup. If this occurs, use task manager to stop WMIBeam and WMINotification processes. If such processes do not exist in task manager, reboot before starting application server.

If you have not logged in and changed the password for OWAdmin with the application's login screen the login to stop the server fails. By default, `OWAdmin` and the installing user have the role `OWServerAdmin`. Any user assigned this role can stop the appserver. Blank passwords are valid if they are defined for the user.

If you used `startappserver` (or `startmedserver`) in a shell to start the Application Server (or mediation server), you can stop the server by either interrupting that shell with Ctrl + C or by closing the shell. Ultimately, you can kill the Java processes on your machine to halt a server.

See Updating an Existing Installation on page 101 for additional notes about shutting down processes and services. If you uninstall when a server is active, the uninstallation will attempt to shut it down and failing that will prompt you to shut it down manually.

Linux Command Line Installation

You can run a Linux installation from a command line with text prompts that are equivalent to the graphic interface prompts described in Installing the Application on page 49, and the following pages. Here is the command line to run the text-only installation:

```
linux_install.sh -i console
```

Modified Files

The following system files may be modified during root installation:

```
/etc/.dsienv - installed
/etc/my.cnf - installed
/etc/rc2.d/S75owaredb – installed
/etc/rc2.d/S76oware – installed
```

The rest of the installation installs program files, does the setup functions, and performs the initial database load.

Overriding Properties

Installation typically makes all of the modifications needed to properties files, but if your installation customizes some properties, best practice is not to change default properties, but to override them. This eliminates updates or new installations overwriting property files you have configured. Best practice also includes backing up the override file(s) as described below.

To override a property, put the property itself in `installed.properties` under `owareapps\installprops\lib`. You can override selected (high availability) mediation server properties in `owareapps\installprops\medserver\lib`. Application property values are loaded first and you can override those values here.

NOTE:

Installation updates or refreshes the appropriate properties in installed.properties, but does not overwrite the file. This means property additions you make are safe from installation changing them in this override file. New properties coming from an installation are appended to the files.

The following is an example of property file content to override an application

cache time-out:

```
#==========================================
# Dependencies
#==========================================
product.dependencies=redcell


#==========================================
# Application Overrides
#==========================================
# set event template cache timeout to 1 minute
redcell.assurance.batch.processing.event.template.cache.expiration=60000
```

CAUTION:

If any of the dependency directory names (for example, `owareapps/redcell`) do not exist, then the application does *not* load override file.

Consult the comments in the properties files you are overriding for further information about specific properties.

You can also override properties by renaming the provided file `\oware\synergy\conf\server-overrides.properties.sample` to `server-overrides.properties`, and enable the properties within it by uncommenting them, and altering them to fit your needs. The comments in this file provide more information.

Mediation Server Properties

If you have a single-host installation, the Application Server acts as a mediation server too (and will back up mediation servers by acting as one if a multi-host installation runs out of mediation server resources). If your mediation server is on a separate machine, the `owareapps\installprops\lib\installed.properties` file configures its startup. The same file name in `\owareapps\installprops\medserver\lib` influences failover. Consult the file for more information.

Properties Loading

First the application loads all property files from the application (`/oware/lib`). Then it loads all property files from `owareapps\*\lib` (on the mediation server this is from `owareapps\*\med\lib`). A special property `product.dependencies` that lets you control the order that files are loaded. For example setting `product.dependencies=myApp` makes `owareapps` properties (other than myApp) load after myApp. The product name for this property is the name of the directory under `owareapps`. You can also specify multiple products with a comma (,) delimited list.

Prepend and Append Keywords

One reason to have dependent property loading is to modify a property used by another product. You may need to ensure that your value comes after the other products, or vice versa. When Java reads properties, its default behavior is to override the old value with the new when encountering an identically-named property. This would compel product maintainers to change a product whenever property file changes occurred in the product on which they depend. Such maintenance would increase geometrically, especially with multiple dependencies.

This application supports property appending or prepending through keywords. If you preface the property to be modified with append. or prepend., you can put your own value after or before the original property's value(s). You must be aware of the original property's delimiters and either add one at the beginning of your value if appending, or add one at the end of your value if prepending. For example: Given a pre-existing property: `oware.foo=original`

```
append.oware.foo=,newappend
```

This produces `oware.foo=original,newappend`

```
prepend.oware.foo=newprepend,
```

This produces `oware.foo=newprepend,original`

If the original property is null, the first character (if appending) or last character (if prepending) is stripped (to eliminate the separator) and the property created with the resulting value. Currently, properties permit only one instance of a keyword within a given property file.

Ports Used

This application uses the following ports. Ensure your firewalls or other network security measures do not block these ports.

Port Number	Used by...
1098	Naming service (JNDI)
1099	Naming service (JNDI)
3100	HA Naming Service (JNDI)
3200	HA Naming Service (JNDI RMI)
4444	JRMP invocation (RMI)
4445	Pooled JRMP invocation (RMI)
6500 to 6510	Mediation cut-through
80	HTTP
443	HTTPS
8093	JMS

The client HTTP cut-through goes directly to the device from the client. So, you must get to devices via port 8080 to cut-through to the embedded web server. Telnet cut-through goes directly to the application server as a proxy on ports 6500-6510.

The following ports are seldom required, but are listed here in case present or future functionality requires them:

Port	Used by...
23	Telnet
1103	JNP Discovery
1123	JNP REPLY

Linux Disk Partition Information

Suggested partitioning includes separation into several partitions including /, swap, /usr, /opt, and /export/home.

/ (root)—The root partition contains everything that is not specifically placed on a slice/partition. The rule of thumb here is: Do not put data on this partition that is likely to grow significantly (logs, applications, data, and so on). This partition can be as little as 200MB, however best practice indicates as much as 2GB if space is available.

swap—swap is the space allocated for the operating system to use as part of its virtual memory to augment physical memory. If something in memory has not been used for a while, the operating system will move it to disk temporarily. Recommendations for this are typically for two to three times the physical memory, however we usually determine the amount available based on physical memory. If you have 512MB, specify 1.5-2.0GB. As physical memory increases, still specify 1-2 times the physical memory so you have enough disk space for the operating system. The following are instructions about setting swap:

a. Check your current swap space setting with `swap -l`

e su to root (if not already).

f Issue `mkfile (size required) (filename)`

g Execute `swap -a (pathname)`. this adds the swap file. You *must* use an absolute path name

h Check with `swap -l` to confirm the new swap addition.

/usr—Typically holds operating system commands and utilities related to the operating system. `/usr` can also contain the documentation associated with these commands. This partition should be a minimum of 1.5GB for a full installation. Best practice is to specify 2GB and potentially more if you know you will be adding operating system utilities.

/etc—We recommend this be located on the root partition, not on its own partition. The data here may change from time to time, but the typically does not grow significantly.

/var—Best practice is to create a partition for `/var`. This contains the syslog data, print spool, mail, and so on. This partition could grow significantly from the required amount of disk space depending on the applications running on the system. We recommend you allow at least 2GB.

/opt—The `/opt` partition holds application software that is added to the system. Dell OpenManage Network Manager would be an application that should be installed here. The size of this partition should depend on the required disk space for applications including Dell OpenManage Network Manager. Both the application's software and data reside in the same directory structure, however, so you can add more volumes to another partition.

/export/home—`/export/home` is typically for user data. Most systems have user home drives specified in this space (for example: `/export/home/auser`). This should have enough space for all user data.

/<some_partition_name> —With a RAID configuration, you can specify a large amount of disk space for data purposes.

3

Troubleshooting Your Application

General Troubleshooting

The following describes troubleshooting steps from installation to execution of this application. Installation logs are in the directory `$OWARE_INSTALL_ROOT`. Log files are `setup.log`, `app_setup.log`, and `db_setup.log` (this last log does not appear if you install an Oracle database).

NOTE:

Because this software installs in many different settings, and permits many add-ons and options, not all troubleshooting tips may apply to your installation.

Troubleshooting Prerequisites

Before you begin troubleshooting any serious problem you will need the following:

System details

- Hardware specifics (as applicable)… processor, memory and disk (free space, and so on).
- Operating system and version?
- Dell OpenManage Network Manager version
- Browser and version? Java? Flash?
- Single or distributed installation? Clustered?

Environment details

- How many managed devices?
- Main features used?

Troubleshooting

- Screenshots of errors
- Logs (the `logs.jar` file produced by running `getlogs`)
- A complete description of the problem, and the steps to reproduce, and a complete description of anything already tried that did not work.

Mini Troubleshooting

Suggested mini-troubleshooting steps for a balky application that is already installed and running:

1. Refresh the browser. If that does not work...
2. Clear the browser's cache (Firefox in particular loves persistent old pages), then refresh.

   When you see a difference between direct access behavior between browsers on two different machines, delete temporary internet files. In Windows, open control panel, and open Java. Click the *Settings* button in the *General* panel, and click *Delete Files*. Delete for *Applications and Applets* and *Trace and log files*.

   If that does not work...
3. Stop and start the browser. If that does not work...
4. Stop and start the web server

   For Windows, to start the web server manager: `oware\synergy\tomcat-X.X.X\bin\startsynergy.` For Linux.

   `/etc/init.d/synergy start` or `/etc/init.d/synergy stop`

   Worth noting: The tray icon for the web server () is "optimistic" about both when the web server has completely started and completely stopped. You cannot re-start web server when its Tomcat process still lingers. If you lack patience, kill the (large) Tomcat process then re-start web server. The smaller one is that tray icon.

   If that does not work...
5. Stop and start application server. Command lines for this:

   `stopappserver` and `startappserver`

   If that does not work...
6. Delete the contents of the `oware/temp` directory and restart application server. If that does not work...
7. Reboot the host and re-start the application server, web server and browser.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

`..\oware\jboss-3.0.8\server\oware\log`

`..\oware\temp\soniqmq.log`

`..\app_setup.log`

`..\db_setup.log`

You can also run `getlogs` from a command line.

NOTE:

If you see errors that say your Linux system has too few threads, make sure you have set the file handles correctly.

Troubleshooting Adobe Flash

Installing the latest Flash version is a part of Dell OpenManage Network Manager's requested prerequisites. When Flash is not installed on the browser, things like Visualize My Network, selecting a license file, importing a file, selecting an OS image to import, and so on, do not work. Selection dialogs require installed Flash to select files from the local system. When Flash is not installed, such buttons appear to be active but they do not work.

Database Aging Policies (DAP)

DAP policies automatically purge or archive stale data so the database can maintain its capacity. Several pre-defined and pre-seeded DAPs come with Dell OpenManage Network Manager. You may need to revise these to fit your system. These start at specific times—see the Schedules portlet for specifics about when.

DAPs amount to preventative maintenance since they help to maintain the database's capacity. Best practice is to do the following regularly:

1. In the Audit Trail Manager, create a Filter for Creation Date = prior Month and Action = DAP Executed.
2. Review the records for Status – Failed. These indicate that a DAP job failed. As long as the following DAP jobs execute, no immediate action is required. If any DAPs are repeatedly failing, then consult the troubleshooting document or Dorado Software support.
3. Review the DAP jobs entries and compare to the scheduled DAP start times. Confirm that audit records are displaying a corresponding audit record for each scheduled execution.

Installation Issues

If you are having difficulty installing the application, in addition to the information in the *User Guide* and/or first chapter of the *User Guide*, as well as the following section may help you resolve installation problems.

Best Practices: Pre-Installation Checklist

The following helps you avoid installation problems.

Pre-Installation

- Select devices (IP addresses, or range) and ports to manage. Gather their authentications (login[s]/password[s]). Typically these include both SNMP communities and command line (Telnet/SSH) authentications. Determine what version of SNMP your devices use, too.
- Select a static IP address for your server. When necessary, configure devices' access control lists (ACLs) to admit this application's access / management.
- Verify firewalls have the required open ports between devices and your server. An easy way to confirm whether your firewall is completely configured is to take down the firewall, install the application and interact with the devices, then put the firewall back up. If the application functions while the firewall is down, but does not when it is up, then you have missed some port(s).
- Review your devices' manuals and release notes for any other caveats and instructions about how to configure the device so Dell OpenManage Network Manager at the designated IP address is an authorized management system.

Other Software to Install

- ActivePerl (then reboot your host). This is not necessary for packages 6.1+.
- Latest Adobe Flash player
- Latest Adobe Reader.

You must also have an FTP / TFTP server for production systems. Dell OpenManage Network Manager includes an internal FTP / TFTP server for testing only.

Installation

Installation host—Log in as an administrative user with write access to the installation target directory.

Do *not* log in with user name *admin*, *administrator*, or a name that contains spaces on Windows, or as user *root* on Linux. The installer confirms you are not one of those users. If you attempt this or other prohibited practices, you may see a message like the following: `The installer cannot run on your configuration:`

Windows 2008, 2012 —You must disable User Account Control if installing on Windows Server 2008. Temporarily disable the system firewall or any anti-virus software prior to installing, too. Install this software and the wizard will walk you through initial setup. Dell OpenManage Network Manager installs as a service and starts automatically. Refer to the *User Guide* and release notes for additional setup information.

When installing on Windows 2012, right click `win_install.exe` and select *Properties* > *Compatibility*. Select compatibility mode for Windows 7 /Vista.

Source / Target Directories—The source directory should not be the same as installation target directory

Clocks—Clocks on all hosts where you install must be synchronized.

Starting Dell OpenManage Network Manager (After installation)

Database Running, Connected—Make sure your database is running. MySQL installs automatically as a service (daemon), Oracle must be started separately. Make sure your database connects to the application server if it is on a separate host. Do not install on Linux with MySQL already installed (uninstall any included MySQL first).

Start Application Server—If you installed this software as a service and application server is down, in Windows right-click the server manager icon in the tray, and start application server. Sometimes, this icon may prematurely indicate application server has started. Wait a little, and the application server will catch up to the icon.

When initiated from the tray icon, startup changes its color from red to yellow to green, when complete. Once the icon has turned green, the web client may display the message "The server is currently starting up. This page will refresh when the server has fully started." This message indicates the application server requires extra time to start. When the message does occur connect the web browser again after a few minutes.

Login—Default Dell OpenManage Network Manager login is *admin*, password *admin*.

NOTE:

The first time you start the application after you install it, you may have to wait some additional minutes for Application to completely start. One indication you have started viewing your web client too soon is that it does not display the Quick Navigation portlet correctly. **Workaround**: Force Dell OpenManage Network Manager to re-initialize the admin user. To do that: Login as Admin. Go To > Control Panel > Users and Organizations. Select and edit the Admin user. Edit any field (Middle Name for example). Save. Sign out. Log back in with admin.

For Successful Discovery (After startup) Have the Following:

Connectivity—Ensure application server has connectivity to devices to discover. One easy way to do this is to ping the discovery target from the application server host. Right-clicking a discovered device and selecting *Direct Access* also lets you ping the device to validate your connection.

Backup / Restore / Deploy (After device discovery)

FTP/TFTP Server—Make sure an external FTP/TFTP server / process is running and has network access to the target device(s). Typically FTP/TFTP must be on the same side of firewalls as managed devices. Dell OpenManage Network Manager's internal FTP/TFTP server is for testing only. If FTP and TFTP are separate processes, configure them so they write to the same directory.

Alarms / Monitoring

Minimize Network Traffic—Configure "chatty" devices to quiet down. Use *Suppress Alarms* to keep performance at acceptable levels, and configure database archiving so the database does not fill up.

CAUTION:

Some Dell OpenManage Network Manager features do not work without internet access. In particular: Maps, because the maps Dell OpenManage Network Manager uses need internet access to retrieve maps and plot locations. But if you do not need functioning map portlet(s), then running Dell OpenManage Network Manager without internet access works well as long as the network is properly configured and resolves the *localhost* name to application server's IP address.

Installation File Issues

When installing from a compressed file, file corruption can result from an incomplete file copy, or (FTP) transmission. One symptom of corruption: the file will not unzip. Corruption can also appear when you copy unzipped installation files from Windows to Linux. These can pick up erroneous line feed characters. **Workarounds**:

- FTP installation files from Windows to Linux
- Copy the entire ZIP or compressed file first, then uncompress/unzip it.

Installer Failure

- The installer fails, and you are installing on Windows 2012 (this error appears: `Installer User Interface Mode Not Supported.`
  Workaround: Right-click the `win_install.exe` file, and, in *Properties*, select compatibility mode for Windows 7 or Vista before (re)initiating installation.
- If you created an installation CD from unzipped package:
  -CD formatting limitations can truncate file names to eight characters
  `-Setup.log` complains about the absence of the `owareapps` directory
  -The directory name is truncated to `owareapp` (no "s"), `win_install.exe` becomes `win_inst.exe`

  Workaround: FTP the zipped package. If you are burning an installation CD, use the ISO file, and something like the `mkisofs` utility as the input to the CD-ROM burner.

Additional Windows problems include the following:

- Installer does not provide options to select the desired network interface card / IP address.
  Workaround: Remove the line `InstallMode=Simple` from the `setup.ini` file in the installation source directory. This enables installation in `standard` mode which provides installation options and detection of a second network interface card (NIC).
- Installer fails immediately with error `Create Process failed ==> %1 is not a valid Win64 application.`

Solution: Change the value of the `%TEMP%` environment variable. Change the default value of the `%TEMP%` environment variable to another path you have already configured, for example: `C:\Temp`. Use the Windows System Tools menu to do this.

- The installing user must have write access on target directories where the application is installed.
- The same user who installed the software must initiate any uninstallation. Uninstalling may also encounter locked files and directories. This may leave files and directories behind since locking prevents their deletion. For completeness' sake, recommended practices are manual deletion or the use of an unlocker program. Clean directories are important, particularly if you are uninstalling then re-installing,

Other Installation Issues

You may see messages like `failed to reset password`. The following deals with this and other potential problems:

- Make sure you can resolve the hostname to the correct IP address: `ping -a [IP address]` and `ping [hostname]` and make sure they are in sync.

  If the application becomes unusable after changing the application server IP address (post-install).

  Solution: To change the application server IP address:

1. Shutdown application/web server
2. Open command prompt/shell and source environment. (for Windows: Type `oware`, for Linux: Type `.[space]/etc/.dsienv`, meaning: `. /etc/.dsienv`)
3. Modify `oware.appserver.ip` property in file `[installation root]\oware\synergytomcat-x.x.x/webapps/ROOT/WEB-INF/classes/portal-ext.properties`.
4. Verify the file does not specify the old IP anywhere else. If it does, replace with new IP address and save.
5. Next, modify the IP address in any shortcut URL properties and click OK. `[installation root]\oware\synergy\tomcat-x.x.xx\bin\portal.url` (Web Document tab)
6. Type `ipaddresschange -n <new IP address>` in a command prompt/shell.
7. Restart application and web server.

- Ensure any other of the application's installation(s) have been completely removed, if you have uninstalled a previous version.
- Make sure no other MySQL databases are installed (some Linux packages include them by default).
- You must be user with administrator permissions to install.

Standalone Database Installation Problems

- Errors appear after installing a standalone database, even though its connection has been verified successful using pingdb utility.

  Solution: After setting the environment in a shell (Windows: `oware`, Linux: `. /etc/.dsienv`) Verify the following commands have been run on the application server.

  - `loaddb` (create Dell OpenManage Network Manager database)
  - `loaddb -d` instead of `loaddb` if the tablespace has not been created.
  - `loaddb -s` (create synergy/portal database)
  - dbpostinstall(seed components and resolve database schema changes)

  After confirming the above, start the application server and synergy portal after application server is up/ready.

Install-From Directory

Installation package files must not be in the installation destination directory.

Installer Logs

Installation logs are in `$OWARE_INSTALL_ROOT`. Log files are `setup.log, app_setup.log,` and `db_setup.log` (this last log does not appear if you install an Oracle database). An empty or missing `app_setup.log` means no applications were installed. This can result from a truncated `owareapps` directory name. **Solution:** Correct the directory name and attempt the installation again.

Startup Issues

The following are some possible problems with application startup. Remember: after you first install this application, the application server takes longer to start. Be patient the first time you start the application.

The two most common reasons for the inability to start an application server which worked previously are the following:

Application Server Does Not Start

To find application server issues, search the server log (`\oware\jboss-x.x\server\oware\log\server.log`) file for the word `error`. Review the log for the first error or exception. This is typically the item that needs to be resolved and the most relevant for troubleshooting information.

- Installation checks to confirm your hardware is adequate, but if you are installing to a VM, you can reduce hardware allocations after that installation. If you do that, your application server may not start and will provide no logs. This indicates you may have inadequate

hardware or an inadequate portion of your hardware assigned to the VM running Dell OpenManage Network Manager. If this occurs, check the hardware requirements, and reconfigure your VM, or install on a different machine.

- Check the total system RAM

- Check the appserver heap setting in `/owareapps/installprops/lib/installed.properties`. If it exceeds the total system RAM either you must allocate more RAM or reduce the appserver setting

Application server should never be allocated less than 3G ram, and Web server should never be allocated less than1G RAM.

- The following socket errors (or similar) are reported when starting the application.

```
(Feb 14, 2014 4:57:50 PM) [OWProcessMonitor] ERROR! command socket failure:
   Address already in use: Cannot bind

(Feb 14, 2014 4:57:50 PM) [OWProcessMonitor] re-initializing command
   socket: attempt 1 of 10
```

  This indicates a port conflict is likely preventing your system from functioning properly. This typically occurs when network management or other applications reside on the same server. Determine the source of the port conflict and remove the application. Best practice is to install on a dedicated server platform.

- Port Conflicts, as described in the previous paragraph, can arise after installation. For example if you install other software that uses the SNMP ports (161 and 162), after you have installed Dell OpenManage Network Manager, the installation cannot catch such a conflict. When you try to start it, application server will report it cannot bind to that port, and fail. See the Ports Used section of the *User Guide* for a list of potential conflicts. The `server.log` file lists to such errors when they occur.
- Confirm your license is current and installed. Search the `\oware\jboss-5.1\server\oware\log\server.log` file for `error`, and the license expired error appears.

  To install a license file without a running application server, run the `licenseimporter` script:

```
licenseimporter license.xml
```

  Your license may have a different name, but the script syntax is the same.

Startup issues for Windows installations

If an application or mediation server goes down ungracefully for any reason the JMS message database may be corrupt in `$OWARE_USER_ROOT\oware\jboss*\ server\oware\data`. When it becomes corrupted the application or mediation server cannot start.

Workaround: Delete the content of the `data` directory. This allows application or mediation server startup.

See Linux Issues on page 151 for additional information about troubleshooting Linux.

Initial Logon after installation fails

If, after installation, your attempt to logon to the application fails with message `Connection to server failed` in the Logon window.

Solution: The most likely cause is that the application server is not running. (Re)start it.

The icon in the Windows System Tray or the presence of the `java.exe` process indicates the status of the application server.

If the icon is red or yellow, no client can connect (although some portlets appear without the benefit of application server). If the icon is red, right-click on it and select *Start* from the menu. The icon turns yellow as the application server starts. Wait until the icon is green, and repeat the logon procedure. If this does not work, contact technical support.

Direct Access Fails Because of Java Security Settings

Some Java installations' security settings (in v.1.7+) may block self-signed websites, interfering with Direct Access. The workaround is to provide a security exception for the application server, as follows:

1. Click Start
2. Type configure java and hit [Enter]
3. Select the Security tab.
4. Click Edit Site List
5. Click Add
6. Type the Dell OpenManage Network Manager URL (example: `http://192.168.0.51:8080/`. Best practice is to use the IP address of the application server, not `localhost` or `127.0.0.1`)
7. Click OK and Continue.
8. Apply this change, and/or click OK.

Logon Fails with Invalid Logon Message

When you enter your User Id and Password in logon dialog and click Logon, an Invalid Logon message appears.

Solution: Ensure you are entering the correct User Id and Password and click Logon. If you have forgotten the User Id or the Password, or if another user has changed the Password for the User Id, you may have to re-install the software.

Logon form missing/Gray screen

Problem: Missing login form - receive gray screen only

Solution:

1. In a command shell type the following: oware.

2 Then type loaddb -l. This drops synergy and lportal database tables.

3 Type `loaddb -s .` This creates synergy and lportal tables.

4 Restart application server.

5 Restart web service. Note: you may have to wait as much as five minutes before logging in the first time.

Mediation Server on separate machine fails

Distributed mediation server failures to start can occur when multicast is disabled on your network. The workaround is to this property in
`owareapps\installprops\lib\installed.properties`

```
oware.application.servers= [application server IP address]
```

Correct this on all mediation server machines.

Unsynchronized Clocks in Clustered Installations

All machines in a cluster, or distributed system, must have synchronized system clocks. If this is not true, systems may start, but will not work correctly.

Other Failures on Startup

- Another instance of appserver/medserver may be running on one host. Common error contents:

```
2005-06-25 08:47:51,968 ERROR [org.jboss.web.WebService] Starting
failed

java.net.BindException: Address already in use: JVM_Bind

at java.net.PlainSocketImpl.socketBind(Native Method)
```

Solution: Stop and if necessary restart application server(s).

Starting and Stopping Servers

Best practice in Windows installations is to start or stop application server with the process monitor icon (installed by the application), when it is installed as a service. Stopping, starting or restarting the service through operating system's Service Manager is not recommended. If the status icon in the tray is green and you restart procman ("process manager") from Windows' Control Panel services, an error message appears saying the service did not stop properly. The tray icon then turns white. Since the application server is still running, when you try to restart the service again, the icon turns red.

To restore the Process monitor icon to function correctly and show status, stop all Java and WMI processes in the process manager. A system reboot also re-initializes the OWProcMan (process monitor). Note that the service name may be different if your package has been specifically branded. The executable path for the service is `\....\oware\bin\owprocman.exe`.

More Failures on Startup

- Failure to connect with a database can occur when...
  - –The Oracle instance not running
  - –Oracle or separate MySQL lacks connectivity. Use `pingdb -u <user> -p <password>` to check. Default user/password for MySQL: root/dorado
  - –Oracle database is not built, or you have not completed its installation
  - –MySQL not running (it should start automatically)
  - –Your firewall blocks ports the database needs.
  - –You see `ERROR...java.lang.OutOfMemoryError` in the log file. Consult the *User Guide* for advice about memory settings and hardware requirements.

  One Solution:

  The following may solve database connection issues and/or failure to see a login screen in web client:

  1. In a command shell type the following: `oware`
  2. Then type `loaddb -l`. This drops synergy and lportal database tables
  3. Type `loaddb -s` . This creates synergy and lportal tables.
  4. Restart application server.
  5. Restart web service. Note: you may have to wait as much as five minutes before logging in the first time.
- Changed properties files
  - –Delete the contents of `oware\temp`
- Connection to application server fails
  - –Application server has not fully started. Look for `>>>>> Oware Application Server initialization COMPLETE. <<<<<` in the `server.log`

Login Failures

- Invalid Logon
  - –Incorrect log in ID or password (the default for web client is User *admin*, password *admin*)
  - –User has changed and forgotten password
- Account is inactive
  - –Application Security Policy may be configured so passwords or accounts have an expiration date.
  - –Use different account.
- Memory errors that indicate too little memory on the application server can also prevent login.

Multi-NIC Host Fails to return to the portal—When you click the *Return to* ... link from Control panel, some unexpected URL appears in the browser. To see the root of this problem, go to *Portal* > *Portal Settings* and compare the *Virtual Host* entry to the application server's IP address. If they are different, then DNS has two different IP addresses associated with the same hostname. Dell OpenManage Network Manager needs an unambiguous IP address and associated hostname for both application server and client.

Workaround(s): 1. Use a local host file and map the IP selected during installation to the hostname. 2. Set the DNS server to only resolve the selected IP address to this machine's hostname.

- Installer fails immediately with error `Create Process failed ==> %1 is not a valid Win64 application.`
  Solution: Change the value of the `%TEMP%` environment variable. Change the default value of the `%TEMP%` environment variable to another path you have already configured, for example: `C:\Temp`. Use the Windows System Tools menu to do this.

Troubleshooting Flow

As part of the troubleshooting process, you can often determine the culprit for problems by a process of elimination. The following questions may help determine what is the real issue:

Discovery / Resync

See Communication Problems on page 125, Preventing Discovery Problems on page 125 and Discovery Issues on page 126

- Can you ping the device you are having difficulty discovering? If you can ping them, and have discovered them, but ping still does not work from within the application, do the devices have an ICMP management interface when you right-click > *Edit* them? If not, add the interface and resync.
- Is your system permitted access to the device (on the Access Control List)?
- Are firewalls blocking access to the device(s)?

NOTICE

The command `service iptables stop` turns off the Linux firewall. Turning it off temporarily is recommended when you first install.

- Is any other software on the application server / mediation server host causing a port conflict? (Uninstall it)
- Is SNMP is configured on the target device and read/trap, write community strings? Is SNMP correctly set up? (check with Network Tools and MIB browser or a tool like iReasoning's MIB browser)

- Is Telnet or SSH configured on the target device and can you Telnet / SSH to the device through a command line shell or an application like puTTY?

NOTE:

Some devices support only SSH v2. Consult release notes for specifics.

- Are authentications created in the Authentication portlet with protocols and passwords set correctly, with adequate timeout and retries configured for your network's latency?
- Are Discovery Profiles using the created authentications?

Backup / Restore / Deploy

See Backup / Restore / Deploy on page 128

- Is your FTP server installed, up and running?
- Is that FTP server on the same side of the firewall as the devices it addresses?
- Does the device support the type of backup (FTP, SFTP, TFTP) you are attempting?
- Do your authentications grant privileged access? The prompt is typically #, not > at this level of access.
- If the device does not successfully execute the command, then either the authentication you have used does not have permission to do such commands, or the device is configured to prohibit their execution.
- Do FTP and TFTP servers write to the same directory, and have permissions to read/write/execute to that directory?

Alarms / Monitors / Performance

Consult the *User Guide*'s recommendations, particularly for Monitoring and for Traffic Flow Analysis. See also Alarm / Performance / Retention on page 129.

- Do you have the recommended hardware to handle the number of devices you are managing?
- Are the devices you are monitoring sending only the relevant traps to your system?
- Is your database configured correctly for the expected load? Symptoms of database configuration inadequacies include slow performance when expanding the Resources portlet or right clicking on a port of a device and selecting show performance. This can also occur if your database size has increased significantly since implementation.

  Solution: For MySQL, adjust/increase the innodb_buffer_pool_size to restore performance. Consult the *User Guide* for more about performance tuning such parameters in MySQL.

  NOTICE

  The internal event `emsDBCapacity` notifies you about how much of the database you have used.

- Have you tailored your monitoring to the available capacity of your hardware? Monitoring or other functionality dependant on writing to the database may stop with error specifying

  ```
  Could not get a database connection
  ```

One example of an error that appears when an active monitor which is suddenly unable to insert data into the database

```
2014-04-10 11:14:47,376 490736076 ERROR
   [com.dorado.broadscope.polling.PollingResultsDAOImpl]
   (WorkerThread#8[71.192.23.246:58220]:) persistsPollingResults failed.
   Rolling back.

com.rendion.ajl.CheckedExceptionWrapper: Could not get a database
   connection.
```

Solution: If the database can be reached over the network and has been confirmed operational/healthy, the configured pool allocation(s) may be exhausted. Refer to the first chapter of the *User Guide* and confirm sufficient pool allocations have been configured for corepool, jobpool, and userpool.

The first chapter of the *User Guide*'s Clustering chapter contains suggestions for properly sizing pool values based on the number of servers in your environment. Based on this information and your current configuration, increase pool values accordingly.

- To isolate the source of performance difficulties, does un-registering Traffic Flow exporters, or turning off monitors have an impact?

Hardware

See Environment / Operating System Issues on page 171.

- Does your hardware match the system recommendations for the number of devices managed, monitoring and concurrent users?
- Have you followed the installation recommendations (particularly important for Linux) in the *User Guide* and first chapter of the *User Guide*?

Advanced Troubleshooting

If you remain unable to resolve issues with your system, the following may be helpful.

- When you contact technical support, create a `logs.jar` file with the `getlogs` command, so you can forward it to them.
- You can change the messages your system generates. That may be necessary. See Debug on page 136.

This chapter contains more troubleshooting advice like WMI Troubleshooting Procedures on page 140, and Linux syslog not displaying on page 161 (setting up devices for various vendors).

Upgrade / Data Migration Fails

I. Unexpected Database Behavior after Upgrade: If you observe unexpected behavior after an application upgrade, review installation logs. Confirm evidence appears that the upgrade executed `dbevolve`. If not...

Solution: Execute the following steps

1 Shut down the application.

2 Open a shell/command prompt on (the primary) application server.

3 Execute command dbpostinstall.

   This step resolves potential database changes between application versions. You must run the command for both MySql and Oracle database environments too.

II. Upgrade Fails with Database Connection Failure: If an upgrade installation fails with the message with the `app_setup.log` error `Connecting to database...>>>>> ERROR: OWSessionIDRDBMS : Failed to make database connection`, the problem is that the database is not running on the host being upgraded. To cure this problem, manually start the database, and then re-try the upgrade installation. The following are the startup commands for the embedded database:

Windows:

```
net start mysql
```

You should see the following response in the shell where you execute this command:

```
The MySQL service was started successfully.
```

NOTICE

If you substitute the word `stop` for `start` in the above, these commands manually stop the database.

Versions

Before you begin more in-depth troubleshooting, you may need to know what versions of various components are installed to ensure they are compatible. To see these before installing, consult the `version.txt` file in the installation source's root directory, or after the application is running, view its *Manage* > *Show Versions* screen. Differences between `version.txt` and *Show Versions* may occur when you install additional applications or patches.

Another way to see the versions for currently installed modules: open a shell (*Start* > *Run* `cmd` in Windows, for example), and type `oware` (`. /etc/.dsienv` in Linux) and [Enter]. Then type `showversions`. The currently installed modules and their versions appear in the shell. You can also use the *Manage* > *Show Versions* menu in web client to find this information.

Search Indexes

Sometimes this software may display Control Panel objects like Users, Roles, and Organizations inaccurately. This occurs because Search Indexes need to be re-indexed every so often, especially when changes to Roles, Users and Organizations are frequent.

To re-index go to Control Panel > Server Administration and then click on the *Reindex all search indexes*. Reindexing is not instantaneous; expect this to take some time.

Communication Problems

Firewalls may interfere with necessary communication between elements within or monitored by your system. Best practice when installing is to bring the firewall down, install, then once you have confirmed the installation runs, bring the firewall up with the appropriate ports open. (See Resolving Port Conflicts on page 138, also see the Ports Used section of the *User Guide*.

Managed devices often have Access Control Lists (ACLs) for management traffic. Best practice is to use a management VLAN or subnet. Note also that in-path devices may filter management traffic creating an obstacle to management messages. Overlapping address spaces may also complicate network management. Identifying such "DMZs" and overlaps is part of network analysis.

Preventing Discovery Problems

Ensure your firewall is not blocking network access to equipment you are trying to discover. The following describes more preventive practices to do when you discover a mixed vendor / mixed class network.

ICMP (Ping)

You can ping devices from a shell or the Network Tools portlet to insure it's up and online.

Telnet / SSH

1 Manually telnet or SSH connect to a device to verify that you have the correct authentication information (although Discovery Profiles' *Inspect* function does this too).

NOTICE

Later versions of Windows do not include telnet by default. In addition to free telnet programs you can download and install, like PuTTY, you can open a shell (*Start* > *Run* `cmd`) and type `oware` to get telnet capabilities. **Also:** Use SSH v2 for Dell devices.

2 If you know the device, look at its configuration file and verify that the SNMP community string is correct.

3 Discover the device.

4 If there are any problems with any devices, then ping them, and/or telnet to problem devices and verify that telnet works / authentication is good.

5 If SNMP problems arise, use this application's MIB browser tool to troubleshoot them.

To verify SNMP and WMI connections are working between your system and the devices in the network, use the following tools:

SNMP

1 Open MIB Browser in the web client's Network Tools portlet, or by right-clicking the device.

2 Select RFC1213, system, from the RFC Standard Mibs branch

3 If necessary, fill out the Authentication tab

4 Select the device tab and information will populate as soon as the query is answered.

WMI

If you are discovering WMI systems on your network, the following may be helpful.

1 Launch the `wmiutil.exe` command line tool from `\owareapps\wmi\bin\"`

2 You need to supply a user and a password along with an IP or hostname

Typing `wmiutil.exe` with no arguments returns launch the WMIUtil User Interface.

```
c:\Dorado\owareapps\wmi\bin\wmiutil.exe -user <user> -password
<password> -host <IP or Hostname>
```

Typing `wmiutil.exe ?` at a command line returns what parameters are available for the command line version.

NOTE:

Even if you do not need a domain to log into your WMI device, the graphic interface for this utility does not work if the domain field is blank. Any content makes it work correctly.

See WMI Troubleshooting Procedures on page 140 and Additional WMI Troubleshooting on page 149 for additional details.

Discovery Issues

Discovery may fail if its authentication or network parameters do not match the configuration of devices discovered. Here, the results panel typically displays a message like `No Devices were detected with selected Discovery Parameters`. Use the *Inspect* function in Discovery Profiles to validate credentials entered.

Some additional sources of Discovery issues, and their solutions:

- Equipment with management IP Addresses in the selected subnet, range, and so on does not exist. Correct the selected range and retry.
- The equipment in the selected range has already been discovered.
  Managed devices can only be discovered once. Those devices that have already been discovered appear in the Discovery Results section of the Discovery Wizard. Update the state of previously discovered devices by selecting *Resync* from the right-click menu. If you want to re-discover these devices, delete them from the Managed Resources portlet
- The SNMP community strings / authentication on the equipment do not match the default values used by this application. Correct the SNMP authentication selected for discovery.
- Discovery finds a device, but features like Direct Access, Backup and Actions do not work.

Solution: The device likely has a correct SNMP authentication, but an incorrect CLI (Telnet / SSH) authentication. Either re-run the Discovery Profile after deleting the device and correcting the authentications, or right-click to edit the device and add the CLI authentication and management interface, then right-click to resync the device.

Note that you must log into the device as a user with enough permissions to accomplish all discovery and other tasks. If you log in as a user with limited permissions, then discovery results reflect those limits.

NOTICE

The *Inspect* feature of the Discovery wizard lets you validate authentications.

Alternative: The device is not supported by your current license or driver set. To request support, use the MIB browser to navigate to RCC1213 ifTable details, and export / save this branch. Navigate to ENTITY-MIB entPhysicalTable details and export / save this branch. Attach the exported files to e-mail to support, or to a trouble ticket.

The following describe additional discovery issues.

HTTP Authentication

Often, an HTTP session with devices that support it exchanges data with the device after discovery. This process fails if the HTTP Authentication information is incorrect. Create HTTP authentications that match your devices' in the Authentications portlet and use it in discovery.

Device O/S Overrides

The device driver installed must support the Operation System version on that device. Verify the equipment's firmware and operating systems are among those supported. Supported firmware and operating systems appear listed in the release notes, or in *Manage* > *Show Versions*.

Example: Override driver-unsupported operating systems for the Juniper devices in `/owareapps/juniper/lib/juniper.properties.` Change `com.dorado.juniper.supported.OS.dc.default.max`

This revision does not support new features. Other device drivers have similar override mechanisms.

If devices appear in Managed Resources as Discovered Entities, rather than specific vendors' devices. This can mean the following:

- The equipment's driver is not installed.
- The driver installed but not seeded to database. `Workaround:` Run `ocpinstall -s` on a command line.
- Monitored devices must be configured to connect and send SNMP traps to the element management system.

If your system discovers only top level equipment, this can mean the following:

- Devices do not have components (interfaces, ports, and so on).
- An incorrect telnet / SSH authentication can have an incorrect password or no enable password. **Workaround:** You can right-click and edit the equipment with this problem to add the telnet / SSH authentication. Make sure you also add a management interface, then resync the device.

Backup / Restore / Deploy

Failures of backup/restore capabilities often stem from failures in the external FTP/TFTP server. This means the FTP / TFTP server is offline, blocked by a firewall or incorrectly configured. Check in the File Server Manager to correct this. Also, on such servers, FTP and TFTP server must share a directory, and the directory must have all permissions to permit these servers to write, read and delete temporary files.

If deploying firmware fails with the following symptoms:

- Selecting *Deploy* does nothing.
- The FTP/TFTP File Server status is Disabled.
  Workaround: Back up the device first to validate it is connected with the FTP server.

When you use the file backup (NetConfig) option, the internal FTP/TFTP server is provided for testing, not production; do not use it. External FTP servers are essential for performance reasons, and, if necessary, the network equipment using FTP to send/receive configuration files must have FTP enabled.

NOTE:

If you have separate FTP and TFTP servers, they must read/write to the same directory.

Timeout

Timeout can occur when backing up / restoring large config files.

Workaround: Change timeout values in the telnet/SSH authentication object. Right-click > Edit the device and change those values in the Authentication tab. Typically this means doubling the timeout, and increasing retries to 2 - 3 times.

NOTE:

Secure FTP connections (scp/sftp) often require SSH services be enabled on the devices addressed. Ensure your system's server and sftp/scp file server can access the devices with SSH too.

Group File Management Failure

If group file management backup operations fail for some devices while individual backups to these devices are successful, typically thread pool-related backup errors appear in logs during the related time frame.

Solution: Your system may have insufficient threads available to handle the number of concurrent tasks required by the group backup operation. Some threads could have already been in use for other tasks when the group operation began.

To address this, increase the size of the thread pool to handle additional concurrent tasks with the following steps:

1 Shutdown application.

2 Edit `owareapps/installprops/lib/installed.properties`

3 Add the following property...

```
ProvisionThreadPoolMBean.PoolSize=70
```

(Adjust as needed based on current setting and need.)

4 Save `installed.properties`.

5 Start application.

6 Execute the group backup operation.

By increasing the Pool Size, the application can perform additional concurrent tasks that fall within the scope of this pool.

Alarm / Performance / Retention

If you install your system to monitor alarms, and experience sluggish performance or a rapidly filling database, several remedies are available.

- Configure “chatty” devices emitting many alarms to stop doing so.
- Configure your system’s Suppress Alarms feature to keep performance the database’s capacity at acceptable levels
- Reconfigure your system’s database archiving policy feature to archive alarms more often so the database does not fill up.

Retention Policies

Retention policies tune how long your system retains data. These policies also have built-in limits (raw, hourly, daily) that help to avoid potential performance/storage problems. The potential impact when going outside these thresholds is significant and generally not recommended.

Configure retention policies with the following limits in mind:

- Maximum # of days to retain daily data: 180
- Maximum # of days to retain hourly data: 14
- Maximum # of days to retain raw data: 1

Network Monitoring

You can monitor your network’s performance two ways.

- Scheduled polling-based monitoring is more reliable, and specific. It also has a lower impact on network. It may, however, lag behind network events.
- Event-based monitoring (typically Traffic Flow Analysis, syslog and SNMP) is more up-to-date, but, can be less reliable. It also often does not disclose the root cause of a problem.
- This software does not support Traffic flow analysis on sFlows from devices using sFlow earlier than v5. Typical error content reads “Data array too short” if you have an unsupported sFlow version.
- Traffic Flow Analyzer support in Dell OpenManage Network Manager collects and process flows with source and destination IP address. Switches or devices that only support L2 flow payloads with MAC address as the source and destination payload are not currently supported. Example: Juniper XE devices.

NOTE:

Typical packages come with a default limit to the number of monitored devices. Upgrade your license if you want to exceed the package limit. Because of the performance demands they make, Traffic Flow exporters are licensed separately from the managed resource license count, so a license to manage 50 devices does not necessarily let you have 50 Traffic flow exporters.

Also: The application discards IP v6 flow packets.

NOTICE

Does Traffic flow not appear when it’s expected? Have you made sure the device is registered to display traffic flow (right-click in resources *Traffic Analyzer* > *Register*)?

- Each monitor should have 10,000 or fewer targets. Use a new monitor to track any targets exceeding that number. The general best practice is to have fewer targets distributed across several monitors.

Using this software’s features, you can create alarms and reports for each. Best practice is to use both polling and event-based protocols. Tune the polling frequency and event granularity for the specific environment, topology, bandwidth, and notification needs. Refer to the *User Guide* for specific Monitor performance recommendations.

NOTICE

Creating a baseline performance measurement report of availability, capacity and performance can provide the basis of capacity planning and proactive network management.

Reachability may vary by protocol (for example, Telnet works, but not ping), so test multiple protocols. If it is remote, try phoning the affected site and asking for information.

Missing Performance Data / Monitor Stops Polling

This is a problem related to missing performance monitor data accompanied by logs errors like the following:

```
2014-02-12 11:23:45,357 705304239 ERROR
   [com.dorado.core.mediation.base.OWMediationDeploymentHelper]
   (WorkManager(2)-63:) The currently deployed targets for polling
   subscription oware.polling.PollingSubscriptionDO::59x8vSybkeEj6I2 on
   mediation partition MED_PART-medPartition have somehow become out of
   synch with the application server and database.

Actual target count, coming from the database: 184 meditation server
   currently has: 0

We are now resynching this information from the appliation server to the
   mediation server so that it will once again be accurate.
```

This error indicates that your mediation servers have no current performance monitor subscription targets when 184 targets were expected. This could possibly be due to a mediation server fail-over to another cluster member or a mediation server coming back on-line, etc. This is an expected error when a difference is detected in the expected (database) monitor subscriptions and actual subscriptions in the mediation server. A periodic process executes to ensure performance monitor subscriptions remain in sync.

Solution(s):

- Verify connectivity between application servers and mediation servers.
- Verify mediation server state/health and cluster member status (active/inactive).
- Verify polling subscriptions in the Monitor Editor.
- Verify polling skip/miss counts in the Monitor Editor.
- Review number of targets in each monitor, verify each has 10,000 or fewer targets. Monitor any targets over that figure in a new monitor.
- Restart the mediation server process if subscription problems persist.

Reports

- I created a report and didn't specify a location. Where's my report?
  Solution: The default location for reports is `/oware/temp/reportfw` under the installation root.

Report Missing Data

This software limits reports to 5000 rows by default when saving reports to the database (*Save* checkbox checked). This limit does not apply when not saving and only exporting the report. Increasing this default value is not best practice because of potential performance impact.

Solution: If you must increase the size of reports you save, increase the following report-related property values and restart application server(s).

```
com.dorado.redcell.reports.max.report.size (Increase to save larger
   datasets to database - not recommended)

com.dorado.redcell.reports.max.report.query.size (Increase to include more
   data in exported reports)
```

Follow these steps:

1 Edit [Installation root]owareapps/installprops/lib/installed.properties and add/modify the desired properties.

```
com.dorado.redcell.reports.max.report.size=<new value>
com.dorado.redcell.reports.max.report.query.size=<new value>
```

2 Restart application server(s).

Web Portal

Web portal problems can occur as described in the following section:

I. Web portal performance is slow or login page inaccessible.

Solution: Check/verify portal memory heap settings and increase as needed.

To manually change the web portal heap settings, verify sufficient system memory exists then modify the setenv.sh (Linux) or setenv.bat (Windows) file:

```
set "PORTAL_PERMGEN=768m"
set "PORTAL_MAX_MEM=4096m"
set "PORTAL_INIT_MEM=4096m"
set "PORTAL_32BIT_MAX_MEM=768m"
```

These files are in the [Installation root]\oware\synergy\tomcat-x.x.xx\bin directory.

For Linux, restart the portal service to apply new memory settings. In Windows, besides updating setenv.bat you must run service.bat update in that same directory.

II. Web Portal Displaying Errors: The application web portal displays errors immediately after starting application processes.

Solution: Allow the application/web server more time to fully start before attempting to access the web portal.

III. Web Portal Down, Cannot Access/Display Login Page: The application web portal displays errors or cannot be accessed.

Solution: Verify the Portal Oracle database password has not expired. By default, netview is the default user to connect to database. This appears in /opt/dorado/oware/synergy/tomcat-[version]/webapps/ROOT/WEB-INF/classes/portal-ext.properties

```
jdbc.default.username=netview
jdbc.default.password=dorado
```

Connect using SQL*Plus to set new password, you can even use the same password you had earlier.

```
$ sqlplus
SQL*Plus: Release 11.2.0.1.0 Production on Mon Dec 13 01:12:07 2010
```

```
Copyright (c) 1982, 2009, Oracle. All rights reserved.

Enter user-name: netview
Enter password:
ERROR:
ORA-28001: the password has expired

Changing password for netview
New password:
Retype new password:
Password changed

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

After resetting the password, best practice is to set profile/policy expiration to LIFETIME to prevent this from expiring again.

NOTE:

Users `netview` and `synadmin` need to have same password.

MySQL Database Issues

Consult the *User Guide* for preventive `my.cnf` performance tuning tips.

I. Slow Performance: If your system's performance slows to the extent application is unusable, and its log contains the error below or similar entries:

```
com.mysql.jdbc.CommunicationsException: Communications link failure due to
   underlying exception:
** BEGIN NESTED EXCEPTION **
java.net.SocketException
MESSAGE: Software caused connection abort: recv failed
STACKTRACE:
java.net.SocketException: Software caused connection abort: recv failed
```

Solution: Follow these steps:

1. Review disk space, verify adequate space is available on partition.
2. Shutdown MySQL database.

3 Edit the `[installation root]\oware3rd\mysql\[version number]\my.cnf` file. Review database size configuration and add another data file to extend size as needed. Save file.

For example: Change:

```
innodb_data_file_path = /ibdata/ibdata1:1024M:autoextend:max:10500M
```

To:

```
innodb_data_file_path = /ibdata/ibdata1:1024M;/disk2/
   ibdata2:1024M:autoextend
```

4 Restart MySQL. Refer to the *User Guide*'s MySQL configuration advice. You can also refer to the following link additional detail: dev.mysql.com/doc/refman/5.1/en/innodb-data-log-reconfiguration.html

II. Tablespace Full / Application crashes. Log entries indicating tables or tablespace are full. Likely accompanied by application crashes. Examples of log entries (which may reflect any table).

```
The table 'rc_notification_hist' is full
```

or

```
InnoDB: Warning: Cannot create table 'owbusdb/pm_dtl_7879' because
   tablespace full
```

Solution: Follow these steps:

1 Review disk space, verify adequate space is available on partition.

2 Shutdown MySQL database.

3 Open `[Installation root]\oware3rd\mysql\[version]\my.cnf` file. Review database size configuration and add another data file to extend size as needed.

For example, change

```
innodb_data_file_path = /ibdata/ibdata1:1024M:autoextend:max:10500M
```

To:

```
innodb_data_file_path = /ibdata/ibdata1:1024M;/disk2/
   ibdata2:1024M:autoextend
```

4 Save the file.

5 Restart MySQL. Refer to the *User Guide*'s MySQL configuration advice. You can also refer to the following link additional detail: dev.mysql.com/doc/refman/5.1/en/innodb-data-log-reconfiguration.html

III. MySQL Connection Exceptions: The following error, or similar errors, appear in log:

```
Caused by: com.mysql.jdbc.CommunicationsException: Communications link
   failure due to underlying exception:

BEGIN NESTED EXCEPTION **

java.net.NoRouteToHostException
```

```
MESSAGE: No route to host

STACKTRACE:

java.net.NoRouteToHostException: No route to host at
   java.net.PlainSocketImpl.socketConnect(Native Method)
```

Solution: This indicates a connectivity issue between your application server and the database. Discover the root cause of this communication issue and correct it. Here are some things to try:

- Check with `ps -ef | grep MySQL` in Linux or in Windows' Services utility to make sure your database is running. If not, re-install (or uninstall / reinstall) until this daemon / service starts without problems.
- Execute pingdb to test database connectivity.
- Check network interfaces and connectivity between application server and database.
- Try connecting with MySQL Workbench or other tool.
- Verify database is up and healthy.
- Verify database login/password has not changed or expired (default user/password: root/dorado)

IV "Too Many Connections" Error. Ironically, this error may indicate the `max_connections` parameter in your `my.cnf` files is too *small*. To use more connections, change the setting in the `my.cnf` file. For example, in `\oware3rd\mysql\X_X_X-64\my.cnf`, under the `[mysqld]` section add:

```
max_connections = 500
```

You can login to mysql to check current settings:

```
mysql -u root --password=dorado

mysql> show variables like 'max_connections';
```

To check open connections

```
mysql> SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

Oracle Database Issues

Best practice for Oracle database users is to have a database administrator configure their Oracle application before installing Dell OpenManage Network Manager to use an Oracle database. This ensures correct configuration, best performance and connection with the database.

If you are installing only a single component, rather that a re-installation with the full installation wizard, installation is a three-step process:

1. Extract (`ocpinstall -x [filename(s)]`)
2. Optionally, update / verify the database schema (on database servers only). (`ocpinstall -l [filename(s)]`)
3. Seed the database (on database servers only). (`ocpinstall -s [filename(s)]`)

Refer to the first chapter of the *User Guide* for more about Oracle databases.

Debug

When an error appears in logs (see Logs on page 138) it indicates for which Java class you need to increase the level of logging if you want debugging information. You can change logging levels to get additional (debug) information.

NOTICE

Best practice is to now alter *Log Categories* in the Application Server Statistics portlet by clicking that button. This alteration simplifies editing `log4j.xml` files since it provides a graphical interface, and if you have more than one server, it alters the log levels for all servers at once.

Flipdebug

You can easily turn debug on or off with the `flipdebug` script. Run this while the application server is running and remember to wait a few moments for the application server to pick up your changes. Here is the usage (just type the script name to see these options):

```
Usage: flipdebug [-d] [-t] [-r] [-h|-?] [-p] product[,product]


-d Turn on debug for all packages
-t Turn on trace for all packages
-p Turn on trace/debug only for product[,product] (no spaces between
   products)
-r Revert to original log4j settings
-h|-? Display usage
```

The *product* name in -p matches the directory under `owareapps`. The debug and trace write to the log and to stdout.

Fine-Tuning Debug

To fine tune debug further, create a file, whose name ends in `log4j.xml` in the `owareapps\installprops\server\conf` directory with the categories you want changed. If the class does not exist within the `log4j` file, add it and set it to debug. Changes preserved in such a file remain in place until you change them again, and are not overwritten when software upgrades occur.

To increase logging levels to DEBUG, change `WARN` or `INFO` to `DEBUG` in categories like the following:

```
-   <category name="com.dorado.redcell">
-       <priority value="WARN"/>
-     </category>
...
-     <category name="redcell">
```

```
-       <priority value="WARN"/>
-     </category>

-     <category name="RedCell">
-       <priority value="INFO"/>
-     </category>
```

To see what categories are available, look in `\oware\jboss-x.x.x\server\oware\conf\log4j.xml`. This file concatenates all logging categories, but is generated, and should *not* be changed.

When application server starts, it detects logging levels in these categories and concatenates them into the server's `log4j.xml` from `*log4j.xml` files in the `server\conf` directories of installed components under `owareapps`.

When it starts, application server processes logging for components in order of their dependency, and overrides any detected settings from a file whose name ends in `log4j.xml` in the `installprops` directory.

This application applies detected changes once a minute. The log4j file scanner can then detect any subsequent changes up to a minute after making them. The `server.log` is not truncated when this occurs.

The following are additional categories that allow logging level changes:

For Mediation Server registration with App Server, add the following category:

```
<category name="com.dorado.mbeans.OWMedServerTrackerMBean">
  <priority value="WARN"/>
</category>
```

For SNMP and Syslog, change INFO to DEBUG in

```
<category name="com.dorado.core.mediation">
  <priority value="INFO"/>
</category>
```

To view debug output:

Server

Debug does not appear in real-time in the application server shell (if you have one). View real-time and historical logs in the `oware\jboss-x.x.x\server\oware\log` directory.

NOTICE

Typing `oware` in a Windows shell lets you use Linux commands like `tail -f server.log`. Tailing it lets you watch the log file as it is generated.

Resolving Port Conflicts

Installation scans for port conflicts, but these may arise after you install too. If your application runs with others, conflicts related to those other applications' ports are possible. For example: the application can have trouble communicating with the built-in TFTP server for backups. Port contention of TFTP on UDP port 69 with other applications can cause this. Try rebooting the system to clear any unused ports and verify that UDP port 69 is not in use before starting the application.

Finding Port Conflicts

You can find ports in use with the following command line:

```
netstat -a -b -o | findstr [port number]
```

Use this command to track down port conflicts if installation reports one. Best practice is to run this software on its own machine to avoid such conflicts. Freeware port conflict finding programs like Active Ports are also available.

Logs

You can execute the `getlogs` script to package relevant logs if you need technical support. Run this script in a command shell where you have sourced the Oware environment (in Windows *Start* > *Run* `cmd`, then run `oware`, or in Linux `. /etc/.dsienv`, and then invoke the `getlogs` script). This script creates a `logs.jar` file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this file to technical support to help troubleshoot problems.

NOTE:

Server logs are in oware\jboss-x.x.x\server\oware\log. **Also:** If you install with an Oracle database, because the Oracle installation is outside Dell OpenManage Network Manager's installer, Dell OpenManage Network Manager does not create db_setup.log.

The `getlogs` script also gathers the tomcat web server logs for the web portal.

If `getlogs` halts, and does not produce a `logs.jar` file, it may be because someone installed this software, or a previous version as root, so `getlogs` does not have access to directories and groups owned by root. Change the permissions and/or ownership of those groups and directories to make `getlogs` work.

Increasing Startup Logging

For applications based on Oware 6.2.1 and later (see your `versions.txt` file or *Manage* > *Show Versions* for your version), you can add the following line to `oware\lib\pmstartup.dat`. If you add this line, this software logs all output from the startappserver script to a file:

```
server.out.filename=/opt/dorado/pmserver.log
server.out.filename=G:\Program Files\Dell\OpenManage\pmserver.log
```

The destination you specify can be any valid path and file name. This helps when the server never starts or errors occur during deployment that would not be in the usual server.log.

Tuning Log Retention

The following properties are in `appserver.properties` and `redcell.properties` file for purging log files. As with all other properties, best practice is to override them in `owareapps/installprops/installed.properties`.

```
owappserver.properties
# This property defines how many days to retain server log files. All log
   files
# older than the specified retention days are purged. Back up older log
   files if
# you want to retain them. Set the property to -1 to disable this option.
   The
# default is 7.
oware.server.log.files.retention.days=7


redcell.properties
# This property defines where redcell client log files are stored The
# following is also the default:
redcell.log.files.location=oware.user.root/owareapps/redcell/logs


# This property defines how many days to retain the client's
# log files. Files older than the specified age are purged.
# Setting the property to a negative value disables log file deletion.
# The default is 7.
redcell.log.files.retention.days=7
```

Log Generation Fails with "Build Failed" Error (Linux)

Log generation and the build process fails when attempting to generate logs and is accompanied by an error like this:

```
BUILD FAILED
/opt/dorado/oware/conf/owrtbuild.xml:46: Problem creating jar: /opt/
   dorado/logs/ocpinstall_14332.log (Permission denied)
```

To successfully build logs, included files must be owned by the installing user (example: MyUser).

Solution: Locate and change the ownership of file(s) breaking the build process. To repair these, follow these steps:

1 Open a shell and source environment by typing `. /etc/.dsienv`.

2 Type `getlogs`.

3 Navigate to the file location(s) that appear in any error.

4 Type `ls -l` and review the owners for the files in this directory.

5 Type `su root` and enter root password.

6 Change the file ownership from user `root` (or other) to the installing user.

Type, for example: chown `MyUser:MyUser ocpinstall_*` to change ownership of all files beginning with `ocpinstall_` .

7 Type `ls -l` to confirm new file ownership.

8 Type `exit` to return to the installing user prompt.

9 Repeat this process until getlogs builds a `logs.jar` successfully without error. You may need to correct file ownership in several locations before a successful build can occur.

To avoid a reoccurrence, do not perform any application-related command line operations while logged in as `root`. Such tasks must always be executed by the installing user.

WMI Troubleshooting Procedures

The following sections describe troubleshooting common WMI problems. To monitor with WMI, the following must be true:

- WMI must be enabled on the remote, monitored server and functioning properly.
- The remote server must be accessible through a Remote Procedure Call (RPC) connection to run WMI queries.

If your system does not meet these conditions WMI displays an *Unknown* status.

Examples of what may prevent the above can include the following:

- Not having local Administrator rights on the monitored host.
- Firewalls blocking the WMI traffic.
- An operating system not configured for WMI.
- An error in the credential password.

To help diagnose these issues, test the WMI services, the remote WMI connections, and you system's component configuration.

The following topics provide troubleshooting assistance:

- WMI Troubleshooting on the local host.
- Testing Remote WMI Connectivity
- Verify Administrator Credentials
- Enable Remote Procedure Call (RPC)
- Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)

- Add a Windows Firewall Exception for Remote WMI Connections
- Checking the Authentication portlet to ensure correct credentials exist.

Finally, if these troubleshooting tips are not enough, see Additional WMI Troubleshooting on page 149.

WMI and Operating Systems

Best practice is to avoid using Windows Vista And Windows 2008 for network monitoring of WMI. WMI works well Windows 7, even for larger networks. But with Vista and Window 2008 this is not true. Some tests even indicate that Windows 7 is up to 70 times faster than Windows 2008 or Vista. In these tests, hardware (CPU, memory) does not strongly affect WMI monitoring performance, nor does virtualization.

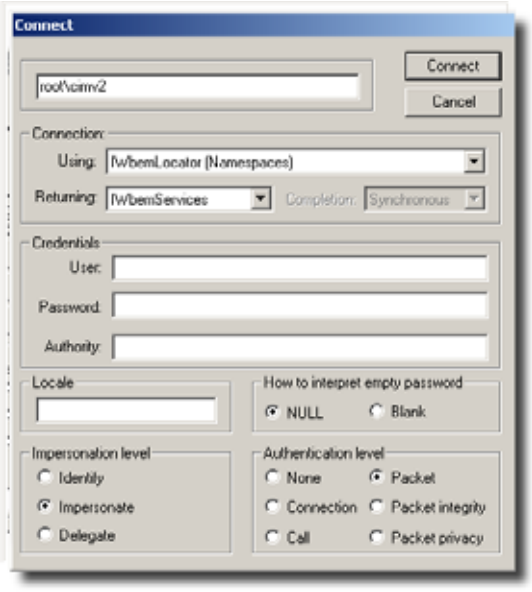
WMI Troubleshooting

To troubleshoot WMI, do the following:

1 To test WMI locally, click *Start* > *Run*, then enter `wbemtest.exe` and then click *OK*. The `wbemtest.exe` program comes with Windows that supports WMI.

2 Click *Connect* on the Windows Management Instrumentation Tester window.

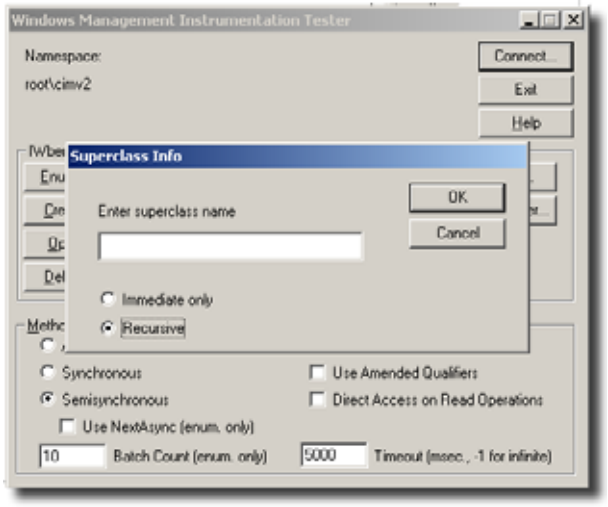
3 Enter `\root\cimv2` in the field at the top of the dialog box next to the *Connect* button.



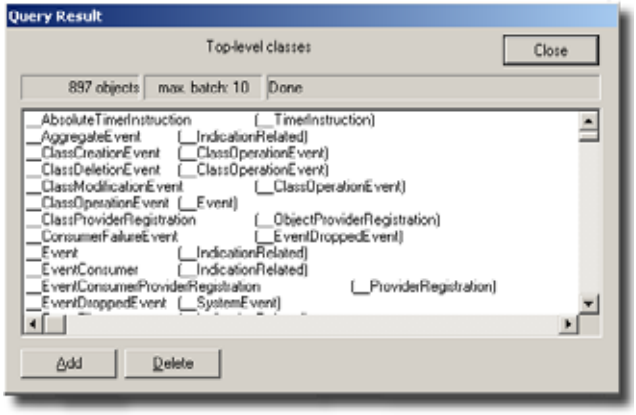
4 Click *Connect*.

5 Click the *Enum Classes* button.

6 Select the *Recursive* radio button. Leave the superclass name blank, and then click *OK*.



7 If the WMI classes you are querying appear in this list, local WMI services are functioning correctly.



8 If the list does not appear or does not contain the desired WMI class, WMI is not functioning correctly. Continue reading this section for guidance on repairing WMI services on the target server.

9 Click *Exit*.

10 If you did not see the desired classes, Reset the WMI Counters, and re-test until those classes appear.

Reset the WMI Counters

At times, the WMI performance counters may not get transferred to WMI because services were delayed or started out of order (see support.microsoft.com/kb/820847).

To manually reset the WMI counters:

1. Stop the Windows Management Instrumentation (WMI) service.
2. Open a shell (Click *Start* > *Run*, type `cmd`, and then click *OK*).
3. At the command prompt, type `winmgmt /resyncperf`, and then press [Enter].
4. At the command prompt, type `wmiadap.exe /f`, and then press [Enter].
5. Type `exit`, and then press [Enter] to close the command shell.
6. Restart the WMI service.

After resetting the WMI counters, retest WMI. If resetting the WMI counters did not solve your problem, see "WMI is Still Not Working, Now What?" on page 12.

Testing Remote WMI Connectivity

Ensure WMI is running on the remote, monitored host. This is similar to WMI Troubleshooting on the local host described above.

1. Click `Start > Run`, enter `wbemtest.exe` and then click *OK*.
2. Click *Connect* on the WMI Tester window.
3. Enter `\\Target_Primary_IP_Address\root\cimv2` in the field at the top of the dialog box. Replace *Target_Primary_IP_Address* in this entry with the actual host name or primary IP address of the target server.
4. Enter the appropriate administrator user name in the User field, the password in the Password field, and `NTLMDOMAIN:NameOfDomain` in the Authority field. Replace *NameOfDomain* with the domain of the user account specified in the User field.
5. Click *Connect*.
6. Click *Enum Classes*.
7. Select the Recursive radio button without entering a superclass name, and then click *OK*.
8. If the WMI class list appears, remote WMI is functioning correctly. Skip to the next topic and validate your credentials.
9. If the list does not appear, remote WMI is not functioning correctly. Continue reading this topic for guidance on restoring remote WMI connections on the target server, and retest remote WMI after completing each troubleshooting step.

11. Click the *Close* button, and then click *Exit*.

Verify Administrator Credentials

Only a credential that has administrator rights on the target server has the necessary permissions to access the target host's WMI services. Make sure that the username and password you are using belongs to an administrator on the target host.

If the administrator credential is a domain member, be sure to specify both the user name and the domain in standard Microsoft syntax. For example: `DOMAIN\Administrator`.

Enable Remote Procedure Call (RPC)

Remote WMI connections use RPC as a communications interface. If the RPC service is disabled on the target server, remote WMI connections cannot be established.

These steps show how to enable the RPC service:

1. Log on to the target host as an administrator.
2. Click *Start* > *Run*, then type `services.msc`, and then press [Enter].
3. Right-click Remote Procedure Call (RPC), and then click *Start* on the shortcut menu.

Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)

If the target computer is running Windows Vista or Windows Server 2008, you may be required to make settings changes to allow remote WMI requests (See msdn.microsoft.com/enus/library/aa822854(VS.85).aspx).

DCOM—Edit Default and Limits permissions to allow the following actions:

- Local launch (default permission)
- Remote launch (default permission)
- Local activation (limits permission)
- Remote activation (limits permission)

  For more information, see Enabling DCOM on page 145.

WMI Namespaces—Modify the CIMV2 security to enable and remote enable the account used to access the server or workstation through WMI. You must ensure the security change applies to the current namespace and subnamespaces. For more information, see Enabling Account Privileges in WMI on page 146.

User Account Control—Remote UAC access token filtering must be disabled when monitoring within a workgroup environment. For more information, see Disabling Remote User Account Control for Workgroups on page 148.

Enabling DCOM

WMI uses DCOM to communicate with monitored target computers. Therefore, for Application Performance Monitor to use WMI, you must have DCOM enabled and properly configured. Follow these steps to enable DCOM permissions for your Application Performance Monitor credentials:

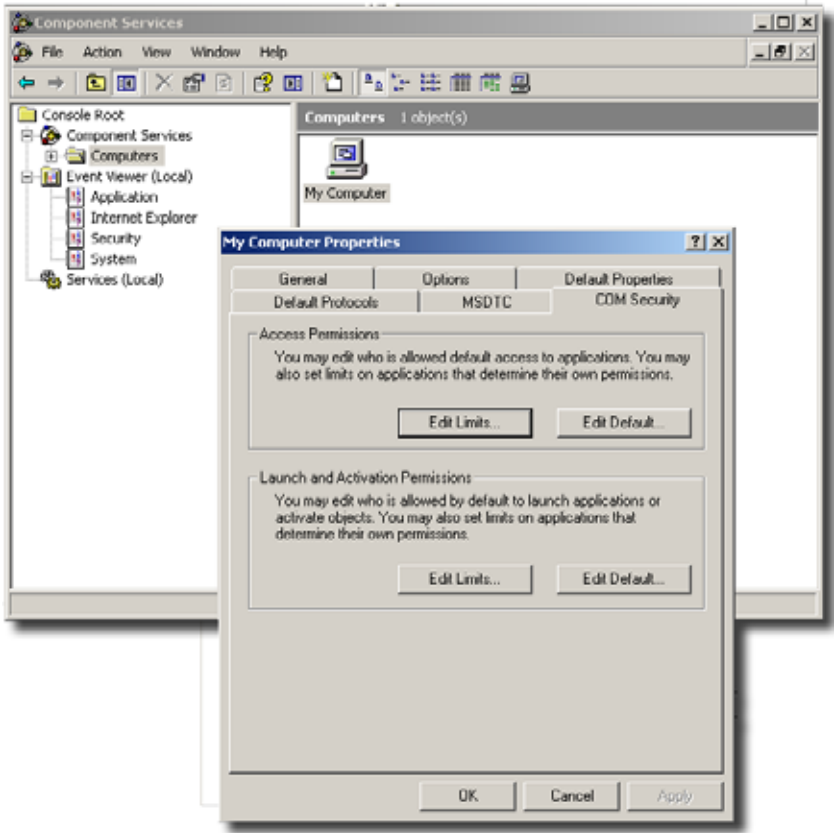
1 Log on to the target host as an administrator.

2 Navigate to *Start* > *Control Panel* > *Administrative Tools* > *Component Services*. (Only the Classic view of the Control Panel has this navigation path). You can also launch this console by double-clicking `comexp.msc` in the `/windows/system32` directory.

3 Expand *Component Services* > *Computers*.

4 Right-click *My Computer*, and then select *Properties*.

5 Select the COM Security tab, and then click *Edit Limits* in the Access Permissions grouping.



6 Ensure the user account collecting WMI statistics has *Local Access* and *Remote Access*, and then click *OK*.

7 Click *Edit Default*, and then confirm the user account collecting WMI statistics has *Local Access* and *Remote Access*, then click *OK*.

8 Click *Edit Limits* in the Launch and Activation Permissions grouping.

9 Ensure the user account collecting WMI statistics has *Local Launch, Remote Launch, Local Activation*, and *Remote Activation* enabled, and then click *OK*.

10 Click *Edit Default*, and then ensure the user account collecting WMI statistics has *Local Launch, Remote Launch, Local Activation*, and *Remote Activation* enabled.

11 Click *OK*.

Enabling Account Privileges in WMI

The account you specify for authentication must possess security access to the namespace and subnamespaces of any monitored target hosts. To enable these privileges, complete the following procedure.

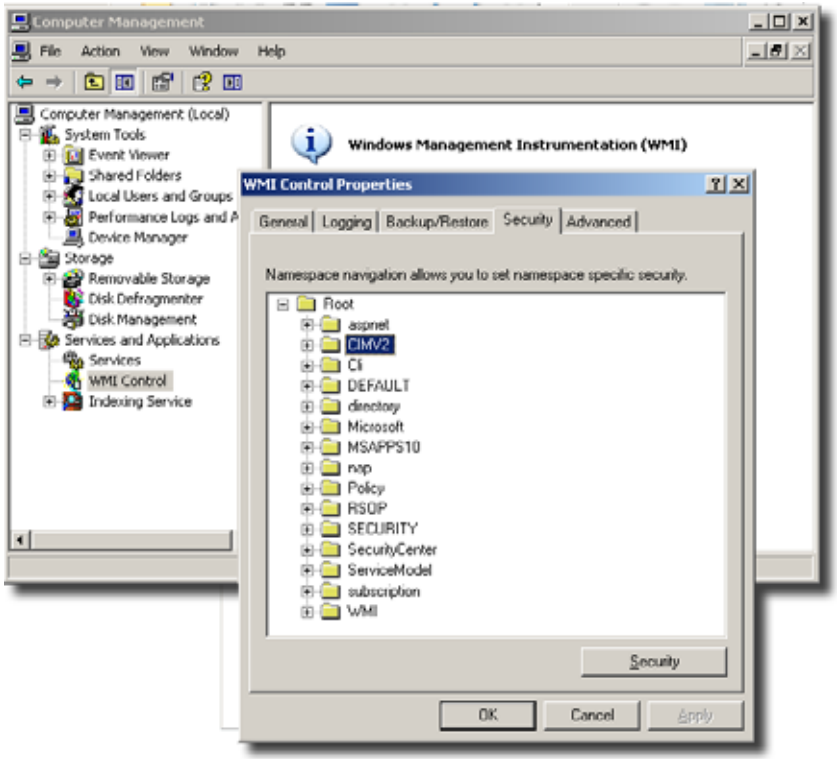
To enable namespace and subnamespaces privileges:

1 Log on to the host you are monitoring as an administrator.

2 Navigate to *Start* > *Control Panel* > *Administrative Tools* > *Computer Management* > *Services and Applications*. (Classic View of the Control Panel this navigation path).

3 Click WMI Control, and then right-click and select Properties.

4 Select the Security tab, and then expand Root and click CIMV2.



5 Click Security and then select the user account used to access this computer and grant the following permissions:

–Enable Account

–Remote Enable

6 Click *Advanced*, and then select the user account that accesses this computer.

7 Click *Edit*, select *This namespace and subnamespaces* in the *Apply to* field, and then click *OK*.

8 Click *OK* on the *Advanced Security Settings for CIMV2* window.

9 Click *OK* on the *Security for Root\CIMV2* window.

10 Click *Services* in the left navigation pane of *Computer Management*.

11 Select *Windows Management Instrumentation* in the *Services* result pane, and then click *Restart*.

Disabling Remote User Account Control for Workgroups

If you are monitoring a target in a workgroup, you must disable remote User Account Control (UAC). Although this is not recommended, it is necessary when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

CAUTION:

The following modifies or creates a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Best practice is to back up your registry before making these changes.

To disable remote UAC for a workgroup computer:

1. Log on to the host you want to monitor as an administrator.
2. Click Start > Run, and enter `regedit`.
3. Expand `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.`
4. Locate or create a DWORD entry named LocalAccountTokenFilterPolicy and provide a DWORD value of 1.

NOTE:

To re-enable remote UAC, change the DWORD value to 0.

Add a Windows Firewall Exception for Remote WMI Connections

If the target computer has Windows Firewall enabled, it must have a Remote WMI exception to allow remote WMI traffic through (See /msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx). Follow these steps to add this exception:

1. Open a command shell (Click *Start* > *Run*, type `cmd` and then press [Enter]).
2. At the command prompt, type

   ```
   netsh firewall set service RemoteAdmin enable
   ```

   Press [Enter]
3. Type `exit` then press [Enter].

If adding the firewall exception did not solve your problem, see Additional WMI Troubleshooting below.

WMI Authentication

If the above troubleshooting has been done correctly, ensure the authentication credentials for the WMI device in *Resources* match those for an administrator. Select the device in the Resources screen, and click *action* > *Open* (or right-click and select *Open*). Go to the *Authentication* node of the tree, and confirm that the correct authentication objects appear there.

Additional WMI Troubleshooting

The above discusses the most common errors behind WMI failures. After trying these, if you are unable to get WMI services working, consult the following articles about this subject on Microsoft's Technet and Developer Networks:

- *WMI Isn't Working!: Troubleshooting Problems with WMI Scripts and the WMI Service.* (See www.microsoft.com/technet/scriptcenter/topics/help/wmi.mspx)
- *WMI Diagnosis Utility: A New Utility for Diagnosing and Repairing Problems with the WMI Service* (See www.microsoft.com/technet/scriptcenter/topics/help/wmidiag.mspx)
- *WMI Troubleshooting* (See msdn.microsoft.com/enus/library/aa394603.aspx)

NOTE:

While the above URLs are believed correct, they may change.

jstack Debugging in Windows 7

Technical assistance sometimes uses the jstack stack trace tool to debug problems in this software. When you install application server to run as a service (autostart), the user SYSTEM owns the application server process. You also cannot log into Windows 7 as user SYSTEM. For security's sake, no other user can access a service running as the SYSTEM user in later Windows 7 kernels. The jstack tool therefore does not work if you run it as the (non-SYSTEM) user logged in to Windows 7.

Workaround: To view a jstack output for application server, or any service (and its subprocesses) running as the user SYSTEM, you must run jstack (and jps) as user SYSTEM. Windows 7 provides no direct way to log in as user SYSTEM, so the following sidesteps this prohibition:

1. Open a command shell (Click the *Start* icon and type `cmd` in the *Search Programs and Files* field.)
2. At the command prompt, type:

```
sc create testsvc binpath= "cmd /K start" type= own type= interact
```

3. Then type:

```
sc start testsvc
```

The `sc start` command immediately creates a new command shell owned by SYSTEM, even if the original command window failed to start with error 1053 (this is expected since `cmd.exe` does not have any service-related code in it).

4 Open an oware shell inside the SYSTEM-owned command prompt created in Step 3. (Type `oware` at the command line.)

5 In that oware shell, run `jps` to see the process ID (PID) of the application server's Java process (`OWLaunchV2`).

6 Then run `jstack [PID]` in the SYSTEM shell.

7 To delete the testsvc when you are finished, type this on a command line:

```
sc delete testsvc
```

FAQs about Monitoring Mediation Servers

After making a UDP-based JGroups discovery request and receiving a response from an application server in the cluster, each mediation server makes an RMI (TCP) call to an application server every 30 seconds. This RMI call results in a "call on cluster" on the application server cluster, using JGroups (UDP by default), to call the agentHeartbeat method of the OWMedServerTrackerMBean on each application server in the cluster. The primary application server updates the timestamp for the medserver in question, and the others ignore the call. Every five seconds, the primary application server checks to see if it has not received a call from a mediation server in the last 52 seconds. If it has not, it attempts to verify down status by pinging the suspected mediation server. Then it issues an RMI call on that mediation server. It considers the meditation server down if the ping or the final RMI call fails. This avoids false meditation server down notifications when a network cable is pulled from an application server.

- Does the application server wait 15 seconds after receiving the mediation server's response? Or does it monitor mediation server every 15 seconds regardless of the mediation server's response?

  The receipt of the mediation server's RMI call is on a different thread than the monitoring code. The monitoring code should run every 5 seconds, regardless of the frequency of mediation server calls. However, after investigating the scheduling mechanism used (the JBoss scheduler - http://community.jboss.org/wiki/scheduler), it is possible that other tasks using this scheduler could impact the schedule because of a change in the JDK timer implementation after JDK 1.4.

- What kind of functionality (JMS?) does application server use to send and receive Dell OpenManage Network Manager messages?

  The application server does not actively monitor the mediation servers unless it fails to get a call from one for 52 seconds. If it does try to verify a downed mediation server, it uses an RMI call.

The RMI calls use TCP sockets. It may use multiple ports: 1103/1123 (UDP - JGroups Discovery), 4445/4446 (TCP - RMI Object), 1098/1099 (TCP - JNDI), or 3100/3200 (TCP - HAJNDI), 8093 (UIL2).

- What kind of problem or bug would it make application server to falsely detect a mediation server down? For example, would failing to allocate memory cause application server to think a mediation server is down (dead)?
  An out of memory error on an application server could result in a false detection of a downed medserver.
- If such memory depletion occurs as described in the previous answer, would the record appears in the log? If it doesn't appear in the log, would it possibly appear if the log-level is changed?
  An out of memory error usually appears in the log without modifying logging configuration, since it is logged at ERROR level.
- The log shows that a mediation server was detached from the cluster configuration, but what kind of logic is used to decide the detachment from the cluster? For instance, would it detach application servers if they detect the mediation server down?
  JBoss (JGroups) has a somewhat complex mechanism for detecting a slow server in a cluster, which can result in a server being "shunned." This logic remains, even though we have never observed the shunning of a server resulting in a workable cluster. This is the only mechanism which automates removing servers from the cluster. The configuration for this service is located in `$OWARE_USER_ROOT/oware/jboss-x.x.x/owareconf/cluster-service.xml`. Shunning can be disabled by replacing all `shun='true'` instances with `shun="false"`. A flow control option also exists which regulates the rate of cluster communication to compensate for one server being slower in processing cluster requests than another. The detection of a mediation server being down with the heartbeat mechanism described here does not attempt to remove the medserver from its cluster.
- Why does Mediation server not appear in the control panel?
  Make sure you have followed the instructions in Enabling Mediation Server in the Web Portal.

Linux Issues

The following are issues with Linux installations:

- Install in `/opt/dorado`, unzip package in, for example, `/opt/installs`, not `/opt/dorado`.
- Linux (executed as the root user) uses this command:

  ```
  /etc/init.d/owaredb start
  ```

  You should see the following response in the shell where you execute this command:

  ```
  Starting MySQL[  OK  ]
  ```

- If you experience problems with discovery, and see errors on startup similar to the following:

```
[com.dorado.core.mediation.snmp.SRSnmpEventReportDispatcher] (Thread-36
   RecvTrap Exception :

com.dorado.core.mediation.snmp.SRSnmpException:

at com.dorado.core.mediation.snmp.SRSnmpSession.nRecvTrap(Native Method)

at
   com.dorado.core.mediation.snmp.SRSnmpSession.recvTrap(SRSnmpSession.jav
   a:733)

at
   com.dorado.core.mediation.snmp.SRSnmpEventReportDispatcher.run(SRSnmpEv
   entReportDispatcher.java:96)

at java.lang.Thread.run(Thread.java:662)
```

  or

```
ERROR [com.dorado.core.mediation.syslog.OWSysLogListener]
   (OWSysLog.Listener Received a null SysLog message. SysLog port may be in
   use. Shutting down SysLog listener.
```

  You may be able to solve this issue by increasing the available memory on the entire system or lowering the heap memory used by your system. The former option is best practice.

Application Server Memory (Linux and Windows)

I. Linux application server appears to have low memory.

Solution: Memory statistics using TOP can be deceiving. Linux may have borrowed some free memory for disk caching. To determine if this is the case:

1 Open a shell and execute command: `free -m`

  This returns the amount of (true) free/available memory for application use in megabytes. See cache value in line `-/+ buffers/cache: 26441 37973` below…

```
[redcell@AppRedcell01 ~]$ free -m
total used free shared buffers cached
Mem: 64414 63823 590 0 364 37018
-/+ buffers/cache: 26441 37973
Swap: 65535 11 65524
[redcell@AppRedcell01 ~]$
```

  Here, 37,973M is still free for application use.

  See www.linuxatemyram.com/ for more detail on this topic.

  Alternatively,

2 If TOP reveals an excessive and abnormally high memory usage for the application java process, you may need to restart your application server and evaluate installed/available memory with regard to your sizing and application usage requirements. Install more server memory as needed.

II. Genuine memory issues appear if logs contain an error like `java.lang.OutOfMemoryError: GC overhead limit exceeded`, and application server performance is slow, possibly preventing log into web portal. You may also see many other errors, for example, from performance monitoring:

```
WARN  [com.dorado.broadscope.polling.PollingResultsDAOImpl]
   (WorkManager(2)-99:) Low on memory.  Discarding this batch.
```

Solution: These errors indicate memory resources are low or have been depleted.

To address this, first review any potential causes for an increase in memory usage. For example, has there been a significant increase in performance monitor load, perhaps from reducing polling times or an increase in targets/attributes? Have there been any other changes?

Assuming sufficient server memory is available, increase heap size. Adjust memory values below according to your environment and configuration needs:

1 Shut down the application.

2 Open `owareapps/installprops/lib/installed.properties` file for editing.

3 Modify the `oware.server.max.heap.size` property

```
oware.server.max.heap.size=3072m
```

In this example, a recommended increase would be 25% to 4096m.

4 Increase `oware.server.min.heap.size` to match (4096m)

5 Save changes to `installed.properties`.

6 Restart the application.

NOTE:

Heap adjustments work for Windows too.

III. Out of Memory errors like `Out of Memory: unable to create new native thread` in logs for server (application or mediation) may indicate memory resources are sufficient, but threads are not.

Solution: The operating system may be limiting the number of available threads for use by the application. Check/modify the `ulimits` settings with these steps:

1 Open shell/CLI and type `ulimits -a`.

Open files and User Processes should not be set to typical defaults (1024). Change these with the next steps.

2 Open `/etc/security/ limits.conf` for editing.

3 Add the following lines and save.

```
<installing user> soft nofile 65536
<installing user> hard nofile 65536
<installing user> soft nproc 65536
<installing user> hard nproc 65536
```

4 Restart the application processes.

How To:

Install on Linux

To run Dell OpenManage Network Manager in Linux, use the Best Practices: Linux and the steps in Create a user and prepare for installation below.

Best Practices: Linux

- This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on).
- Most Linux intstallations include lib-apr for Tomcat. This application requires it, so if you have customized your Linux host(s) to omit it, put it back.
- Make sure any third party firewall or Linux's IP Tables firewall is off or allows traffic on the ports needed for your installation. See the *Ports Used* section of the *User Guide* for specifics.
- Install your Linux distribution (example: CentOS) on the server, choosing *Basic Server* when prompted to select software. *CentOS* should be the only repository selected. Choose *Customize Later* to decline further customizing the installation.
- Xvfb must be running to have a web client work correctly. This is automated when application server starts automatically. You can manually start this process with root access using the following:

  ```
  [root@test X11]Xvfb :623 -screen 0 1152x900x8 2>/dev/null &
  ```

  Confirm xvfb is running as follows:

  ```
  >ps -ef | grep Xvfb
  root 25991 21329 0 16:28 tty2 00:00:00 Xvfb :623 -screen 0 1152x900x8
  qa 26398 26053 0 16:31 pts/3 00:00:00 grep Xvfb
  ```

  (The path may differ from this example.)

- If you are installing with an Oracle database, do not set the Oracle in Dell OpenManage Network Manager to user `redcell`.

Create a user and prepare for installation

1 Add your IP and hostname to `/etc/hosts`. For example (for host `Test.localdomain`):

```
10.18.0.241 Test Test.localdomain
```

Also: verify that `/etc/hosts` points to new name—use the `cat` command and you should see output with the correct IP Address / hostname pair(s).

```
[qa@Test Desktop]$ cat /etc/hosts
10.18.0.241 Test Test.localdomain
Remember: Dell OpenManage Network Manager requires a fixed IP address for
   its host.
```

2 Login as *root*, create a new user with a home directory, set the password and add the user to the proper group. Here are examples of the commands for this. configuring user *test*:

```
useradd -m test
passwd abcxyz
usermod -aG wheel test
```

The wheel user group allows password-less `sudo`.

CAUTION:
If you are installing with an Oracle database, do not make the user for Oracle `redcell`.

3 Copy the installation files to the system.

4 After unzipping the installation files, copy the folder with source files as a subdirectory of the `/home/test` directory on the server. Set permissions on the installation directory:

```
chown -R test /home/test
chmod -R 777 /home/test/MyInstallation
```

5 Make sure the installation script has permission to execute:

```
chmod +x /home/test/MyInstallation/linux_install.sh
```

6 Create the target installation directory structure and set permissions. The following are examples, not defaults:

```
mkdir /test
mkdir /test/InstallTarget
chown -R test /test
chmod -R 777 /test
```

7 Disable Firewall with System > Administration > Firewall, or disable the firewall, and configure the network interface card with a static IP address from a command shell with the following command(s):

```
setup
```

You may be prompted to enter the root password; the password dialog may also appear behind the Firewall Configuration Startup dialog.

8 In some Linux distributions, by default the Network Interface Card (NIC) is not active during boot, configure it to be active and reboot:

```
nano /etc/sysconfig/networking/devices/ifcfg-eth0
```

Change `ONBOOT=no` to `ONBOOT=yes`

9 Disable SELINUX. Turn this off in `/etc/selinux/config`. Change `SELINUX=disabled`.

This and the previous step typically requires a reboot to take effect.

10 So...from a command line, type `reboot`.

11 Once reboot is complete, login as *root* update the system:

```
yum update -y
```

12 Linux (CentOS particularly) sometimes installs MySQL libraries by default, this interferes with Dell OpenManage Network Manager since it installs its own MySQL version. Remove mysql-libs from the system:

```
yum remove mysql-libs -y
```

Dell OpenManage Network Manager needs C++ compatibility libraries installed

```
yum install compat-libstdc++-33.x86_64 -y
```

...and install 32-bit compatibility libraries (for MySQL). (See 32-bit Linux Libraries on page 157)

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

...and reboot:

```
reboot
```

Alternatively, do these steps in the System > Administration > Add/Remove Software user interface.

13 If you have not already done so, configure file handle maximums. Open `/etc/security/limits.conf` and ensure the following are at minimum 65535:

```
test soft nofile 65536
test hard nofile 65536
test soft nproc 65536
test hard nproc 65536
```

Here, `test` is the installing user login.

Set these limits higher for more heavily used systems. You can also check/set file handles temporarily using the `ulimit -H/Sn` command. For example:

```
$ ulimit -Hn
```

```
$ ulimit -Sn
```

CAUTION:
If you enter ulimit -a in a shell, open files should NOT be 1024, and User Processes should NOT be 1024. These are defaults that *must* be changed. If you do not have enough file handles, an error appears saying not enough threads are available for the application.

14 Restart Linux. (`reboot`)

Post Installation

The following commands work only if you elected to autostart your system during installation. When running these commands ($service oware start/stop/status) with the installing user, Dell OpenManage Network Manager prompts for the user's password

1 To start the application server:

```
root > /etc/init.d/oware start
```

2 To check the status of the application server:

```
root > /etc/init.d/oware status
```

3 To start the web server:

```
root > /etc/init.d/synergy start
```

4 To check the status of the web server:

```
root > /etc/init.d/synergy status
```

5 When application server and web server have completed their startup, open a browser to this URL: `[application server IP or hostname]:8080`

32-bit Linux Libraries

For 64 bit installations, you must identify the appropriate package containing 32-bit libtcl8.4.so (for the example below: `tcl-8.4.13- 3.fc6.i386.rpm` for Red Hat).

Do not use any x86_x64 rpms; these would not install the 32-bit libraries. Any 32-bit tcl rpm that is of version 8.4 and provides libtcl8.4.so works. You can download them from Sourceforge: http://sourceforge.net. Download these, then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect
    /opt/dorado/oware3rd/expect/linux/bin/expect
[someone@RHEL5-64bit ~]$ ldd /opt/dorado/oware3rd/expect/linux/bin/ expect
        linux-gate.so.1 => (0xffffe000)
        libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/
   libexpect5.38.so (0xf7fd2000)
```

```
libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000)
libdl.so.2 => /lib/libdl.so.2 (0x0033e000)
libm.so.6 => /lib/libm.so.6 (0x00315000)
libutil.so.1 => /lib/libutil.so.1 (0x00b8d000)
libc.so.6 => /lib/libc.so.6 (0x001ba000)
/lib/ld-linux.so.2 (0x0019d000)
```

Make sure that `libtcl8.4.so` maps to `/lib/libtcl8.4.so`

An Alternative for Red Hat Linux:

1. Copy `/usr/lib/libtcl8.4.so` from a 32-bit RH system to `/usr/local/lib/32bit` on your 64-bit Red Hat system
2. As root, execute: `ln –s /usr/local/lib/32bit/libtcl8.4.so /usr/lib/libtcl8.4.so`

Install Dell OpenManage Network Manager:

3. You cannot install as root user, so, if necessary, log out as root and login as the user (here, `test`) created in the previous steps and run the installation script:

   ```
   cd /home/test/MyInstallation
   ./linux_install.sh
   ```

   ...or if you prefer a text-only installation:

   ```
   ./linux_install.sh -i console
   ```

4. Now follow the instructions in the installation wizard or text, making sure to specify the configured target directory (in this example `/test/InstallTarget`) as its installation root.
5. As part of the installation, you must run a specified installation script as root. When you run the setup script, among other things, it automatically re-routes event/alarm traffic from port 162 to port 8162.

NOTE:

You may see benign errors during the root portion of the Linux installation. Installation always attempts to find the CWD (current working directory). If another process deleted it, an error appears before the script runs. The error is benign and the script still runs, using a temp location controlled by the operating system.

6. If you did not elect to autostart them, start the web server and/or application server. The command line for application server:

   ```
   startappserver
   ```

   For web server.

```
/etc/init.d/synergy start
```

7 When application server and web server have completed their startup, open a browser to this URL: `[application server IP or hostname]:8080`

NOTE:

When you log in, if you see the message "Credentials are needed to access this application." Add `oware.appserver.ip=[application server IP address]` to `/oware/synergy/tomcat-XXX/webapps/ROOT/WEB-INF/class/portal-ext.properties`.

How To:

Upgrade on Linux

The following are best practices for upgrading from a previous version of Dell OpenManage Network Manager on a Linux machine:

1 Verify your previous version's installation application server starts without exceptions.

2 Back up the database, and any other resources that need manual installation. See the *User Guide* for more specifics.

3 Make sure your operating system does not include a MySQL database (or remove the Linux MySQL first). See step 12 in How to: Install on Linux on page 154.

4 Make sure to remove or rename the `my.cnf` file for that previous installation. The origin of the configuration in the several my.cnf files on Linux is `[installation target]/oware3rd/mysql/5.0.51-pc-linux-i686-64/my.cnf`, so be sure to alter that one if you are reconfiguring Dell OpenManage Network Manager's MySQL.

5 Ensure you have installed the 32-bit Linux Libraries, as described in step 12 of How to: Install on Linux on page 154.

6 If necessary, disable firewalls and create directories and permissions as in How to: Install on Linux on page 154.

The origin of the configuration in the several my.cnf files on Linux is `[installation root]/oware3rd/mysql/5.0.51-pc-linux-i686-64/my.cnf`, so be sure to alter that one if you are reconfiguring Dell OpenManage Network Manager's MySql.

Linux Upgrade Procedure

The following are suggested upgrade steps, when you are installing a new version of Dell OpenManage Network Manager, *and* a new Linux operating system. See also the upgrading instructions in the *User Guide*. Essentially, this outlines backing up what you can, upgrading the operating system, then upgrading Dell OpenManage Network Manager:

1 Backup the MySQL database and copy the backup to another machine or network drive with the following command lines:

```
mysqldump -a -u root --password=dorado --routines owbusdb > owbusdb.mysql
```

```
mysqldump -a -u root --password=dorado  owmetadb > owmetadb.mysql
mysqldump -a -u root --password=dorado lportal > lportal.mysql
```

The password may be different than the default (dorado).

2 Install the upgraded Linux (in this example, 6.2).

a. Prepare ISO DVDs. For example, Centos-6.2-x86_64-bin-DVD1 and DVDBi2

a Select boot from cd-rom in the Boot Menu

b Install linux 6.2

c Select your install type. For example: Desktop. Best practice is to use same settings for hostname, IP, and so on.

3 Install the Dell OpenManage Network Manager upgrade on the updated Linux installation. Make sure to look at How to: Install on Linux on page 154, including the following:

a. Remove package (if it exists) `"The shared libraries required for MySQL clients" = mysql-libs-5.1.52-1.el6_0.1 (x86_64)`

d Install package `"Compatibility standard c++ libraries" = compat-libstdc++-33-3.2.3-69.el6 (x86_64)`

4 Import the MySQL database. Shutdown application server and webserver. Use `ps-ef | grep java` to confirm no running java process exists. Kill them if any exist.

a. Drop the database with the following command lines:

```
mysqladmin -u root --password=dorado drop owmetadb
mysqladmin -u root --password=dorado drop owbusdb
mysqladmin -u root --password=dorado drop lportal
```

e Create a new database with the following command lines:

```
mysqladmin -u root --password=dorado create owmetadb
mysqladmin -u root --password=dorado create owbusdb
mysqladmin -u root --password=dorado create lportal
```

f Import the backed up database:

```
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb < owbusdb.mysql
mysql -u root --password=dorado lportal < lportal.mysql
```

To validate data:

g Start the application server with: `#service oware start`

Check status with `oware status`

h Start the webserver when the application server is ready: `#service synergy start`

Check status with `synergy status`

i Log in to confirm data were imported correctly

5 Upgrade Dell OpenManage Network Manager further, if needed.

Shutdown application server and webserver. Use `ps-ef | grep java` to confirm no Java process exists. Kill any such process if it lingers.

a. Go to the installation package's InstData directory, open a terminal and type `. /etc/.dsienv`.

j Type `./linux_install.bin` to start installing (or include the `-i console` parameters for a text-based installation.

The servers autostart when they finish installing. You may need to reboot the server if your performance monitor data do not appear.

Uninstalling

Use Control Panel to uninstall in Windows. Uninstall by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/uninstall.sh
```

You must uninstall from Linux as root. No graphic wizard appears, and you must respond to the command-line prompts as they appear.

Linux syslog not displaying

Application does not display syslog messages.

On Linux based platforms, under certain circumstances, a race condition at application startup may impact syslog event/messaging functionality. If syslog messages are not displaying as expected, please apply the following **workaround** to restore functionality.

1) Shutdown the webserver.

2) Restart the appserver.

3) Start the webserver after the appserver's status shows 'ready'.

This process may need to be repeated if the server is restarted.

Linux HA does not support IPv6 as default

While IPv6 is supported on Windows HA, Linux HA does not support IPv6 as default. To acquire IPv6 on Linux HA, it's suggested that users must follow these steps enable unicast within the Mediation cluster. Apply the configuration changes to all Mediation servers.

1 Add the property oware.unicast = true to installed.properties file located in .../dorado/owareapps/installprops/lib directory.

2 Locate .../oware/jboss/server/oware/deploy/cluster/jgroupschannelfactory.sar/META-INF/jgroups-channelfactory-stacks.xml.

3 In the TCP section (you can search by <stack name="tcp"), comment this portion:

```
<!--Alternative 1: multicast-based automatic discovery. -->
<MPING timeout="3000"
num_initial_members="3"
mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"
mcast_port="${jgroups.tcp.mping_mcast_port:45700}"
ip_ttl="${jgroups.udp.ip_ttl:2}"/>
```

4 And Uncomment

```
<!-- Alternative 2: non multicast-based replacement for MPING. Requires
a static configuration of all possible cluster members.>
<TCPPING timeout="3000"
initial_hosts="${jgroups.tcpping.initial_hosts:localhost[7600],localhost[7601]}"
port_range="1"
num_initial_members="3"/-->
```

CAUTION:
Make sure you modify stack "tcp" section, not "tcp-sync" section

Example:

```
<!--Alternative 1: multicast-based automatic discovery.
<MPING timeout="3000"
num_initial_members="3"
mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"
mcast_port="${jgroups.tcp.mping_mcast_port:45700}"
ip_ttl="${jgroups.udp.ip_ttl:2}"/>
-->
Alternative 2: non multicast-based replacement for MPING. Requires
a static configuration of all possible cluster members.>
<TCPPING timeout="3000"
initial_hosts="${jgroups.tcpping.initial_hosts:10.35.35.200[7600],10.35.35.201[7601]}"
```

port_range = "1"

num_initial_members = "3"/

Where 10.35.35.200 and 10.35.35.201 are IPaddresses of Mediation servers.

5 Restart Mediation servers. (#service oware stop/start)

Device Prerequisites

Often, devices require pre-configuration before they are manage-able by this software. For example, the management system application server must have access to the device, and often must be listed on the access control list for the managed device.

Common Device Prerequisites

The following are common prerequisites:

Credentials— WBEM credentials have a role in discovering the device. Your system must have access to the computer using Administrative only credentials. These are the same credentials as the user installing WBEM on the device.

Telnet / SSH credentials are necessary for other supported applications.

For full functionality, this WBEM device driver requires administrative (root) access. Many devices may only allow root logins on a local console.

In such cases, configure the Telnet/SSH authentication for these devices to login as a non-root user—and, in Authentication Manager, enter `su` in the *Enable User ID* field and enter the root user's password in *Enable User Password* in that same authentication. This enables full device management functionality with root access.

NOTE:

Credentials for Telnet / SSH should have a privilege level sufficient to stop services and to restart the computer system.

Firewall— Some firewalls installed on the computer may block Web-Based Enterprise Management requests. Allow those you want to manage.

License— Make sure you have the correct WBEM driver license installed. Licenses come in the following types:

- Major Vendor by Name - Such as Dell, Compaq, HP, Gateway.
- Server/Desktop individual license support.
- Generic computers - non-major vendors.
- ALL - this gives the driver all capabilities for any computer system.

Aruba Devices

By default, only SSH interactions work on these devices. If you want to use telnet you have to configure the device through the console or through an SSH session and turn it on.

Cut through or direct access sessions are only supported for SSHv2. You must create an SSHv2 management interface for the device and use it when attempting direct access. If you use SSHv1 the session does not connect (the ArubaOS does not support SSHv1), and if you select telnet, the driver cannot log into the device automatically, and must login manually.

SNMP v2c only supports read operations, not write. SNMP v3 supports both read and write, but not SNMP v3 informs. To manage Aruba devices you must use SNMP v2 or v3. Up to Aruba OS3.1.1.2, SNMPv2c (read-only) and v3 (read-write) are recommended. SNMP v1 does not work correctly.

NOTE:

Although SNMP handles the bulk of the communication with this device, and you must supply the correct SNMP authentication information, some information comes through telnet interaction, so you must supply telnet/SSH authentication too for all device interactions to work correctly.

Backup and Restore

You can backup or restore text files that reflect the *Startup Config*, and *Running Config* as well as backup/restore of a binary *Flash* memory for the selected device. You can compare, store, view and version the text files, and can restore either text or flash memory to the device if you have the File Management option installed.

Because the Aruba mobility controller's flash memory backup is a compressed, binary `.tar.gz` file, the displayed Current Config is not always textual. The flash file is binary, so you cannot view it as text. Nevertheless, you can restore it as long as the backup file has the extension of `.tar.gz` Using this application to backup the flash automatically creates the file with this extension.

Avaya Device Prerequisites

You must do the following for the device driver to function correctly with Avaya devices. Whether you use RTCP or not, do the bullet point setup steps outlined in Setting Up RTCP on page 165, below.

Cut-Through

Avaya Communication Manager uses a special port for telnet sessions. To use the Telnet Cut-thru feature in this software, you must modify the port. You can do this during the discovery process by creating a Telnet authentication object and entering port 5023. Alternatively, once you install Communication Manager, open it from the Resources screen, select the Authentication tab and create a new Telnet management interface with port 5023. When you initiate a Telnet cut-thru session, Customer Manager asks for an emulation type. Select type 4410.

Setting Up RTCP

The following describes setting up RTCP with Avaya devices. Do this on the Avaya Media Server with the Media Server's Management Web Interface using a browser (for example, Internet Explorer) to access the IP address of the media server. For an S8300, S8400, S8500 use the server's IP address. For the S87xx, use the active server IP address—not server A or server B but the active server address. When accessing the web manager, after logging in, navigate to the Maintenance Web Page to see the following menu choice:.

NOTE:

When changing SNMP settings Avaya recommends stopping and restarting the agent.

- Enable SNMP v2 on the device (under *Alarms > SNMP Traps*)
- Ensure the SNMP community strings match on the authentications you have configured and on the device (*Alarms > SNMP Agents*).
- Mediation Server (or Application Server, if enabled as a Mediation Server) must be allowed access on the device, either through its specific IP address(es) or by checking *Any IP address* under *Alarms > SNMP* Agents.
- *Security > Firewall* must have *SNMP, HTTP* and/or *HTTPS*, and *Telnet* and/or *SSH* and *RTCP* enabled both as *Input* and *Output* from the Server. If your system collects SNMP Traps and syslog messages, select those for Output from Server only.
- You must confirm, or start, the SNMP agent (Master Agent) on the device under *Alarms > Agent Status.*

After modifying the alarm and security areas of the web manager, you need to access the *Communication Manager* command line interface (CLI) using telnet, the *Native Configuration Manager* (from the main web management page) or use Avaya's *Site Administration* software. If telnetting to the CLI, choose the `w2ktt` terminal type upon login. You must have a Communication Manager login which may or may not be the same as the web manager login and password.

Execute and change the following:

1 Change **system-parameter ip-options** and specify under RTCP Monitor Server the:
   - Default server IP address = the Application server IP address
   - Default port = Must match what you put in your software
   - Default RTCP Report Period = you can leave at default

- Enter/submit the changes

```
display system-parameters ip-options                          Page 1 of x

                    IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS
   Roundtrip Propagation Delay (ms)     High: 800      Low: 400
            Packet Loss (%)     High: 40       Low: 15
            Ping Test Interval (sec): 20
   Number of Pings Per Measurement Interval: 10

RTCP MONITOR SERVER
                Default Server IP Address:
                        Default Server Port: 5005
          Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
          Link Failure? y


H.248 MEDIA GATEWAY                 H.323 IP ENDPOINT
Link Loss Delay Timer (min):5       Link Loss Delay Timer (min):
                                      Primary Search Time (sec):
                                Periodic Registration Timer (min):
```

2 Change **ip-network-region x** (for every network region that pulls RTCP information)

- On page one, make sure that RTCP Reporting is enabled.
- Under RTCP monitor server Parameters,

  –Use default server parameters (this uses the parameters you set up on the `system-parameter ip-options` form)

  –If you want to specify a separate server IP address, specify it under server IP address and server port

  –Enter/submit the changes.

```
change ip-network-region n                                    Page 1 of x
                          IP NETWORK REGION
  Region: n
Location:                 Authoritative Domain:
    Name:
                            Intra-region IP-IP Direct Audio: n
MEDIA PARAMETERS            Inter-region IP-IP Direct Audio: n
   Codec Set: 1                       IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3028                   RTCP Reporting Enabled? y
                          RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS   Use Default Server Parameters? y
 Call Control PHB Value:                  Server IP Address:   .   .   .
        Audio PHB Value:                        Server Port: 5005
        Video PHB Value:

802.1P/Q PARAMETERS                RTCP Report Period(secs): 5
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 7
                          AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? y
  H.323 Link Bounce Recovery? y            RSVP Refresh Rate(secs): 15
 Idle Traffic Interval (sec): 20       Retry upon RSVP Failure Enabled? y
   Keep-Alive Interval (sec): 5                        RSVP Profile:
            Keep-Alive Count: 5       RSVP unreserved (BBE) PHB Value: 40
```

Brocade Devices

This software will not telnet connect to some devices if they use the factory default password. You must set the password to something other than that default. This software does not recognize the additional prompt asking that default password be changed each time login occurs.

Follow these steps and update firmware on the non-RX devices:

1. Download the firmware update (.zip file) from www.brocade.com
2. Extract that zip file to the download directory of the External FTP file server your system uses.
3. Create an empty file named `release.plist` and load into the OS Image manager portlet.
4. Deploy that image, selecting the device and `release.plist` file loaded in your system. To deploy the image, select the device(s) and select the `release.plist` file in OS Manager.
5. Remove any remaining files before attempting the next Brocade firmware update.

NOTE:

You cannot deploy these updates using this software's internal FTP server.

For RX devices, download and deploy firmware updates as you ordinarily would, registering the OS image in the OS Images manager (see the *OS Images* section of the User Guide), and deploying it to either a device or group with the *action* menu.

BIG-IP F5

Dell OpenManage Network Manager supports the BIG-IP F5 load-balancing appliance and software. It supports the following capabilities, and requires the listed device configurations:

- SNMP—This requires adding the IP address from which you manage the F5 to its Client Allow List under System -> SNMP -> Agent -> Configuration). Supports SNMP-based default device/resync using the ifTable - creates interface sub-components.
- Event Management—SNMP Trap Definitions (Tip: search for event definitions beginning with "big").
- Reports—Run any default Dell OpenManage Network Manager reports against F5 inventory.

Features not supported

- Any CLI-based functionality (NetRestore, CLI Cut-Thru, and so on)
- Link Discovery
- Port creation

Cisco Devices

The following sections discuss prerequisites and limitations of Cisco device management capabilities.

Setup Prerequisites

You must include the *Enable* user ID. Omitted enable user IDs may interfere with correct device management.

You must create Authentication objects for Cisco Switches with an Enable user and password. Otherwise authentication for Interface level DC login sessions fail. The Cisco Router authentication rules automatically send the Enable user/password at the interface level.

For IOS devices, access to various system command modes on the device may be defined by specifying an access privilege level for a user account. Access privilege level 15 is required to access Enable (privileged) mode. This software requires the user account for authenticating with and managing a device has a privilege level of 15.

Ensure that user accounts associated with CLI Authentication objects in your system are configured on the device with privilege level 15. Consult your device's manuals for additional information about configuring this privilege level.

CAUTION:

If you upgrade IOS when you have not copied running-config to Startup-config, provisioning services may fail because of the unexpected device error message below. This message causes "write memory" command to fail. In the application the user may see a message like "failure to terminate telnet session" Device message: *Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image.* **Also:** Currently unsupported: Chassis View, Discrete configuration.

Saving Running-Config to Startup Config

To save the running-config to startup-config whenever the router's configuration is updated uncomment the following in cisco.properties to enable this feature.

```
#cisco.ios.save.running.config=true
```

This copying behavior should not be fatal to the configuration that was updated but a job message displays the failure or success.

NOTE:

Nexus configuration restore to start-up is not supported. When you attempt this, an error including `This command is deprecated` appears on 3000 series devices. On 5000 series, the error is `sysmgr_copy_nvram_dest_action: src uri_type = 1 is not supported yet`. (25242)

Copying to the Device Rather than Your System

You can have backup copy running configurations to the device's disk rather than the system's database. This requires no intervention of FTP since everything occurs on the device itself. The option appears when you change the following properties in the cisco.properties file in `owareapps/cisco/lib:`

```
#flags that enable direct copy run start
cisco.rmc.save.config=false
cisco.backup.save.config=false
```

When these are *true* you can back up running-config to startup-config for Cisco devices. You can select this option in addition to standard backup in the backup configuration screen (choose *running-config* from the File System pick list, and *startup-config* from the File Server Protocol pick list.) You can also trigger it from the *System* > *General* screen's *Save Config* button.

Service/Policy Troubleshooting FAQs

The following sections answer frequently asked questions about Services and Policies.

Service Integrity Check

- When you right-click in the Service or Policies portlet, Maintenance > Integrity Check checks the service targets to see if they are still in the database. Are these targets just physical resources like ports or subinterfaces?

  Whatever the target is for the service, most typically this is the router itself.

- Will Dell OpenManage Network Manager do this check when you invoke it? For example, if an equipment discovery finds a port is gone, will that flag the service as compromised or is it only flagged when Dell OpenManage Network Manager runs the integrity check on the service?

  You must run the service integrity check, Dell OpenManage Network Manager does not connect general device resync with any consequence to services.

About Services Discovery

- Are altered services flagged as compromised if service rediscovery detects services in the network have been changed manually is some way (for example, a different VLAN assignment), or does the Dell OpenManage Network Manager service just get aligned to what is in the network? How would a user know it was different?

  Services in the database get updated to what is found on network. Here are the potential outcomes:

  –If Dell OpenManage Network Manager finds a “provisioned” service in the database, but not on network, the service is flagged as “Not Found.”

  –If data found on network does not pass validation, the service is flagged as “Error”

  –If the data on network is different than what appears in Dell OpenManage Network Manager’s database, Dell OpenManage Network Manager saves the new data and versions the previous configuration, updating the *Last Modified* field. Users can compare/diff versions and revert to previous version through the application. Service Discovery Job/Audit trails log the creation of a new version and that the service was modified.

  Depending on what actually changes, Dell OpenManage Network Manager may create a new service. If a key field changes, then what is discovered is a different service. Dell OpenManage Network Manager cannot distinguish that VRF1 was modified to VRF2. These are therefore

two different services. In such a case, Dell OpenManage Network Manager marks VRF1 “Not Found” and creates a new service, VRF2.

- How do I discover pooled resources into Dell OpenManage Network Manager pools? With service discovery? With equipment discovery? With something else?
  Service discovery, through the creation/update of services maintains the pool allocations used/required by those services. Dell OpenManage Network Manager requires no separate pool discovery.

Adaptive CLI FAQs

- Why share an existing schema from another Adaptive CLI (ACLI) versus creating a new one with each ACLI?
  One reason to use the same schema is to accommodate a complementary ACLIs. For example one ACLI creates an entity and you want a script to remove the same entity. For such examples, the valid values, labels, and so on, for the attributes are always going to be the same in your create and delete ACLIs. Therefore, it is safest to use the same single referenced version of the Schema. You can share the same schema, and your delete script can mark the attributes it does not use as *Not applicable*.

- What is the best practice for exporting ACLIs to import later into another system?
  If you have ACLIs that you need to export so that you can import them into a production system, then the recommended practice is to create a separate file for each ACLI and export them one at a time.

  You can group select multiple ACLIs in the Adaptive CLI Manager and export them to a single file, but this can be difficult to maintain if changes are being made frequently to the ACLIs. Best practice is that only ACLIs directly sharing a common Schema (example a Create ACLI and its complimentary Delete ACLI) be exported to the same file. Keep in mind how to maintain/version/update the ACLIs and associated shared schemas when plotting how to map your export files, and frequently back up your export files to external devices/machines. You can use source control systems version/maintain ACLI export files, since they are in XML format.

- If I change an ACLI’s schema shared by other ACLIs, do I need to do anything to the other ACLIs?
  If you have multiple ACLIs sharing the same Schema, you should be in the habit of retesting the other ACLIs using that schema for to ensure no unintended side effects occur.

NOTICE

Regularly export all ACLIs with the same schema before modifying the schema by editing any of the ACLIs that use it. **Also:** Test your ACLI scripts in a telnet or direct access session with the target device(s).

Server Information

You can see mediation and application server information in JMX Console. The URLs for this console:

- **Mediation Server JMX**: http://[mediation server IP address]:8089/jmx-console/ (for stand-alone mediation servers), or port 8489 for HTTPS.
- **Application Server JMX**: http://[application server IP address]:8089/jmx-console/, or port 8489 for HTTPS.

Some information visible in these consoles:

Is a mediation server active or standby?—Open the JMX console for the mediation server, then click PollingEngine and view the *Active* attribute. If *true* the mediation server is primary, if *false* it is standby.

To which application server is mediation server posting data?—In the mediation server's console, click ClusterPrimaryDesignator and then view the AppServerPartitionName attribute.

List active subscriptions and targets—Click PollingEngine, then invoke the getSubscriptionAndTargetInfo operation.

Is mediation server writing polling results to the spool file?—Click MonitorPollingHandlerMBean and then view the DataBeingWrittenToSpoolFile attribute. While there you can also see the most recent time the mediation server posted data to the application server (item 7) by viewing the MostRecentPostTime attribute.

When does a server skip execution and what is the total number of skips?—Click PollingEngine and then viewing those attributes. While there, you can also see the last time the server rejected execution and the last time that happened.

NOTE:

The jmx-console is a Development tool used for troubleshooting and not accessible to the application user. Please request assistance through Dell support channels to investigate any potential application issues.

Environment / Operating System Issues

The following are items that have historically caused some problems. They may not apply to your environment.

CRON Events

CRON events can update Linux Releases, check for linkage errors and run through other tasks. This should occur when server traffic is generally higher. If necessary, change it to run late during off peak hours.

Potential Problem Processes

auditd— This process logs errors periodically, and can send RESTART or KILL signals to processes outside of its policies. This could be dangerous if configured wrong.

cpuspeed— Throttles down CPU speeds within the Kernel. Since Dell OpenManage Network Manager's Java runs in a VM it is unaware of sudden increase/decrease in CPU speeds, and this could pose issues in threading and calculating thread counts.

SELINUX

This should be disabled. To check, run the following:

```
[root@AppRedcell01 bin]# selinuxenabled && echo enabled || echo disabled
```

To fix this, if it indicates it is enabled, modify the `/etc/selinux/config` and change `targeted` to `none` so this is preserved on reboots.

Hardware Errors

A fragment found in `dmesg`, triggered further investigation. This detected memory errors.

```
[Hardware Error]: Machine check events logged
Errors found in /var/log/mcelog:
Hardware event. This is not a software error.
MCE 0
CPU 30 BANK 9
TIME 1370474184 Wed Jun  5 17:16:24 2013
MCA: MEMORY CONTROLLER GEN_CHANNELunspecified_ERR
Transaction: Generic undefined request
STATUS 900000400009008f MCGSTATUS 0
MCGCAP 1000c18 APICID c0 SOCKETID 3
CPUID Vendor Intel Family 6 Model 47
```

DNS Does Not Resolve Public Addresses

DNS must permit application servers to resolve public DNS names like google.com. Web server needs this to determine its public facing interface by determining which route the packet went out on quick test.

Raise User Limits

If User Limits are low on the Application Servers and possibly Mediation Servers, these can impact threading and normal server behaviors.

Web Server

The memory configuration (heap min/max) should also be the same for all server environments.

Portal Memory Settings

To manually change the web portal heap settings, change the `setenv.sh` (Linux) or `setenv.bat` (Windows) file:

```
set "PORTAL_PERMGEN=512m"
set "PORTAL_MAX_MEM=3072m"
set "PORTAL_INIT_MEM=768m"
set "PORTAL_32BIT_MAX_MEM=768m"
```

These files are in the `Tomcat***/bin` directory. For Linux, restart the portal service to apply new memory settings. In Windows, besides updating `setenv.bat` you must run `service.bat update` in that same directory.

(The *User Guide* has much more about setting memory / heap sizes.)

You can increase these to even higher figures if your system has the memory available.

NOTICE

Make sure only one Tomcat process is running, otherwise your web server may exhibit poor performance.

Post Upgrade Web Portal Problems

After applying patches, restarting processes or other recent activity, web portal exhibits undesired behavior like the following:

- Displaying pink bar in application portlets indicating applications are `temporarily unavailable`.
- Message in application portlets indicating `resource unavailable`.
- Actions screen does not appear after right-click device and choosing *Actions*.

- Inability to expand containers or previously selected container expands when clicking another container.

Solution: These, and other symptoms, can stem from browser caching or attempting to login too soon after starting the application. To resolve, try waiting and/or clearing the browser cache.

Clustering

You must enable Clustering on multiple web servers, otherwise index and users become out of sync. To solve this: enable clustering on the web servers by turning on cluster properties found within `synergy/conf/server-overrides.properties`

Upgrade Installations

The following outlines tasks to execute when you are updating your drivers, extensions or license. Refer to Upgrade / Data Migration Fails on page 123, Post Upgrade Web Portal Problems on page 173 and the *User Guide* for instructions about how to prevent and/or handle upgrade problems that can occur.

Patch Installation

Updating Driver Patches

1. Shut down your system.
2. On the application server designated as `oware.config.server` in `[installation root]/owareapps\installprops\lib\installed.properties`, copy the update file with the `ocp` or `ddp` extension to the `owareapps` directory.
3. Open a shell or command prompt, and Source the oware environment (Windows: `oware`. Linux: `. /etc/.dsienv`), and execute the following command lines:
4. `cd $OWAREAPPS`
5. `ocpinstall -x <ocp/ddp filename>`
6. `ocpinstall -u <ocp/ddp filename>`
7. `ocpinstall -s <ocp/ddp filename>`

Repeat steps 1 - 5 on any secondary application or mediation servers.

Adding or Updating Extensions

1. Copy extensions to the extensions folder: `[Installation root]\oware\synergy\extensions`
2. Restart web portal (Synergy) process.

Synergy Portal Updates (netview.war)

CAUTION:
Do this when no users are on the system. Apply this to all web servers.

With the portal running and the tomcat catalina log being tailed:

1. Navigate to `[Installation root]/oware/synergy/tomcat-x.x.xx/webapps` and delete the `netview` directory. After a brief pause you should see it being undeployed in the log.
2. Drop the new `netview.war` into the directory `[Installation root]/oware/synergy/deploy`. Wait a few minutes and you should see it hot deploy the new WAR file and load registry items.
3. After this is deployed, shut down the web servers.

CAUTION:
Ensure no old copies of netview.war remain in the [Installation root]/oware/synergy/deploy folder. This software automatically deploys any files in this folder. This will cause a conflict.

Synergy Portal Updates (NetviewFactory.war)

1. Shutdown your system (both webserver/appserver processes).
2. Navigate to `[Installation root]/oware/jboss-x.x/server/oware/deploy`. Apply `NetViewFactory.war` by overwriting any existing version with the new one.

License Installation

1. Stop the application or mediation server.
2. Rename the old license file (`[Installation root]\license.xml`)
3. Copy the new license file to your installation's root.
4. Rename it to `license.xml` if it is named anything else.
5. Open a shell and cd to your installation root.
6. Source the application's environment (Windows: `oware`. Linux `. /etc/.dsienv`)
7. Type `licenseimporter license.xml`

SMTP Mail Sender

If you require a sender / reply to e-mail address on mail sent, you can configure that with the following property (as always, it's best to override in `owareapps/installprops/lib/installed.properties`)

```
redcell.smtp.returnaddress.name
```

4

Performance Management (PM) Best Practices and Sizing

If you are going to use the optional Performance Management (PM) capabilities of Dell OpenManage Network Manager, the following describe considerations best practices and installation for those capabilities.

PM Best Practices

The following are best practices for PM:

- Follow the PM Sizing Guidelines

PM Sizing Guidelines

See Best Practices: Single Server Hardware on page 14 for sizing parameters. The following are general recommendations for sizing

Fault Management—Assumes sustained trap traffic does not exceed 1200/sec when using a single 7200RPM drive. Faster drives or disk arrays can manage higher trap throughput.

Performance Management—Sizing depends on the monitor intervals, number of monitors and attributes within each monitor. Dell OpenManage Network Manager supports this data at 300 to 600 database insertions per second (for 7200 to 15000 rpm drives respectively). Every attribute is considered 1 insertion. For and example an ICMP monitor has 3 attributes so also has 3 insertions for the selected monitoring interval.

Traffic Flow Analysis—Database lags limit performance for this Dell OpenManage Network Manager capability—the software is faster than the hardware. Traffic Flow Analysis supports a maximum of 300 to 600 inserts per second (7200 to 15000 rpm drives respectively). Actual Insert rates are highly variable and depend on how devices are configured for flows. Current licensing limits Traffic Flow Analysis exporters to 20 but this is arbitrary since one exporter can generate so much data it overwhelms the system. Alternatively100 exporters can generate minimal data and still have good performance.

NOTE:

15k drives can support 3000 inserts / 5 sec on a Mysql db. In this scenario network lag and device response are not considered. So, actual results will likely be slower.

Types of deployment available: single-server, HA. Consider the following in these architectures:

- Hardware sizing & selection
- Database sizing & selection
- Scalability considerations for each Monitor type (monitor protocols – SNMP, Telnet, WMI, etc.)
- User tunable/configurable parameters within Dell OpenManage Network Manager and/or APM
- Examples of monitored environments (central-centric, branch office, etc.) – basic and advanced, polling intervals, roll-up intervals, etc.
- PM data export (how to extract needed PM data for 3rd-party use)

5

Clustering

Clustering transparently balances the computing load for this application's EJB components—rule engine, scheduler, logger, Business Object Manager (BOM), workspaces and mediation. This is especially beneficial for the applications' communication with the database storing its business data.

By default, this application supports the distribution of its processes. It distributes the load per client (not per request). To make a genuine highly available system, you must cluster application servers, mediation servers, and database servers (Oracle RAC). Consult your sales representative for the licensing requirements for fail-over, or high availability clustering.

The following are some of the benefits of clustering:

- Elimination of bottlenecks and single-point failures—Clustering servers distributes computing tasks, and enhances performance. Replication protects your application and users' state to ensure that the failures—like server crashes—can be fully masked from the user and application.
- Transparency to your applications and application developers—developers do not have to deal with intricacies of replication and load balancing. This means developers do not have to modify their application components to run in a clustered environment.
- Hardware and OS independence—You can use clustering across disparate hardware and operating system platforms.

Dell OpenManage Network Manager Deployment Architecture

Dell OpenManage Network Manager supports two primary deployment models:

Single-Server—The full application is installed on one server.

Clustered/HA—multiple servers of each type may be used for performance gains or to achieve High Availability.

The Dell OpenManage Network Manager platform software architecture consists of the following principal run-time software components:

Web Server—Eliminates the need for a separate Java client interface. Deployments that have more that one web server or application server also require a load balancer.

Application Server—The system's central processing unit. It executes application business logic. You can deploy it in both fault tolerant (Master/Slave) and cluster configurations to limit downtime and optimize performance.

Upgrading application server first, if you are using the embedded database, also upgrades the database, if necessary. It's often easiest to install application server first simply because this upgrade impacts any other application servers too, if they are clustered.

Database Server—Like the Application Server, you can deploy the Database Server in a fault tolerant configuration to eliminate data loss during a system failure and to ensure data integrity. This configuration typically uses Mysql replication or Oracle RAC. You can cluster the Oracle database servers. See Installing Oracle on page 213. References to database servers below apply to all supported databases.

Mediation Server—Mediation Server manages the communication between the Dell OpenManage Network Manager and the network elements. Like the application and database servers, you can deploy mediation servers in a fault tolerant master/slave configuration to maintain constant communication with the network elements. You can make mediation servers highly available.

NOTE:

If Mediation Servers or clients are outside a firewall from the Application Server, you must disable multicast connections to Application Servers. See Disabling Multicast on page 184.

Load Balancer (Proxy)—Deployments where many users access the system concurrently may require a Load Balancer, also known as a Proxy, to manage traffic to multiple Web Servers. If one web server is overloaded or un-responsive, the Load Balancer directs users to a responsive Web server. Single-server installations do not require a Load Balancer.

All deployments with multiple application servers require an additional load balancer for application servers too. This ensures that active web servers always direct traffic to an available application server in the cluster. If the current application server is unresponsive, the load balancer re-directs the web server to another application server.

With the proper configuration the same load balancer can serve both web server and application server. See Using Load Balancers on page 190 for more.

Data Flow

Clients access the Dell OpenManage Network Manager system through a web browser. The system routes requests to web server(s) to a proxy device (load balancer [LB]) that routes traffic to a suitable application server. Application server returns data retrieved from the database. If an application needs to communicate with managed devices, a mediation server handles the task. The mediation server retrieves the data from the device, and sends it to the application server. Application server processes, then stores the data in the database.

Cluster/HA Constraints

This section describes the constraints within which a cluster configuration must work.

- All servers in a cluster must be on the same local area network (LAN), be reachable for IP v4 multicast, and must have unique names. Clustering is *not* designed for servers in different time zones (however, you can have mediation agents send data from distant locations). For an exception to the multicast requirement, and for managing servers and clients outside firewalls, see Disabling Multicast on page 184. You will need to use unicast instead of multicast when cluster member nodes are on different IP subnet.

  To ensure that application server nodes do not miss server-to-server heartbeats that may erroneously initiate fail-over processes, you must connect clustered application servers via a LAN with maximum latency of 100ms. That said, you can put clustered server nodes several miles/kilometers apart, as long as the connection does not exceed the maximum latency (using Fibre ethernet, for example). WAN connectivity is not recommended.

NOTE:

Although high-speed interconnects may be able to increase the distance of application server nodes to over 5km, the High-Availability solution is not designed for disaster recovery situations. Dorado Software recommends the use of a separate Redcell deployment located at the disaster recovery location to be used as a cold standby system. The database of the primary system should be copied to the disaster recovery standby system on Real-time or on regularly scheduled intervals(Database Dump). Application servers can be replicated by software like VEEAM, Avamar etc. database Server to be replicated by oracle data guard(Real-time) or MySQL Replication(Real-time).

- All servers must run the same version of the application and listen on the same port.

NOTE:

The heartbeat between mediation and application servers now contains the software version information. If the versions do not match, then Dell OpenManage Network Manager generates an event/alarm to indicate the issue.

- You must identically configure all servers running Enterprise JavaBeans (EJBs) with Java Database Connectivity (JDBC) connection pools.
- For clusters using database connection pools, each cluster member must have an identical connection pool. See Database Connections on page 182 for more details.
- The Access Control Lists (ACLs) and servlets must be identical for every machine serving servlets.
- All servers must have identical service configurations. You cannot, for example, turn on mediation services in some cluster application servers and not others.

- Database servers can always be separate, no matter how you configure the other machines. You can make a database machine part of an application server cluster/partition, but this is not recommended.

  NOTICE

  For non-embedded database installations (Oracle) best practice is keeping the database server(s) separate from the other machines.

- Although application servers process more than just mediation, any application server can also run mediation services. Stand-alone mediation servers themselves run *only* mediation services. You can also turn mediation on and off on any host running an application server. If you cluster application servers, one or more distributed mediation servers typically handle mediation, and the clustered application servers have mediation turned off.

  As stated above, you can also run both the application server and mediation services on a single machine. A cluster of such combined application / mediation machines is also possible—minimally two servers each running an application server with mediation services.

  One caveat: Mediation processes have an impact on application server performance. This is why best practice for larger deployments is to distribute mediation services to dedicated mediation servers. Once you distribute mediation, you can ensure better performance by disabling mediation on application servers in the application server cluster.

- SNMP Mediation agents can back each other up as primary/secondary for any subnet (any range of IP addresses). A mediation agent which is primary for one subnet can be secondary for a different one. Such subnets may not overlap.

Database Connections

By default each deployed application server has 60 database pool connections available. In cluster/HA systems, size connections by multiplying the number of application servers deployed in the system by 60 to get a starting point for the total number of required database connections.

NOTE:

This is just a general starting point and as demand on the system grows, various web and Dell OpenManage Network Manager components requiring connections naturally increase.

The database connection pools configuration file locations for Oracle and MySQL appear below with their default max connection pool sizes. These numbers determine the overall pool requirements per application server.

Oracle database file locations:

Oware connection pools

```
/oware/jboss-5.1/owareconf/oracle-ds.xml
    corepool uses default max-pool-size (5)
```

```
        jobpool uses default max-pool-size (10)
        userpool uses default max-pool-size (25)
```

Performance connection pools

```
   /owareapps/performance/server/conf/pm-oracle-ds.xml
     pmpool uses default max-pool-size (10)
```

Dell OpenManage Network Manager connection pools

```
   /owareapps/redcell/server/conf/rc-oracle-ds.xml
     eventhistory pool uses default max-pool-size (10)
```

MySQL database file locations:

Oware connection pools

```
   /oware/jboss-5.1/oware/conf/mysql-ds.xml
        corepool uses default max-pool-size (5)
        jobpool uses default max-pool-size (10)
        userpool uses default max-pool-size (25)
```

Performance connection pools

```
   /owareapps/performance/server/conf/pm-mysql-ds.xml
     pmpool uses default max-pool-size (10)
```

Dell OpenManage Network Manager connection pools

```
   /owareapps/redcell/server/conf/rc-mysql-ds.xml
     eventhistory pool uses default max-pool-size (10)
```

To calculate total number of connections:

Add the number of pool connections per server times the number of deployed servers. That equals the total number of maximum database connections

For example, the suggested total for HA system which has two application servers is 2 x 60 = 120 connections. Again, this is just a general starting point and to account for a natural increase in database connections. Best practice here would be to increase that number by at least a factor of at 5 for a total of 600 connections.

MySQL's online support suggests that you can create as many as 10,000 connections depending on the amount of RAM available: "Linux should be able to support at 500 to 1000 simultaneous connections routinely and as many as 10,000 connections if you have many gigabytes of RAM available and the workload from each is low or the response time target undemanding."

Oracle Database Connections

You may need more connections for Oracle since it can recursively consume database connections internally. Refer to the following for more about this: http://tech.e2sn.com/oracle/oracle-internals-and-architecture/recursive-sessions-and-ora-00018-maximum-number-of-sessions-exceeded

Notifying Users of Lost Database Connection

In the `owareapps\installedprops\installed.properties` file, you can configure the application server to send e-mail when it loses connection to the database. Here are the properties to insert:

```
redcell.smtp.host=mail_server.com
redcell.smtp.authentication.enabled=true
redcell.smtp.authentication.username=user@company.com
redcell.smtp.authentication.password=password
redcell.smtp.recipients=user_1@company.com
redcell.smtp.subject.message=Lost DB connection ### optional
redcell.smtp.message=Call 911!!!! ### optional
```

The contents specified above are examples.

Disabling Multicast

Disabling Multicast for a Standalone Server

Multicast is enabled to facilitate communication between servers in distributed, multi-server installations. If your system is a standalone server, it may be useful to disable this feature to reduce performance delay. Follow these steps to disable multicast.

1. Stop appserver

2. Add the property oware.unicast = true to installed.properties file located in `.../dorado/owareapps/installprops/lib` directory

3. Locate `.../oware/jboss/server/oware/deploy/cluster/jgroups-channelfactory.sar/META-INF/jgroups-channelfactory-stacks.xml`

4. In the TCP section (you can search by <stack name = "tcp"), comment this portion:

```
<!--Alternative 1: multicast-based automatic discovery.-->
<MPING timeout = "3000"
num_initial_members = "3"
mcast_addr = "${jboss.partition.udpGroup:230.11.11.11}"
mcast_port = "${jgroups.tcp.mping_mcast_port:45700}"
ip_ttl = "${jgroups.udp.ip_ttl:2}"/>
```

5. And Uncomment

```
<!-- Alternative 2: non multicast-based replacement for MPING. Requires
a static configuration of *all* possible cluster members.>
<TCPPING timeout = "3000"
```

```
initial_hosts="${jgroups.tcpping.initial_hosts:localhost[7600],local
host[7600]}"
port_range="1"
num_initial_members="3"/-->
```

CAUTION:
Make sure you modify stack "tcp" section, not "tcp-sync" section

Example:

```
<!--Alternative 1: multicast-based automatic discovery.
 <MPING timeout="3000"
 num_initial_members="3"
 mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"
 mcast_port="${jgroups.tcp.mping_mcast_port:45700}"
 ip_ttl="${jgroups.udp.ip_ttl:2}"/>
-->
 Alternative 2: non multicast-based replacement for MPING. Requires
 a static configuration of *all* possible cluster members.>
 <TCPPING timeout="3000"
 initial_hosts="${jgroups.tcpping.initial_hosts:localhost[7600],local
 host[7600]}"
 port_range="1"
 num_initial_members="3"/
```

6. Start appserver

Disabling Multicast within a Cluster

Disabling multicast may be useful if a firewall exists between application servers or mediation servers that must discover each other. (See also Configuring the Cluster's Multicast Address on page 194.) Application-to-mediation server communication does not use multicast, although mediation-to-application server does, unless disabled.

To disable multicast communication between application and mediation servers, define the property `oware.application.servers` in the `installedprops/medserver/lib/installed.properties` file and the property should point to the application server ip address and should be in the following format:

```
oware.application.servers=<application server ip address>
```

If the mediation server is communicating to a cluster of application servers then the value should define all the application servers separated by a comma For example:

```
oware.application.servers=<application server A ip address>,<application
   server B ip address>
```

Define this property on all mediation servers.

This configuration change is only for application and mediation server communication. The mediation servers in a cluster/HA still use multicast between themselves. If you use `oware.application.servers`, you must (comma-separated) list all available servers wherever you use it to bypass multicast.

NOTICE

If you make a mistake in installing portions of your cluster, remember you must either re-source the Oware environment, or delete all files in `oware/temp` (and restart the process in question) before changes can be effective.

CAUTION:

Multicast is still required between the cluster mediation servers, or application servers in a cluster unless you follow the instructions in the next section.

You can disable Multicast and using Unicast within a cluster. To do that, you must add this line to the `installprops\lib\installed.properties` file:

```
oware.unicast=true
```

And in file `jgroups-channelfacotry-stacks.xml` in `$OWARE_ROOT/jboss-x.x/server/oware/deploy/cluster/jgroups-channelfactory.sar/META-INF/` change the following:

CAUTION:

Make sure you modify stack “tcp” not “tcp-sync”

Comment this portion:

```
<!--Alternative 1: multicast-based automatic discovery.
<MPING timeout="3000"
num_initial_members="3"
mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"
mcast_port="${jgroups.tcp.mping_mcast_port:45700}"
ip_ttl="${jgroups.udp.ip_ttl:2}"/>
-->
```

Uncomment this portion:

```
<!-- Alternative 2: non multicast-based replacement for MPING. Requires a
   static configuration of *all* possible cluster members.>
```

```
    <TCPPING timeout="3000"
   initial_hosts="${jgroups.tcpping.initial_hosts:localhost[7600],localhos
   t[7600]}"
    port_range="1"
    num_initial_members="3"/-->
```

Example:

```
<!-- Alternative 1: multicast-based automatic discovery.
<MPING timeout="3000"
    num_initial_members="3"
    mcast_addr="${jboss.partition.udpGroup:230.11.11.11}"
    mcast_port="${jgroups.tcp.mping_mcast_port:45700}"
    ip_ttl="${jgroups.udp.ip_ttl:2}"/>
-->
Alternative 2: non multicast-based replacement for MPING. Requires a static
   configuration of *all* possible cluster members.-->
    <TCPPING timeout="3000"

   initial_hosts="${jgroups.tcpping.initial_hosts:192.168.53.15[7600],192.
   168.53.16[7600],192.168.53.17[7600]}"
    port_range="1"
    num_initial_members="3"/>
```

CAUTION:
Unicast depends on configuring this file. Upgrade overwrites it. If you upgrade, copy the file configured as you might like to a separate location, then return it to its correct location.

Synergy Web Server Clustering

If your system deploys multiple web servers, cluster them to work more efficiently. Enabling clustering keeps events, indexes and documents in sync between servers in case of a Node failure. Configure the following to have a successful clustered environment:

- Point all nodes to the same Portal Database or database cluster.
- Make Documents and Media repositories accessible to all nodes within the cluster.
- Configure search for replication.
- Replicate cache across all nodes of the cluster.
- Synergy versions should be the same since they share a database and the schemas must match the runtime environment for each node.
- Each server should be within the same network and able to access each other without restrictions. Disable any firewall between nodes.

- Use a load balancer to delegate traffic through out the clustered nodes allowing web browsers to point to a single host/ip (load balancer). See Using Load Balancers on page 190.

Most of these settings are properties to set within the `server-overrides.properties` file in the `synergy/conf` directory. This file preserves property overrides on upgrade.

NOTICE

Online colleagues only appear when they are connected to same web server in a load-balanced situation when clustering is incorrectly configured.

Web Server Clustering Setup

The following describes tasks needed to move existing files to the common share and basic properties which you must enable to turn on clustering. You must shut down Dell OpenManage Network Manager during this process.

Common Documents and Media Share Setup

1. Set up a network share location dedicated to store the documents and media. If you are unsure how to do this consult with your network administrator and ask him/her to setup a share that can be mounted across the clustered nodes. Each operating system type is different and this is standard network setup, not covered in this document.
2. Mount the new share on each node within the cluster.
3. If you used a single server setup previously or multiple servers without clustering, locate the original or first node in the previous setup and do the following:
   a. Navigate to the nodes `<installdir>/oware/synergy/data` directory and copy the `document_library` to the share. If an `images` directory exists, copy that too.
   a. If other nodes were previously running then do the previous step (a), but copy/merge the contents to produce a merged view

You should now have a directory structure of `SHARE/document_library` and (if it existed during the steps above, `SHARE/images`).

Property Configuration

Do the steps below on each node within the cluster. Start with the first node and repeat the same steps until complete.

Edit the Property File

1. Navigate to the `<installdir>/oware/synergy/conf` directory

2 If you have an existing `server-overrides.properties` file then you can edit it here. If not rename or copy the `server-overrides.properties.sample` to `server-overrides.properties`. Edit the new `server-overrides.properties` file.

3 Locate the Clustering section within this file. If you do not have a clustering section or some of the properties mentioned below do not exist, you can edit the `.sample` file and copy the updated section into the `.properties` file. You can also add the properties mentioned below. Installation updates the sample file with the most current comments and newer properties. The `server-overrides.properties.sample` file is a reference template.

Turn on Clustering and Index Replication

1 Turn on Clustering: Uncomment or add the `cluster.link.enabled` and make sure its value is `true`.

2 Turn on Index Replication: Uncomment or add the `lucene.replicate.write` property, and make sure its value is `true`.

Set the Share Path

1 *Document Library Share*: Uncomment or add the `dl.store.file.system.root.dir` property. The value should point to the `/path/to/share/document_library` or, for Windows, if your share was drive G: then this entry would be `G:/document_library`

2 *Legacy Images Share*: Uncomment or add the `image.hook.file.system.root.dir` property. The value should point to the `/path/to/share/images`, or, for Windows, if your share was drive G: then `G:/images`. Even if you had no `images` directory copied previously, you still need this property and the system creates the directory when needed.

Your property setup is now complete. Save the file and do the same for each Node within the cluster.

Start the Nodes

You have now mounted the common share on all server nodes. Each server should have clustering and Lucene replication enabled along with the share paths for the document library and legacy images within the `server-overrides.properties` file for each server. You can now start each server. Start the nodes one after the other so each node has time to adapt to the new setup. During the startup extra log entries should appear referring to members joining or other nodes found.

Disable Multicast and using Unicast within a webserver cluster

1 Create or copy the unicast.xml to

$OWARE_ROOT/synergy/tomcat-7.0.40/webapps/ROOT/WEB-INF/classes

The unicast.xml can be found at https://web.liferay.com/web/fimez/blog/-/blogs/configuring-a-liferay-cluster-and-make-it-use-unicast-

2 Add following to $OWARE_ROOT /synergy/conf/server-overrides.properties

cluster.link.channel.properties.control = unicast.xml

cluster.link.channel.properties.transport.0 = unicast.xml

ehcache.bootstrap.cache.loader.factory = com.liferay.portal.cache.ehcache.JGroupsBootstrapCacheLoaderFactory

ehcache.cache.event.listener.factory = net.sf.ehcache.distribution.jgroups.JGroupsCacheReplicatorFactory

ehcache.cache.manager.peer.provider.factory = net.sf.ehcache.distribution.jgroups.JGroupsCacheManagerPeerProviderFactory

net.sf.ehcache.configurationResourceName.peerProviderProperties = file = /unicast.xml

ehcache.multi.vm.config.location.peerProviderProperties = file = /unicast.xml

Using Load Balancers

Dell OpenManage Network Manager's web server(s) is (are) between application servers and clients. To add high availability-like capabilities a web served application system, you may use an open-source load balancer like HAProxy either between the web servers and application servers, or between clients and web.

For high availability (HA) installations, systems typically use pairs of load balancers. Dell OpenManage Network Manager needs at least one load balancer pair to distribute loads among webservers. The load balancer IP is what clients connect to. If webserver and appserver are on same machines, all web servers can point to 127.0.0.1 to use their own local appserver. If webserver and appserver are on different machines, they must have another load balancer pair to distribute loads among appservers. All web servers then point to the appserver load balancer IP.

Load Balancer recommended hardware (or equivalent)

Configure your minimum hardware based on the expected number of connection per second:

- Less than 10000 connection/ sec 1 GB RAM, 2GB HD, Atom processor
- Up to 20000 connections/sec 4 GB ram, 10GB HD, Core DUO processor.

Deployments vary based on application usage, system availability and redundancy needs. Deployment recommendations depend on system sizing factors discussed in the Sizing section.

Refer to Best Practices: Single Server Hardware on page 14 for hardware recommendations.

HTTPS Support with Load Balancer

The industry norm is to configure the load balancer to handle SSL Offloading (SSL Termination). In this configuration SSL secures communication from the client browser to the load balancer/ firewall, but communication from the load balancer / firewall to the web servers is not. There are a number of benefits to this type of configuration, the most prominent being ease of management, since users only have to purchase and manage one certificate per load balancer instead of one per web server. Performance also improves since the individual web servers are not impacted with encryption/decryption overhead.

To configure Load Balancer to support a secure web connection, additional properties need to instruct the portal that a front end termination point exists. To do this, in the `oware/synergy/conf/server-overrides.properties` add the following:

```
# The HTTPS Port that the load balancer is listening to, Default is 8443
web.server.https.port=8443
# The Protocol used by the load balancer
web.server.protocol=https
# The Port that Synergy is listening on
portal.instance.http.port=8080
```

After setting these properties, restart Dell OpenManage Network Manager. You can fully login and use the Portal in SSL on 8443 even though the server is running on 8080 internally, before it reaches load balancer.

See the *User Guide* for instructions about implementing HTTPS on a single server installation.

Verifying Clustered/HA Installations

The following example tests load balancing between servers (web server + application server). Here is the configuration:

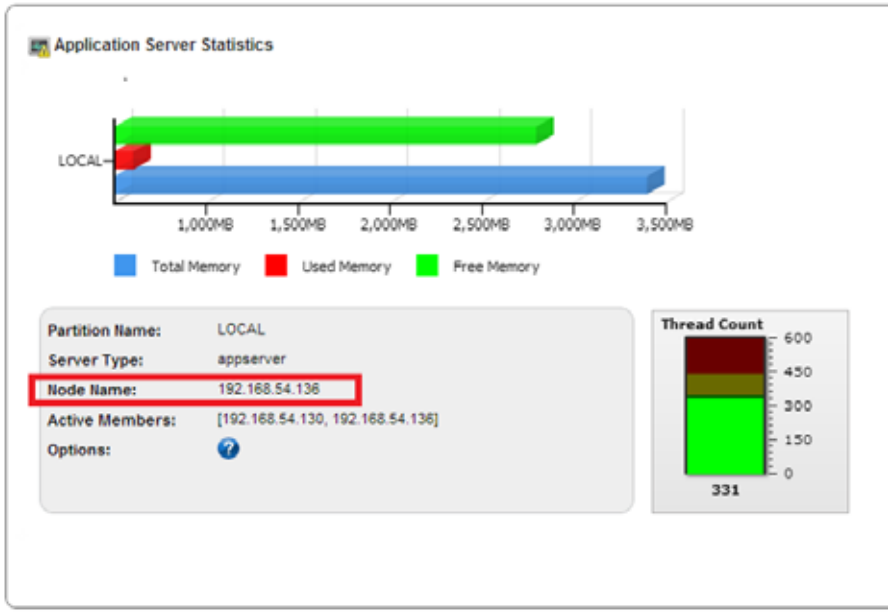
- Server 1 hosts first web server + appserver
- Server 2 hosts second web server + appserver
- User A connects to load balancer from distinct IP and Resyncs a device
- User B connects to load balancer from distinct IP and Resyncs a device

Several verifications are available, including the following:

- Verifying Application Server
- Verify Application Server Redundancy Fail Over
- Validate Mediation Server

Verifying Application Server

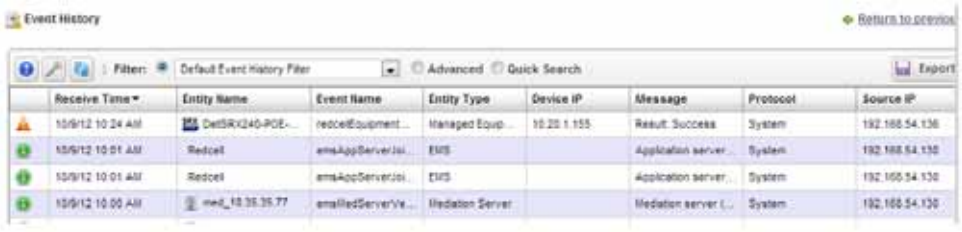
In the Application Server Statistics portlet, you can see to which application server node the logged in user connects.



When different users, for example, resync a device or deploy a service, the expectation is that they would use different web server + appserver hosts. That is, user A connects to server1 and user B connects to server 2 and user C connects to server 3, and so on.

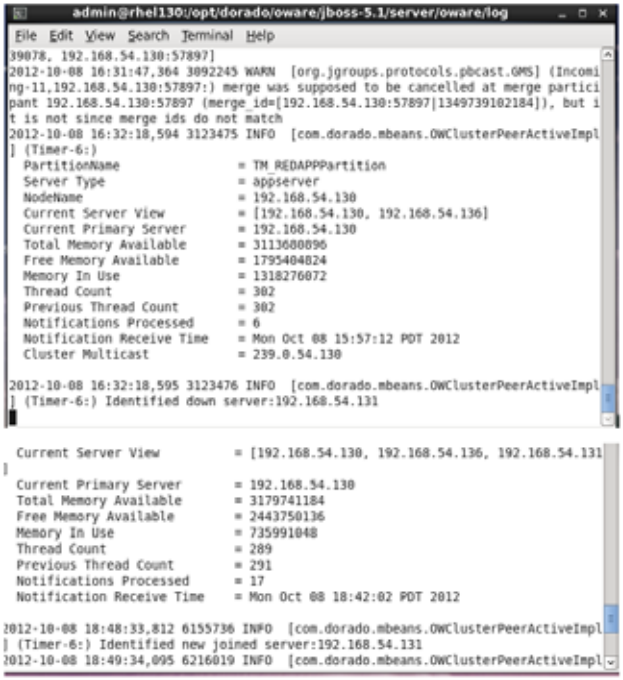
To validate this follow these steps:

1. In Managed Resource portlet, right click and resync a device.
2. Go to the Event History portlet and maximize it.
3. Go to the Columns tab in the *Settings* menu and click on *Show* for Source IP'.
4. The Source IP indicates which server did the Resync action.



Verify Application Server Redundancy Fail Over

On one of server, go to directory `/opt/dorado/oware/jboss-5.1 /server/oware/log`, open a shell, type `/etc/.dsienv` (on Windows type `oware`), and then `tail -f server.log`.



Observe changes to the log when one other cluster member goes down/up by unplugging/re-plugging the network cable or (disable/re-enable network connection).

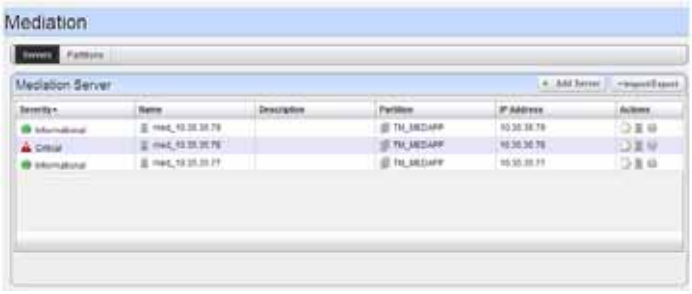
Validate Mediation Server

On one of server, go to directory `/opt/dorado/oware/jboss-5.1 /server/oware/log`, open a shell, type `/etc/.dsienv` (or `oware` in Windows), and then type `tail -f server.log`.[1]

Observe when one other member goes down/up by unplug/re-plug the machine cable or (disable/re-enable network connection).

1. When devices try to use mediation servers, the mediation cluster assigns that mediation server to the device using a round-robin method. The same mediation server handles that device thereafter. To see which medserver the device is using, enable debug on all mediation servers. See the *User Guide* for instructions about how to do that.

You can also observe medserver status within the Mediation panel in Control Panel. When a mediation server goes down you should see its severity turns to Critical..



Configuring the Cluster's Multicast Address

The installation process sets this application's multicast address automatically. Multicast must handle the communication between elements of a cluster—whether application or mediation servers. You can disable multicast discovery of servers (mediation server to application server) or clients (client to application server[s]) as described in Disabling Multicast on page 184.

The range for multicast as defined by the *Host Extensions for IP Multicasting [RFC1112]* is from 224.0.0.0 to 239.255.255.255. The following is an excerpt from the article *Internet Multicast Addresses* that should be considered when assigning addresses:

"The range of addresses between 224.0.0.0 and 224.0.0.255, inclusive, is reserved for the use of routing protocols and other low-level topology discovery or maintenance protocols, such as gateway discovery and group membership reporting. Multicast routers should not forward any multicast datagram with destination addresses in this range."

Use an address above 225.0.0.0, like the one cited in the example above.

Application servers in a cluster use multicast to determine when a peer has come up or when one goes down. This communication usually has to be done in a matter of seconds or even milliseconds and should probably be exclusive on the multicast channel chosen. In other words, best practice is to use a multicast address exclusively for a cluster. Do not use the same multicast address for two clusters and do not use the same multicast for other multicast communication.

If a cluster member asks a running peer to respond but the traffic on the channel prevents a response within the designated timeout, then the requesting member concludes the running peer is gone and takes appropriate fail-over action, even if the peer is running without problem. This can be the source of undesirable behavior from your cluster. For example, it could initiate the rule resynchronization process on the cluster.

Starting Clusters/HA Durably

Clusters provide failover protection for the processes they maintain, or "high availability." To automate restarting this and other applications' processes, install the application with process monitor. To configure process monitor to start and stop clusters if you have not installed electing autostart, you must modify the `owareapps/lib/installprops/lib/installed.properties` file with a text editor.

Starting, stopping and managing such installations uses the following scripts:

- `pmstartall` (or `startpm`[1])
- `pmstopall`
- `pmgetstatus` (displays the system's status as proccess monitor knows it.)

The command line includes the host IP address and port:

```
pmstartall -h <server IP> -p <port>
```

Defaults are for server IP and port are localhost and 54321. (Though you can use the host name, best practice is to use the server IP address.) To see all available command line options, run the above commands with `-?` as a parameter.

You can override the administrative port of Process Monitor (originally in the property file `owmisc.properties`) by setting the property `com.dorado.core.processmonitor.remoteCmdPort` to the desired numeric value. If this port number is changed, all process monitor clients must send requests to the changed port number value.

CAUTION:
If you start a server in a remote shell, killing the shell can kill the server process.

pmstartup.dat

The text file `/oware/lib/pmstartup.dat` manages restart frequency if your application server starts automatically. For more information about using this file, consult the comments within the file itself.

Recovery Procedure

The procedure for recovery from server failure is automated. If something other than server failure is at the root of a cluster's failure, you must stop any running server the process manager, as follows:

```
pmstopall <hostname> <port>
```

The process manager automatically restarts the failed server.

1. **Tip**: It's often helpful to add nohup to this command line

Temp Directory Deletion

Starting your application server may be inhibited by corrupted files in `\oware\temp\`. This is identified when the application / mediation server does not start successfully and reports a probable JMS startup failure. Delete the contents of the `oware\temp\` and restart. Unfortunately, when this directory's contents are deleted and you are using a cluster, you must restart the entire cluster.

System Backup

This is typically something the installing customer does:

1 Perform a system backup of the following Servers

If the Dell OpenManage Network Manager upgrade of the server(s) is not successful, a full system restore will be required. This backup ensures that the system is consistent before any upgrade or patching. Therefore a full system backup is important for each server before the Dell OpenManage Network Manager software upgrade or patching exercise.

Servers:

Backed Up	Application Server Name
❑	
❑	
❑	
❑	

Backed Up	Mediation Server Name
❑	
❑	
❑	
❑	

2 Perform a system backup of the database Server and Database Instance

Database Server

Backed Up	Database Server Name
❑	
	Database Instance
❑	

Refer to the *Oracle Database Management* Chapter of your Dell OpenManage Network Manager first chapter of the *User Guide* for recommended practices. Also refer to your Oracle product documentation.

Insert any Oracle backup process steps specifics to the site here:

ORACLE Database Backup Steps

Completed	ORACLE backup steps
❑	
❑	
❑	
❑	

MySQL Database Backup Steps

Completed	MySQL backup steps
❑	login as the Dell OpenManage Network Manager User ID on the Database Server
❑	Navigate to a directory outside of the Dell OpenManage Network Manager installation path with writable access. Example: cd $HOME/dbbackups
❑	mysqldump -a -uoware -pdorado owbusdb > ./ owbusdb.backup.mysql
❑	mysqldump -a -uoware -pdorado owmetadb > ./ owmetadb.backup.mysql

Final Clustered System Testing

Perform a full system test as follows with all Application and Mediation Servers being up and running as a cluster.

❑	Open Dell OpenManage Network Manager Client in a browser and Test User Login
❑	Test Network Discovery
❑	Test Device Resync
❑	Upgrade Remaining Application Servers

Test Cluster Failover

Once All Application and Mediation Servers are up and running, perform the following tests:

❑	Locate the application server designated as 'primary' in the server.log file's heartbeat status.
❑	Verify that another Application Server becomes primary.
❑	Connect the primary Application Server's network plug again.
❑	On the matching Physical machine and pull its network plug.
❑	Find the active mediation server in a cluster and pull its network plug.
❑	Verify any of the backup Mediation Servers becomes active.
❑	Connect the previously disconnected Mediation Server's network plug again.

Do a Second System Backup of the Production Servers

Do a system backup of the production Application and Mediation Server(s) after the upgrade is completed and tested as functioning fine.

Servers:

Backed Up	Application Server Name
❑	
❑	
❑	
❑	

Backed Up	Mediation Server Name
❑	
❑	
❑	
❑	

6

Database Management

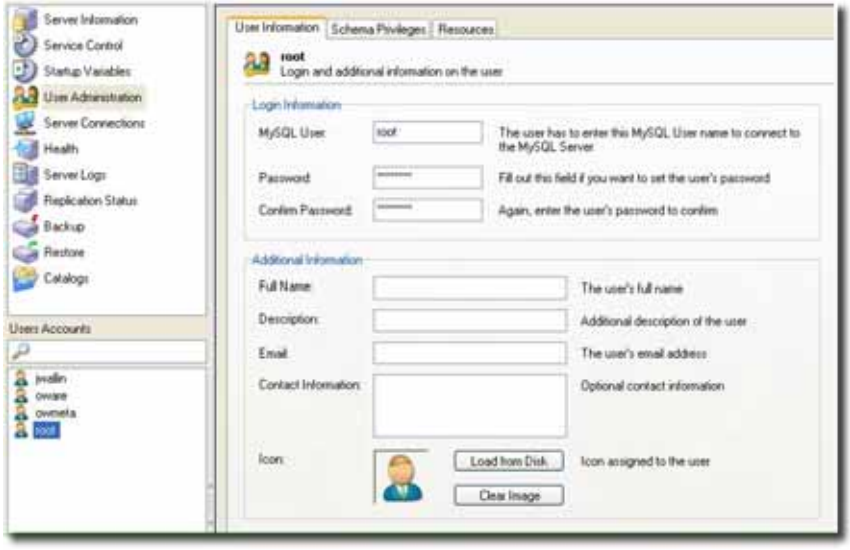
This chapter discusses database management procedures. This discussion includes installation both with the embedded MySQL database and the supported Oracle database. You must distribute Oracle installations and you can distribute MySQL.

In addition to correctly sizing your database, best practice is to develop a plan to regularly back up the database, including steps to verify this backup with recovery. The frequency of backups depends upon your environment, but you should back up often enough to minimize data loss.

Administration Basics

You can download the MySQL administrator and, can get its manual online. Use your favorite search engine to locate it. This optional tool has a graphical user interface, and provides an overview of the MySQL settings. It displays performance indicators graphically, making it easier to determine and tune server settings.

Start this tool to view databases. When you install the embedded database, installation creates a database named `owbusdb`. The installation also creates a `root` and `<O/S user>` login (it creates user *oware*, too).



Read the tool's instructions for the details about how to use it.

Database Login / Passwords

The default login/password combinations for database access

For MySQL:

```
owbusdb: oware/dorado
lportal: root/dorado
synergy: root/dorado.
```

For Oracle:

```
owbusdb ( specified during installation)
lportal :   netview/dorado
synergy: synadmin/dorado
```

For loaddb, use the system user's password. For the portal databases (lportal, synergy) access, set the password in `oware\synergy\tomcat-X.X\webapps \ROOT\WEB-INF\classes\portal-ext.properties.`

The property `com.dorado.jdbc.password.encrypted` specifies whether the database password is encrypted between Dell OpenManage Network Manager and the database.

Database Security

The properties that control the default user and password for application server's database are in

```
oware/lib/owdatabase.properties
```

They are these properties with their default values:

```
## Database logon name
com.dorado.jdbc.user=oware
## Database logon password
com.dorado.jdbc.password=dorado
##******
```

You can change the password after installation, but not the username. If you change the password in a database tool for either Oracle (after setting it to the original during installation) or the embedded database, you must change it in these properties.

CAUTION:

Best practice is to change the default password. You must change it in both the database and the above properties.

NOTICE

As always, properties in `owareapps/installprops/lib/installed.properties` override those in other property files, and are preserved if you upgrade your software.

Database Timeout

When managing large networks or equipment with many interfaces, you may have to increase a timeout property: the `com.dorado.bom.lock_timeout` property in `owareapps\installprops\lib\installed.properties` (originally in `owdatabase.properties`).

Copy that property into `installed.properties`, then increase this setting based on the equipment managed. Generally, you should set this value to the maximum number of interfaces you expect your network elements to have. For example, if the element is expected to have 500 logical interfaces then the timeout value should be set to 500. The minimum recommended timeout value is 60 seconds.

Database Emergency E-mail

To send an e-mail notification to emergency support contacts, if the Dell OpenManage Network Manager database becomes unavailable do the following:

1. In the file `owareapps/installprops/lib/installed.properties` add the following property:

   `oware.monitor.database=true`

2. Ensure that the following Email MBean properties are set:

   `SMTPHost`

   `DefaultSenderAddress`

   `EmergenyContacts`

   The `emergenyContacts` attribute is a comma-separated list of e-mail addresses for the recipients of emergency notifications. The following describes where to set these:

   Open the file `$OWARE_USER_ROOT/oware/jboss-x.x.x/owareconf/oware-service.xml` in a text editor. The following section contains the configuration for the email MBean:

```
<!-- Email MBean -->
<!-- Change the SMTP Host attribute below to point to the right SMTP server
   -->
    <mbean code="com.dorado.mbeans.OWEmailMBean"
        name="oware:service=OWEmailMBean">
        <attribute name="SMTPHost">smtp.doradosoftware.com</attribute>
        <attribute name="Port">25</attribute>
        <attribute name="UserName"></attribute>
        <attribute name="EmergencyContacts"></attribute>
<attribute name="DefaultSenderAddress">redcell@doradosoftware.com</
   attribute>
```

```
        <attribute name="MaxRatePerMinute">200</attribute>
        <depends>jboss:service=@PART_NAME@Partition</depends>
        <depends>oware:service=ClusterPrimaryDesignator</depends>
        <depends>jboss.j2ee:jndiName=RuleEngine,service=EJB</depends>
    </mbean>
```

This file's settings override the Graphical User Interface settings for mail described in the *Properties* chapter of the *first chapter of theUser Guide*.

Embedded Database Sizing

The initially installed Embedded Database is a relatively small instance—possibly too small for your application. This is important because errors can occur when your system reaches the size limit of the database. Therefore, after installing, you may want to resize the Embedded Databases to fit your application. See Modifying the MySQL FAT File Systems on page 206Modifying the MySQL FAT File Systems for instructions about modifying an existing, installed system.

NOTICE

Table and User limits for the embedded database make Oracle the preferred database for large installations.

Follow these steps to resize your database

For Windows,

1. Shut down all applications and application server. And, if applicable, disconnect any other processes from MySQL.
2. Stop the MySQL service on Windows with the command line: `net stop mysql`.
3. Edit the text file `innodb_data_file_path` in `my.ini.`
4. Add the new file path to `innodb_data_file_path`, for example:

   Original:

```
innodb_data_file_path =d:/data/ibdata/ibdata1:600M:autoextend:max:2000M
```

   To add the path `f:/data/ibdata/ibdata2:200M,` the new entry should be:

```
innodb_data_file_path = d:/data/ibdata/ibdata1:600M;f:/data/ibdata/
  ibdata2:200M:autoextend:max:2000M
```

NOTE:

Case sensitivity is important here. Be sure to use uppercase "M's". Omitting this prevents your database from restarting

You must remove the `initial`, `max` and `autoextend` parameters from the initial line that includes `ibdata1`. You must also set the file size to what it really is. To find the size of `ibdata1` run this command (in an command shell where you have already run `oware` in Windows):

```
ls -lh /opt/dorado/..../ibdata1
```

In `my.cnf`, using "1G" is acceptable. The line following this description of the original volume describes the additional volume:

```
/opt/dorado/oware3rd/.../ibdata1:1G;
/opt/dorado/..../ibdata2:1024M:autoextend<optional params>
```

The MySQL Reference Manual for adding a data volume to a MySQL database is http://dev.mysql.com/doc/refman/5.0/en/adding-and-removing.html. See MySQL Server Configuration File Examples on page 21 for other examples.

5 Save `my.ini`.

6 Start MySQL service on Windows by running `net start mysql`'. You should see the following messages,

```
The MySql service is starting.

The MySql service was started successfully.
```

7 Check the file `f:/data/ibdata/ibdata2` appears, and is the right size.

For Linux

1 Shut down all applications and application server. And also disconnect any other process connected to MySQL.

2 Stop the MySQL server process by running the following command:

```
mysqladmin -h <DBServerName> --user=root --
password=<RootUserPassword> shutdown'
```

For example, if *DBServerName* is `nova`, *RootUserPassword* is `dorado`:

```
mysqladmin -h nova --user=root --password=dorado shutdown'
```

If that command fails, run the following command:

```
$MYSQL_ROOT/support-files/mysql.server stop
```

3 Log on as the root user and use a text editor like vi to open `/ect/my.cnf.`

4 Locate the entry `innodb_data_file_path` in `my.cnf`.

5 Add the new file path to innodb_data_file_path, for example,

Original:

```
innodb_data_file_path = /data1/ibdata/ibdata1:600M:autoextend:max:2000M
```

To add the path `/data2/ibdata/ibdata2:200M,` the new entry should be:

```
innodb_data_file_path = /data1/ibdata/ibdata1:600M;/data2/ibdata/
   ibdata2:200M:autoextend:max:2000M
```

NOTE:

Remove the remove the initial, max and autoextend parameters from the initial line that includes ibdata1, as described in the Tip for Windows.

6 Save `my.cnf`

7 Log on as an authorized user to start MySQL server process as `mysqld_safe`.

NOTE:

You may need to specify the path for mysqld_safe.

You should see messages indicating MySQL server started successfully.

8 Check the file `/data2/ibdata/ibdata2` appears, and is the right size.

Modifying the MySQL FAT File Systems

If you have upgraded from older operating systems you may still have a FAT file system that limits your database size or expansion beyond 2GB. The database is a file as far as the operating system is concerned, and FAT limits file size. There is also a 4GB limit on early versions of NTFS that may linger because of upgrades.

To change the installed database sizes, you must edit the configuration file:

- Windows: `%SystemRoot%\my.ini`

The origin of the configuration in the several my.cnf files on Linux is a path like `/opt/dorado/oware3rd/mysql/5.0.51-pc-linux-i686-64/my.cnf`, so be sure to alter that one if you are reconfiguring Dell OpenManage Network Manager's MySql.The following line controls maximum database size (at end):

```
innodb_data_file_path = d:/work/oware3rd/mysql/ibdata/
ibdata1:600M:autoextend:max:2000M
```

To recreate database after modifying config file, use the following command from the application server:

```
loaddb -q -d -m
```

Syntax details:

```
innodb_data_file_path =
pathtodatafile:sizespecification;pathtodatafile:sizespecification;
...
```

```
innodb_data_file_path = ...
;pathtodatafile:sizespecification[:autoextend[:max:sizespecificati
on]]
```

If you specify the last datafile with the *autoextend* option, InnoDB will extend the last datafile if it runs out of free space in the tablespace. The increment is 8 MB at a time. An example:

```
innodb_data_file_path = /ibdata/ibdata1:100M:autoextend
```

This instructs InnoDB to create just a single datafile whose initial size is 100 MB and which is extended in 8 MB blocks when space runs out.

If the disk becomes full you may want to add another datafile to another disk, for example. Then you must look at the size of `ibdata1', round the size downward to the closest multiple of 1024 * 1024 bytes (= 1 MB), and specify the rounded size of `ibdata1' explicitly in `innodb_data_file_path`. After that you can add another datafile:

```
innodb_data_file_path = /ibdata/ibdata1:988M;/disk2/
ibdata2:50M:autoextend
```

Be cautious on filesystems where the maximum file-size is 2 GB. InnoDB is not aware of the operating system's maximum file-size. On those filesystems you might want to specify the max size for the datafile:

```
innodb_data_file_path = /ibdata/ibdata1:100M:autoextend:max:2000M
```

Some additional caveats:

- You must use foreslashes (/) instead of backslashes (\) when you specify the path.
- The subdirectory iblogs must be used by MySQL exclusively
- Make sure you enough disk space available on the data path specified
- You can add as many entries as you like. However, you can use `initial, max` and `autoextend` only in the last entry, and must change the first entry to reflect the actual size of the database.
- The name of filepath must be valid on the filesystems. However, you must always have your leaf directory in the path as ibdata.

Database Backup / Restoration

The recommended procedures for database backup and restoration for the embedded database follows. Best practice is to develop backup plans using these procedures for the sake of database reliability.

For MySQL (embedded) databases, use this database's native backup/restore utilities, described in the following section, to backup the `owbusdb` database. You can also refer to the MySQL manual available online for instructions about backup and restoration. For instructions about backing up / restoring Oracle databases, refer the Oracle manuals.

MySQL Backup / Restore

Follow these instructions to back up and restore the embedded MySQL database using native MySQL utilities on a command line.

Backup

Open a command shell (*Start* > *Run* `cmd`, in Windows), and then type the following at the prompt. By default, the primary database is `owbusdb`, and `owmetadb` includes meta-information. For the web server, back up `lportal` and `synergy` too (the latter contains multitenancy information). The example includes defaults for name and password. These are typically different from the login / password for the application.

```
mysqldump -a -u root --password=[password] owbusdb > FILENAME.mysql
```

For example:

```
mysqldump -a -u root --password=dorado owmetadb > owmetadb.mysql
```

If you have Performance monitors or Traffic Analyzer, you must also back up your stored procedures otherwise they do not get restored when you restore the database. The command line here adds `--routines`. For example:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

This writes the owbusdb to a plain-text file called `FILENAME.mysql` (`owbusdb.mysql` in our examples). This file is a full backup with which you can fully restore your database in case of problems.

Here are the backup commands for all the databases:

```
mysqldump -a -u root --password=dorado owbusdb > owbusdb.mysql
mysqldump -a -u root --password=dorado owmetadb > owmetadb.mysql
mysqldump -a -u root --password=dorado lportal > lportal.mysql
mysqldump -a -u root --password=dorado synergy > synergy.mysql
```

Restoring

Restoring from `FILENAME.mysql` is a three step process. This occurs, again, in a command shell:

1. Drop the database:

```
mysqladmin -u USERNAME -p drop owbusdb
```

or

```
mysqadmin -u USERNAME --password=[password] drop owbusdb
```

2. Recreate the database

```
mysqladmin -u USERNAME -p create owbusdb
```

or

```
mysqadmin -u USERNAME --password=[password] create owbusdb
```

3 Import the backup data

```
mysql -u USERNAME -p owbusdb < FILENAME.mysql
```

or

```
mysql  -u USERNAME --password=[password] owbusdb < FILENAME.mysql
```

Here are restoration commands for all the databases:

```
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb  < owbusdb.mysql
mysql -u root --password=dorado lportal  < lportal.mysql
mysql -u root --password=dorado synergy  < synergy.mysql
```

Database Failover

You can configure the embedded MySQL database with multiple instances that fail over. For a new installation with a distributed mysql db server on the application server machine, follow these steps:

1 To create Dell OpenManage Network Manager's database, run `loaddb` (the default user/password is `oware/dorado`).

2 To create portal and synergy databases, run `loaddb` (default user password is `root/dorado`), as follows: `loaddb -u root -w dorado -s`

3 To seed the database, run `ocpinstall -s`

Oracle

Oracle's RAC technology handles all Oracle "failover."Consult this product's websites for further information.

Distributed Database Upgrades

For an upgrade with distributed mysql database server, run on the (primary) application server. Despite its name, the needed commands are the same for MySQL in the script `dbpostinstall`. These include:

```
dbevolve -a -x
ocpinstall -s
licenseimporter
```

MySQL Replication

Install mysql database into 2 servers
master 10.35.35.170
stop Redcell Synergy appservers/webservers
slave 10.35.35.174

On master (10.35.35.170) edit my.cnf file ...\dorado\oware3rd\mysql\5_0_51-64 directory
add under [mysqld] section:
log-bin = mysql-bin
server-id = 1
restart mysql for changes to take effect.

On slave (10.35.35.174) edit my.cnf file ...\dorado\oware3rd\mysql\5_0_51-64 directory
change server-id from 1 to 2
restart mysql for changes to take effect

log into master mysql server (10.35.35.170) and create users: "mysql -u root --password = dorado"
mysql > CREATE USER 'repluser'@'10.35.35.170' IDENTIFIED BY 'slavepass';
mysql > CREATE USER 'repluser'@'10.35.35.174' IDENTIFIED BY 'slavepass';

still on master mysql server, grand privileges for created user:
mysql > GRANT ALL PRIVILEGES ON *.* TO 'repluser'@'10.35.35.170';
mysql > GRANT ALL PRIVILEGES ON *.* TO 'repluser'@'10.35.35.174';

on master mysql server (10.35.35.170) grant user permissions for replication:
mysql > GRANT REPLICATION SLAVE ON *.* TO 'repluser'@'10.35.35.170';

stop adding more information into master database by executing following on master database:
mysql > FLUSH TABLES WITH READ LOCK;

Copy databases to slave

backup databases in oware prompt on master (10.35.35.170)

```
mysqldump -a -u root --password=dorado --routines owbusdb > owbusdb.mysql
mysqldump -a -u root --password=dorado owmetadb > owmetadb.mysql
mysqldump -a -u root --password=dorado lportal > lportal.mysql
```

move *.mysql files to slave

on slave (10.35.35.174) in oware prompt execute following commands

```
mysqladmin -u root --password=dorado drop owmetadb
mysqladmin -u root --password=dorado drop owbusdb
mysqladmin -u root --password=dorado drop lportal
mysqladmin -u root --password=dorado create owmetadb
mysqladmin -u root --password=dorado create owbusdb
mysqladmin -u root --password=dorado create lportal
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb < owbusdb.mysql
mysql -u root --password=dorado lportal < lportal.mysql
```

To obtain master file position which is required to know, execute following command on master mysql, (in this example it is 73):

```
mysql>show master status;

+----------------------+------------+------------------+----------------------+
| File                 -----   | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+----------------------+-----------+------------------+----------------------+
| mysql-bin.000001 | 73           |                          |                              |
+----------------------+-----------+------------------+----------------------+
```

log into slave mysql server (10.35.35.174) and create users: "mysql -u root --password=dorado

```
mysql> CREATE USER 'repluser'@'10.35.35.170' IDENTIFIED BY 'slavepass';
mysql> CREATE USER 'repluser'@'10.35.35.174' IDENTIFIED BY 'slavepass';
```

still on slave mysql server, grand privileges for created user:

```
mysql>GRANT ALL PRIVILEGES ON *.* TO 'repluser'@'10.35.35.170';
mysql>GRANT ALL PRIVILEGES ON *.* TO 'repluser'@'10.35.35.174';
```

setting up master configuration on slave and start replication:

```
mysql> CHANGE MASTER TO
    ->     MASTER_HOST='10.35.35.170',
    ->     MASTER_USER='repluser',
    ->     MASTER_PASSWORD='slavepass',
    ->     MASTER_LOG_FILE='mysql-bin.000001',
    ->     MASTER_LOG_POS=73;
mysql> START SLAVE;
```

unlock tables and restart appserver/webserver on master

log into master mysql database and execute:
mysql>UNLOCK TABLES;

restart appserver/webserver

To verify that replication is functioning execute
on master: mysql>show master status;
on slave: mysql>show slave status\G;

both instances should have file position growing and it should be identical.

7

Oracle Database Management

Installing Oracle

Before running this application's Oracle setup, you must first install Oracle and create the database instance. The following is a set of basic guidelines for installing Oracle. This may not describe the optimum configuration for every environment, but it provides a simple example of how to install Oracle in a basic configuration. Best practice is to employ a trained Oracle DBA to either assist or manage the installation and ongoing maintenance required to keep your application performing properly.

The Oracle site containing Oracle's Installation guide, covering settings, creating database instances, operating system support, and so on is http://www.oracle.com/technetwork/documentation/index.html#database

Username / Password Considerations

We do not support using `sys` or `system` user as the user for the Dell OpenManage Network Manager application. If you entered one of these during installation, modify the `$OWARE_USER_ROOT/owareapps/installprops/installed.properties` file. Before running `loaddb`, change the following parameters:

```
com.dorado.jdbc.user=<user>
com.dorado.jdbc.password=<password>
```

The following assumes that a database instance has been created and configured properly. If you wish to use Oracle RAC for high availability of, then consult your Oracle resource for proper practices on configuring the RAC environment. See also Encrypting the Oracle Password on page 217.

CAUTION:
Do not install Oracle with the username `redcell`

An Outline of Installation Steps

Before installing Dell OpenManage Network Manager, your Oracle DBA needs to do the following tasks:

1 Install Oracle according to its installation instructions.

The Dell OpenManage Network Manager installer does the following:

2 Install Dell OpenManage Network Manager, selecting Oracle as the database, and filling in the user, password, IP address of the server, and so on. Note that the following steps may be useful in installing Dell OpenManage Network Manager:

a. Open command prompt/terminal and source environment using `oware` (Windows) or `. /etc/.dsienv` (Linux).

a Test database connectivity with the command: `pingdb -u <dba user> -p <dba password>` to test connectivity. For example: `pingdb -u system -p manager.` Without these parameters, `pingdb` consults the `installed.properties` file for the user / password.

NOTE:

With Oracle 11G, the parameter sec_case_sensitive_logon defaults to TRUE when you install the database. You must change this to FALSE for loaddb and pingdb to work if you have upper case characters in the login / password for your Oracle database.

3 Run the following on a fresh installation to create the database schema and users (system / manager are the database user and password for this example).

```
loaddb -u system -w manager
loaddb -u system -w manager -s.
```

Run this only with the Oracle system user (See Running Loaddb on page 216). This creates and loads the portal database. The user running this must have dba privileges—more specifically, this user must have permission to create or delete users, roles, tablespaces, tables, and so on.

if `loaddb -u system -w password` does not work the first time then add `-d` to the command.

4 Running this automatically creates a user `oware` with password `dorado` in the database.

5 Create synergy database with this command:

```
loaddb -u system -w <password> -s -g
```

This automatically creates user `netview` with password `dorado` in the database.

6 Run `dbpostinstall` on the (primary) application server. (See Running dbpostinstall on page 217)

7 Restart application server.

The following steps only apply if you did not choose the option for the server to start automatically:

8 Open a shell and set the environment with `oware` (Windows) or `. /etc/.dsienv` (Linux). Enter `pmstartall` to start the application server.

In Linux: to start the web portal, enter:

```
/opt/dorado/oware/synergy/tomcat-6.0.32/bin/startportal.sh start
```

You can also use the Start menu in Windows to start RC Synergy.

NOTE:

In a HA application server environment, you need to run this only once from one application server. Mediation servers do not need to have database connectivity, so you do not have to run this on distributed mediation servers.

CAUTION:

See Upgrading Oracle Databases on page 117 for instructions about updating an existing Oracle installation. Also, see Oracle Database Connections on page 183 for information about configuring those.

Important Hardware Considerations

Refer to the Oracle Installation guides for minimum requirements. Note that Dell OpenManage Network Manager uses the Oracle database in a highly transactional way. This means that there will be significant IO to the Redo logs. Some basic recommendation to optimize IO for the Oracle server would be to increase the number of physical disks available to the server which will help to eliminate lock contentions.

Initial testing of the Oracle installation

Run the following as `system` before running loaddb, and as the Dell OpenManage Network Manager user before starting the application server to validate the success of loaddb's user creation:

- Verify your application server can access the Oracle server. Use the following command to do this:

  ```
  pingdb -u <username> -p <password>
  ```

- Although Oracle's installation offers options to select replication in one of the Oracle trees in addition to Default, this application's installation supports only Default. Any Oracle database's high availability feature support is outside this application's JDBC connection to the database (you must use Oracle's RAC technology or equivalent).

Initial Database Setup

Creating an Oracle user for the application server is unnecessary. Dell OpenManage Network Manager's installation scripts create all required schema objects for the application server. Follow these steps to configure your database for use with Dell OpenManage Network Manager.

1 After the Dell OpenManage Network Manager Installer finishes, source the `oware` environment in a shell to execute the following commands.

Windows: `oware`

Linux: `. /etc/.dsienv`

2 To successfully install against an Oracle server running on a Windows *Server* Operating System you must create a user with DBA privileges on the Oracle server:

```
sqlplus system/<system password>@SID
create user foo identified by foo;
grant dba to foo;
exit
```

You can then run `loaddb` from application server as described below.

Running Loaddb

3 Before running the `loaddb` script, you can optionally replace the occurrences of the literal values OWARE_DEFAULT_SIZE and OWARE_ORADATA_PATH in the tablespace creation script with your desired tablespace size and location. If you do not modify this script, your data files will be created under your `$ORACLE_HOME` directory. The tablespace creation script is in:

```
$OWARE_USER_ROOT/oware/dbscript/oracle/owaredba/
  create_oware_tablespaces.sql
```

NOTE:

You must modify this script if you are running Oracle RAC, otherwise altering it is optional.

You will need your DBA password to run the `loaddb` script. The user and password you select must be able to perform user, role, and tablespace creation tasks. You must run this as `system` user. The -w option is required for the password:

```
loaddb -u system -w <system password> -s
```

With the `-s` it creates the Dell OpenManage Network Manager tablespace: OWSYNERGY01 and the portal tablespace. Without `-s` it creates Dell OpenManage Network Manager tablespaces: owdata01 and owidx01. Here are the options:

```
loaddb -u system -w <system password>
```

Creates:

- tablespace owdata01
- tablespace owidx01
- role owrole
- user redcell

(assuming you specify the user “redcell” during installation or in the `install.properties` file)

```
loaddb -u system -w <system password> -s
```

Creates:

- tablespace OWSYNERGY01—Includes user credentials, multitenancy information.

- role OWSYNERGYROLE
- user SYNADMIN
- tablespace OWPORTAL01 (portal information)
- role OWPORTALROLE
- user NETVIEW

Running dbpostinstall

4 After running `loaddb`, you must seed the database with all required information. This is based on what software is installed with your package. Running he `dbpostinstall` command on the (primary) application server examines your package and seeds all appropriate information. To see options available with this script, run `dbpostinstall -?`

Encrypting the Oracle Password

5 By default, the JDBC username and password are stored in clear text, during installation, in the following file:

```
<install_root>/owareapps/installprops/lib/installed.properties
```

The username and password properties must be clear text to run the loaddb script. This script creates/re-creates the database schema. Once the schema is created, you may encrypt the database password stored in the `installed.properties` file.

A utility script, `owjdbcutil`, supports changing the username and/or password used for database access. This script also supports encryption of the database password:

```
owjdbcutil -u <database user> -p <database password> -e
```

Oracle Server Settings and Parameters

The following are general recommendations for Oracle installations:

Oracle Server Initialization Parameters Recommendations

The following sections describe how to configure the application's initialization parameters with an Oracle database. Modifying Oracle initialization parameters in the init < InstanceSid > .ora file. Refer to recommendations provided with your Oracle installation's default init.ora (located in $ORACLE_HOME/ srvm/admin/ typically)

```
Shared_pool_size Minimum size 150M
Shared_pool_reserved_size Minimum size 15M
Open_cursors Minimum 1500
Processes Minimum 100
Job_queue_processes Minimum 2
Sort_area_size = 1048576
```

```
Sort_area_retained_size= 1048576
```

Other Best Practices

- Set CURSOR_SHARING = FORCE reduces CPU use.
- Increased log size from 3 groups of 52M, to 4 groups of 500M apiece. This definitely decreased the log_file_sync wait event, improving throughput.

Oracle Database Sizing

Sizing an Oracle database is part of its installation. Even before installing Oracle you should consult your DBA to estimate how big your data is going to be and size the database accordingly.

CAUTION:
Size your database server's disk based on anticipated traffic. Oracle's archive logs can grow rapidly. (In one test these archive logs grew to 12 GB in two weeks). If the file system fills up with the archives, Oracle stops, and may need to be restarted to clear an archive error.

Installation of Oware-based products produces files like the following:

`load_{product_name}_sizing.sql`

For example: `load_redcell_sizing.sql`. The `sql` extension for this file has no significance (you cannot run this file in a SQL tool).

Here is an excerpt from the sizing file generated for Oware service classes:

```
REM
#####################################################################
REM #
REM # Script Name  : load_oware_svc_sizing.sql
REM # Creation Date: Fri Jul 05 16:17:29 PDT 2002
REM #
REM # Columns:
REM # sql Prompt, Classname, tablename, Tablesize, Blob size (0/
1024)
REM
#####################################################################
```

This is a comma-delimited file. The comma-separated columns are as follows:

Column #	Definition
1	n/a

Column #	Definition
2	class name
3	tablename
4	Tablesize (non-blob fields)
5	Blob size (0 if table does not contain a blob 1024 otherwise)

To use this sizing file, do the following:

1. Import this file into a spreadsheet, choosing comma-delimited formatting.
2. Once imported, you can see the record sizes (in bytes) for the application.
3. Multiply these record size amounts by the number of rows expected for those tables/classes.
4. Calculate number of bytes for each class.
5. Sum calculated byte count to determine total datafile size (convert to mega- or gigabytes, if needed)

NOTICE

Best practice is to size your database at least 20% larger than calculated above.

Oracle Backup / Restore

For Oracle fault tolerance, back up your Oracle database. To do this, we recommend using Oracle's Recovery Manager (RMAN) backup utility. This is an Oracle tool that lets you back up, copy, restore, and recover data files, control files, and archived redo logs. It is included with Oracle server and does not require a separate installation. For details about using RMAN, see the *Recovery Manager User's Guide* provided by Oracle.

The next section describes backup and restoration in a little more detail. By default, the primary database is `owbusdb`. For the web server, back up `lportal` and `synergy` too.

Backup with exp and imp

Although best practice is to use RMAN, Oracle's backup utility, you can also use `imp` and `exp` export and import a schema in Oracle.

Installing Dell OpenManage Network Manager creates two new user schemas: `netview` is the owner for the database (or tablespace) `owportal01`, `synadmin` is the owner for the database `owsynergy01`, the default password for these two user is: `dorado.` (See Database Login / Passwords on page 202)

Installation asks for an a oracle user, and this example selects `redcell`. This selection also appears in the `installed.properties` file.

User `redcell` is the owner for the database `owdata01` (loaddb creates tablespace `owdata01` under user `redcell`) as follows:

```
loaddb -u system -w dorado
```

Executing this command creates `owportal01` and `owsynergy01`

```
loaddb -u system -w dorado -s
```

so the complete backup/restore should includes

In this example dorado is the database administrator's password, and sample61 is the SID:

Backup

```
exp system/dorado@sample61 owner=redcell  file=redcell.dmp
exp system/dorado@sample61 owner=netview  file=netview.dmp
exp system/dorado@sample61 owner=synadmin file=synadmin.dmp
```

Restore

```
imp system/dorado@sample61 fromuser=redcell touser=redcell ignore=y
   file=redcell.dmp
imp system/dorado@sample61 fromuser=netview touser=netview ignore=y
   file=netview.dmp
imp system/dorado@sample61 fromuser=synadmin touser=synadmin ignore=y
   file=synadmin.dmp
```

You may encounter an ORACLE 2291 error when using command line `imp.`

For example:

```
. importing table "RCC_TASK_USAGE_ENTITY"
IMP-00019: row rejected due to ORACLE error 2291
IMP-00003: ORACLE error 2291 encountered
ORA-02291: integrity constraint (REDCELL.FKE609020E14863754) violated -
   parent key not found
```

The workaround for this is to find the foreign key reference table and import the parent table first then re-import the problematic table. For example:

```
imp system/dorado fromuser=redcell touser=redcell ignore=y constraints=n
file=redcell_17012013.dmp tables=rcc_task_usage_entity
```

NOTE:

There is no substitute for having a DBA. Such an administrator could tell you how Oracle has improved on its previous import/export utility with RMAN and Data Pump. Oracle's manuals explain the use of these utilities.

On-line/Off-line Backup (OS)

You can back up your database using Operating System (OS) commands along with Oracle system views. Although OS backups allow database recovery, the recovery process may be more complex than using RMAN. We recommend OS backups as an interim backup strategy until RMAN is in place.

A cold backup is a backup performed when the database is completely shut down. A hot backup is one performed when the database is open and possibly in use. An Instance is a synonym for an Oracle database.

Off-line backups, or cold backups, require database shutdown before making a backup. Restored cold backups resolve any kind of database failure, as long as the backed up files are intact.

On-line backups, or hot backups, do not require database shutdown. Active transactions can be running while the backup occurs. On-line backups can recover from many failures, but some types of failures may require restoring to an off-line backup and then recovering from there. See the Oracle manuals for instructions about how to do hot and cold backups.

Oracle Export/Import (Oracle utilities)

Oracle's export and import utilities back up the data contained within an Oracle database. The RMAN/OS Oracle backups back up the entire database at the datafile/tablespace level whereas export/import backup/restore at the user/table level. An export is a good supplement to any of the above backups.

Oracle's export/import can backup/restore a Database (all users), a particular user, or a set of tables. See Oracle’s manuals for details about Oracle’s Export and Import.

Database Recovery Procedures

You can recover Oware’s backed up databases if your system fails. The quality of recovery naturally depends on the frequency and integrity of the database backups. The more frequent the backups, the less data loss occurs. Since Oware supports multiple database types, the method used to recover the databases differs according to type.

If RMAN is in place, use it for recovery. If it is not in place, and you have used the OS backups (On-line/Off-line Backup (OS) on page 221), consult Oracle’s manuals for their recovery procedures.

Oracle Failover

Oracle RAC is a clustering solution from Oracle that allows this application to communicate with a database cluster using one service name. This also provides failover and load balancing.

- Oracle versions that support RAC: 9.2.0.5 or newer. In an RAC configuration, all nodes access a single database. Dorado applications built with Oware 6.0.2 and later support Oracle RAC. See Oracle Version Support on page 29.
- RAC requires specific hardware and Cluster Manager software to run. Refer to Oracle's instructions for installing this feature.
- You need apply any schema changes only once for RAC regardless of the number of nodes accessing the database.

To support RAC, you must manually configure the property `com.dorado.oracle.rac.connect.url` listed in the `owdatabase.properties` file, in addition to all existing oracle properties. See Oracle RAC installation.properties File on page 222 for information about that file.

The property `com.dorado.oracle.rac.connect.url` defines a database connection URL used by the JBoss connection pool at application server startup. This property defines the following configurable attributes:

Address List—A list of database servers in the RAC cluster.

Failover—*On/Off*

Load Balancing—*On/Off*

Dedicated Server—*On/Off*

Service Name—This is a Global Database Name and not a SID.

The Oracle 10g jdbc jar is included in the Oware classpath by default (in `oware/lib3rd`). This is backward compatible with Oracle 9i. Modify the RAC property by overriding it in the `owareapps/installprops/installed.properties` file. Make sure the URL is well-formed, with the brackets that appear in the sample property in the `oware/lib/owdatabase.property` file. See Oracle Version Support on page 29 for more about the JDBC driver.

Oracle RAC installation.properties File

The following differs slightly for each Oracle versions. For example, 10G RAC uses VIP; 11G RAC uses Scan (and can also use VIP). Therefore, the `installation.properties` file needs to be like one of the following options:

Option 1

```
com.dorado.oracle.rac.connect.url=@(DESCRIPTION=(ADDRESS_LIST=\
(ADDRESS=(PROTOCOL=TCP)(HOST=vip1)(PORT=1521))\
(ADDRESS=(PROTOCOL=TCP)(HOST=vip2)(PORT=1521))\
)\
(FAILOVER=on)(LOAD_BALANCE=on)(CONNECT_DATA=(SERVER=DEDICATED)\
(SERVICE_NAME=orcl)))
```

Option 2

```
com.dorado.oracle.rac.connect.url=@(DESCRIPTION=(ADDRESS_LIST=\
(ADDRESS=(PROTOCOL=TCP)(HOST=orascan)(PORT=1521))\
)\
(CONNECT_DATA=(SERVER=DEDICATED)\
(SERVICE_NAME=orcl)))
```

NOTE:

Check the DNS server to make sure it is configured correctly.

Installation also needs the following to install Dell OpenManage Network Manager device drivers:

```
com.dorado.jdbc.database_name.oracle=@ServerIP:1521:Service_Name
```

Performance Tuning RAC

If you experience performance issues with your Oracle system, the following are some performance changes and reports you might try:

- Increase portion of SGA (System Global Area) memory dedicated to the data buffer rather than shared buffer pool.
- Change `cluster_interconnects` parameter used in RAC interconnection from the default MTU of 1500 bytes to 9000 bytes (jumbo frames).
- Investigate and analyze AWR & RDA reports against RAC Nodes.

Setting the MTU to Jumbo Frames may reveal issues with any switch (or switches) between hosts. You often must set older switches to accept them. You can also adjust the properties on the physical NICs, but if the switch is not configured to accept them CRS will not start. Most newer switches do this automatically, but some may not.

Example Tune-up

Example setup:

```
10.17.7.10 cbj-ip-do-orac01-priv
10.17.7.11 cbj-ip-do-orac02-priv
g2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
inet 10.17.7.10 netmask ffff0000 broadcast 10.17.255.255
```

Tasks before making the change to jumbo frames for example servers g1 and g2:

Verify:

1. Check all devices between databases support jumbo frames.
2. Identify if failover/bonding/teaming is active for your g2 (g1, for example). Modify these as appropriate.

3 Check with network engineering and system administrators who have activated jumbo frames before to see if they have any other suggestions.

Steps:

1 Modify `MaxFramSize` in `/kernel/drv/g.conf` to `3` as described below on the man page for g1 or g2.

Set the upper limit on the maximum MTU size the driver allows. All Intel gigabit adapters (except the 82542-based Intel PRO/1000 adapter) allow the configuration of jumbo frames.

For an Intel PRO/1000 adapter that is later than 82571, (including 82571), the maximum MTU accepted by the MAC is 9216. For others, the maximum MTU accepted by the MAC is 16128. Use ifconfig(1M) to configure jumbo frames. Use ifconfig with the adapter instance and the MTU argument (ifconfig g0 mtu 9216) to configure adapter g0 for the maximum allowable jumbo frame size.

Allowed values are:

0 Standard ethernet frames with a MTU equal to 1500.

1 Jumbo frames with a maximum MTU of 4010.

2 Jumbo frames with a maximum MTU of 8106.

3 Jumbo frames with a maximum MTU of 16298.

2 Shut down Oracle and CRS with `crsctl stop` on both nodes.

3 Modify the MTU and test on both nodes.

```
ifconfig g2 mtu 9194
```

From opposing nodes:

```
ping -c 2 -M do -s 8972 cbj-ip-do-orac01-priv
ping -c 2 -M do -s 8972 cbj-ip-do-orac02-priv
```

4 Set the MTU in the `/etc/hostname.g2` file on both nodes

```
existing options "mtu 9194"
```

5 Verify setting with `ifconfig -a` after reboots on both nodes, making certain the public interface and VIPs remain at MTU 1500

6 Restart CRS and services on both nodes.

Database Sizing

This section suggests sizing solutions, but any final sizing decisions must realistically be guided by business managers working with DBAs to weigh data storage requirements versus costs.

A typical recommendation is to size your database 20% larger than the expected data.

You can store roughly 0.5 million traps per 1G of disk space. Performance typically does not suffer if you oversize. Twenty gigabytes of storage is typical. Refer to the Monitoring and Traffic Flow Analysis chapters of the *User Guide* for additional advice about configuring those monitors relative to database capabilities. The *User Guide* also offers database sizing information in the Getting Started chapter.

Database Aging Policies

This application includes a Database Aging Policy (DAP) Manager, which lets you set up policies that control the length of time that data persists in the database. Best practice is to set up DAPs for records that are continually persisted. Several aging policies come with the application. You can edit them to suit your needs, too. See Chapter 6, Database Management for more information about database backup.

Autoextend

By default the autoextend property in Oracle tablespaces allows them to grow, as needed, until they exhaust all file system space. In this default, the only way to fail to extend the tablespace is by running out of disk/file system space.

The embedded MySQL database lets you define an initial size and an autoextend ceiling. This ceiling is a hard coded value in the MySQL config file. To change this, define the following in the `my.ini/my.cnf` files at creation time:

```
[Installation root]/oware3rd/mysql/ibdata/
ibdata1:1024M:autoextend:max:2048M
```

What this says is to create a 1G data file at initiation and allow it to grow to a maximum of 2G, as needed. Once 2G is reached the server will start issuing errors (number 1114) for each insert attempted. If this occurs, you must add another data file to the system and revise Database Aging Policies accordingly. See MySQL Server Configuration File Examples on page 21 for more.

The installer also lets you choose these MySQL values, defaulting to 1024M for initial and 8096M for the ceiling.

One example system would add a data file to the database to account for alarm/event history data:

```
[Installation root\/oware3rd/mysql/ibdata/ibdata1:2048M;c:/dorado/
oware3rd/mysql/ibdata/ibdata2:2048M:autoextend:max:2048M
```

The autoextend property can only be found in the last data file specified. YOu must specify the size to which the first file grew when adding the second data file. See MySQL's documentation on the addition or removal of innoDB data files to determine the syntax. It is located at *dev.mysql.com/doc/refman/4.1/en/adding-and-removing.html*

The process essentially follows these steps:

1. Shutdown the application
2. Shutdown MySQL
3. Modify `my.ini/my.cnf.` See MySQL Server Configuration File Examples on page 21.
4. Restart MySQL
5. Restart the application

If you store more historical data online (in your database) you must size it accordingly. This avoids databases filling before you are ready to manage the system.

9

SNMP MIBs

Locations of this application's MIB Files, are as follows:

Ocp	Location	File Name	Description
redcell.ocp	owareapps/Redcell/mibs	DoradoSoftware-MIB	Base MIB for all other MIBs. Contains the enterprise MIB registration.
eventmgmt.ocp	owareapps/eventmgmt/mibs	AssureAlarms-MIB	Contains SNMP Notifications encompassing Oware, Dell OpenManage Network Manager and Event Management ocp functionality.
netrestore.ocp	owareapps/netrestore/mibs	RedCellNetConfig-MIB	Contains SNMP Notification definitions for the Netrestore product. Currently contains notifications (traps) for backup, restore and deploy failures.
performance.ocp	owareapps\performance\mibs	RedcellMonitor-MIB	SNMP notifications definitions for performance monitor.
changemgmt.ocp	owareapps\changemgmt\mibs	RedCellChangeMgmt-MIB	SNMP notifications definitions for change management.
trafficanalyzer.ocp	owareapps\trafficanalyzer\mibs	TAAlarms-MIB.txt	SNMP notifications definitions for traffic analyzer.
activeconfig.ocp	owareapps/activeconfig/mibs	ACTIVECONFIG –MIB	SNMP notifications definitions for Adaptive CLI.

MIB file locations are subject to change without notice, but generally are under the `owareapps/[product name]/mibs` directory for different application modules.

Driver Standard MIB Usage

The following sections outline MIB items used in various Dell OpenManage Network Manager functions.

Discovery / Resync

The MIBs in the following sections are related to discovery and resync.

ENTITY-MIB

entPhysicalTable

Obtains port and card information from device

entPhysicalDescr—optionally used as name of card, port or Dell OpenManage Network Manager model

entPhysicalContainedIn—used to map position in hierarchy in Dell OpenManage Network Manager model

entPhysicalClass—used to map to port or card in Dell OpenManage Network Manager model

entPhysicalParentRelPos—used to map position in hierarchy in Dell OpenManage Network Manager model

entPhysicalName—optionally used as name of card, port. If type port expect to map to ifName or ifDescr

entPhysicalHardwareRev—recorded in Dell OpenManage Network Manager model for applicable types

entPhysicalFirmwareRev—recorded in Dell OpenManage Network Manager model for applicable types

entPhysicalSoftwareRev—recorded in Dell OpenManage Network Manager model for applicable types

entPhysicalSerialNum—recorded in Dell OpenManage Network Manager model for applicable types

entPhysicalModelName—recorded in Dell OpenManage Network Manager model for applicable types

RFC1213-MIB

system

sysDescr—informational in Dell OpenManage Network Manager model

sysObjectID—used to identify device type, prefer to be unique per device model

sysContact—informational in Dell OpenManage Network Manager model

sysName—optionally used as part of device name in Dell OpenManage Network Manager model

sysLocation—informational in Dell OpenManage Network Manager model

ifTable

ifIndex—recorded against port or interface in Dell OpenManage Network Manager model

ifDescr—optionally used as name of port or interface in Dell OpenManage Network Manager model (ifName from ifXTable preferred)

ifType—aids in mapping to Dell OpenManage Network Manager common type for port or interface

ifMtu—recorded in Dell OpenManage Network Manager model

ifSpeed—recorded in Dell OpenManage Network Manager model, for high speed interfaces ifXTable is used if supported.

ifPhysAddress—if port is Ethernet maps to mac address in Dell OpenManage Network Manager model

ifAdminStatus—recorded on port or interface in Dell OpenManage Network Manager model

ifOperStatus—recorded on port or interface in Dell OpenManage Network Manager model

ipAddrTable

Associates IP addresses with a device

ipAdEntAddr—recorded as IP used by device

ipAdEntIfIndex—used to map IP to a port or interface in Dell OpenManage Network Manager model

ipAdEntNetMask—recorded on port or interface in Dell OpenManage Network Manager model

IF-MIB

IfXTable

Gets more precise interface information, if available

ifIndex—obtained from oid instance, must map to entry in ifTable

ifName—used as LI Name in Dell OpenManage Network Manager model also optionally the name of the interface or port

ifHighSpeed—used as speed for port in Dell OpenManage Network Manager model

ifStackTable

If supported, identifies sub-interfaces and places interfaces in Dell OpenManage Network Manager model

ifStackHigherLayer—obtained from oid instance

ifStackLowerLayer—obtained from oid instance

ifStackStatus—Used to understand if entry is active or not

BRIDGE-MIB

dot1dBase

dot1dBaseBridgeAddress—optionally used to define a unique id for the device

dot1dBasePortTable

Optional, determines if ifTable entry is a physical port or not.

dot1dBasePort—unique id for a port

dot1dBasePortIfIndex—maps to ifTable and ifXTable by index. Expected to map to physical port entries.

LLDP-MIB

lldpLocalSystemData

Get device identification

lldpLochassisIdSubtype—used to understand format of chassis ID

lldpLochassisId—optionally used as unique ID for the device

Key Performance Indicators

The following MIBs are related to KPI.

IF-MIB

ifXTable

Used for port and interface monitors

ifIndex—Obtained from instance, mapped to port or interface in Dell OpenManage Network Manager model

ifInMulticastPkts

ifInBroadcastPkts

ifOutMulticastPkts

ifOutBroadcastPkts

ifHInOctets

ifHInUcastPkts

ifHInMulticastPkts

ifHInBroadcastPkts

ifHOutOctets

ifHOutUcastPkts

ifHOutMulticastPkts

ifHOutBroadcastPkts

ifHighSpeed

RF1213-MIB

The following section's MIBs provide KPI and monitor information.

ip

ipDefaultTTL

ipInReceives

ipInHdrErrors

ipInAddrErrors

ipForwDatagrams

ipInUnknownProtos

ipInDiscards

ipInDelivers

ipOutRequests

ipOutDiscards

ipOutNoRoutes

ipReasmTimeout

ipReasmReqds

ipReasmOKs

ipReasmFails

ipFragOKs

ipFragFails

ipFragreates

ipRoutingDiscards

imp

impInMsgs

impInErrors

impInDestUnreachs

impInTimeExds

impInParmProbs

impInSrQuenchs

impInRedirects

impInEchos

impInEchoReps

impInTimestamps

impInTimestampReps

impInAddrMasks

impInAddrMaskReps

impOutMsgs

impOutErrors

impOutDestUnreachs

impOutTimeExds

impOutParmProbs

impOutSrQuenchs

impOutRedirects

impOutEchos

impOutEchoReps

impOutTimestamps

impOutTimestampReps

impOutAddrMasks

impOutAddrMaskReps

tp

tpAtiveOpens

tpPassiveOpens

tpAttemptFails

tpEstabResets

tpurrEstab

tpInSegs

tpOutSegs

tpRetransSegs

tpInErrs

tpOutRsts

udp

udpInDatagrams

udpNoPorts

udpInErrors

udpOutDatagrams

snmp

snmpInPkts

snmpOutPkts

snmpInBadVersions

snmpInBadCommunityNames

snmpInBadCommunityUses

snmpInASNParseErrs

snmpInTooBigs

snmpInNoSuchNames

snmpInBadValues

snmpInReadOnlys

snmpInGenErrs

snmpInTotalReqVars

snmpInTotalSetVars

snmpInGetRequests

snmpInGetNexts

snmpInSetRequests

snmpInGetResponses

snmpInTraps

snmpOutTooBigs

snmpOutNoSuchNames

snmpOutBadValues

snmpOutGenErrs

snmpOutGetRequests

snmpOutGetNexts

snmpOutSetRequests

snmpOutGetResponses

snmpOutTraps

Link Discovery

The following MIB is related to link discovery.

LLDP-MIB

A primary means of determining physical links

lldpLocalSystemData

Obtains identification information for device

lldpLocChassisIdSubtype—used to understand format of chassis ID

lldpLocChassisId

lldpLoPortTable—obtain identification information for physical ports

lldpLocPortNum—obtained from oid instance

lldpLocPortIdSubtype—used to understand format of ID

lldpLocPortId—Maps to port in Dell OpenManage Network Manager model. Must be unique per device, expected to map to ifIndex, IfName, ifDescr or MAC address for physical port recorded in Dell OpenManage Network Manager model

lldpLocPortDes—optionally used to map to port in Dell OpenManage Network Manager model

lldpRemTable

Used to understand other end of link for physical port on device

lldpRemLocalPortNum—obtained from oid instance and mapped to port by way of local port table

lldpRemChassisIdSubtype—used to understand format of chassis ID

lldpRemChassisId—identifies the remote device

lldpRemPortIdSubtype—used to understand the format of the Port ID

lldpRemPortId—identifies the remote port on the remote device for other end of the link

RF1213-MIB

ipAddrTable

Used to understand IP Address to port mappings

ipAdEntAddr

ipAdEntNetMask

ipAdEntIfIndex

ipNetToMediaTable

Used to understand what ARP entries a given port has seen

ipNetToMediaIfIndex—mapped to port in Dell OpenManage Network Manager model for this device

ipNetToMediaPhysAddress—used to obtain Mac Address for Ethernet ports

ipNetToMediaNetAddress—used to get ip address

IP-FORWARD-MIB

ipidrRouteTable

used to understand IP routing information on device

ipidrRouteDest—obtained from oid instance

ipidrRouteMask

ipidrRouteNextHop

ipidrRouteIfIndex

ipidrRouteType

ipidrRouteProto

ipidrRouteStatus—used to filter on read

BRIDGE-MIB

dot1dBase

Used to obtain bridge address

dot1dBaseBridgeAddress

dot1dBasePortTable

Used to map Q-BRIDGE-MIB data for a port to an IfIndex then to the Dell OpenManage Network Manager model

dot1dBasePort—used for mapping index in tables in Q-BRIDGE-MIB to an ifIndex

dot1dBasePortIfIndex—used to map to a physical port in Dell OpenManage Network Manager model

dot1dStp

Used to understand STP setup on device

dot1dStpPortTable

Used to understand STP setup per port

Q-BRIDGE-MIB

dot1qBase

Used to understand VLAN setup and capabilities

dot1qMaxVlanId

dot1qMaxSupportedVlans

dot1qNumVlans

dot1qGvrpStatus

dot1qTpFdbTable

Used to understand what mac addresses have been seen by a port and on what VLAN

dot1qFdbId—obtained from oid instance

dot1qTpFdbAddress—obtained from oid instance

dot1qTpFdbPort—maps to BRIDGE-MIB dot1dBasePortTable to get ifIndex to map to Dell OpenManage Network Manager model

dot1qTpFdbStatus—used to filter entries read

dot1qVlanurrentTable

Used to get list of current VLANs configured on the device

dot1qVlanIndex—used to understand the VLAN ID

dot1qVlanurrentEgressPorts—used to understand mapping to ports

dot1qVlanurrentUntaggedPorts—used to understand mapping to ports

dot1qVlanStatus

dot1qPortVlanTable

Used to understand how a port is setup relative to VLAN's

dot1qPvid—used to understand how packets will be tagged

dot1qPortAeptableFrameTypes

dot1qPortGvrpStatus

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W