Technical white paper

HP Backup Navigator

Install and Configuration Guide

Table of contents

Executive summary

HP Backup Navigator is one of three products that support HP's Adaptive Backup and Recovery solution. Adaptive Backup and Recovery is an innovative approach to data protection based on the use of operational analytics targeting the day-to-day use of the backup infrastructure. More importantly this approach adds trending capabilities and predictive algorithms enabling IT teams to make decisions about the backup and recovery process before problems surface. As a core component of the Adaptive Backup and Recovery solution, HP Backup Navigator delivers an interactive web-based reporting and analytics tool that correlates related, but often disparate, pools of information presenting the content graphically in the form of customizable dashboards, graphs, charts, summaries, trending views and detailed information concerning the backup performance, capacity utilization and daily operational details. With HP Backup Navigator, organizations have access to the following:

• Application and infrastructure backup analysis to effectively prioritize backup operations

• Infrastructure performance monitoring to identify potential conflicts associated with interconnects between the source and target, media and session throughput rates.

• "What-if" scenarios to characterize backup datasets use a common federated deduplication model to potentially curb backup capacity requirements before the space is depleted.

• Capacity trending to expose current infrastructure utilization rates in conjunction with forward-looking, or predictions, gaps in the infrastructure where the backup and recovery needs are not going to be met.

• Quickly identify root-cause analysis with correlation and causation.

• Recommend solutions to optimize backup environments, as well as tune and correct backup policies to improve business continuity within your IT environment.

This document is intended to assist backup administrators and/or the IT staff with the setup, installation and configuration of the HP Backup Navigator product.

Planning and Preparation

HP Backup Navigator is deployed on RedHat Enterprise Linux (RHEL) 6.4 (rhn.redhat.com/rhn/software/downloads/SupportedISOs.do) and relies on MariaDB version 5.5.37 (www.mariadb.org) and Tomcat (www.tomcat.apache.org) version 7. An architectural overview of HP Backup Navigator and its relationship the HP Data Protector can be seen in Figure 1 below.
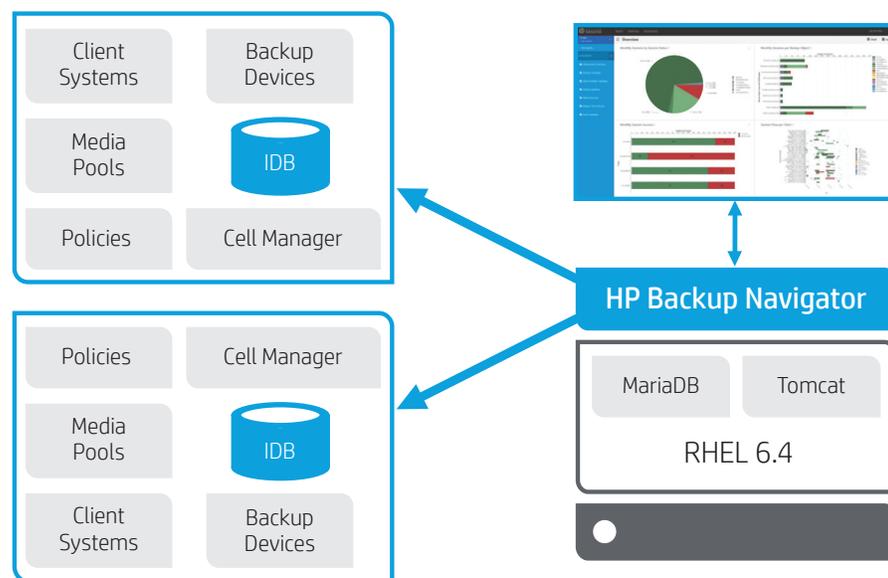
Figure 1: HP Backup Navigator – Architectural Overview

To begin, allocate the physical server or virtual machine for which HP Backup Navigator will run and install the RHEL operating system.

Hardware Requirements

At a minimum, the operating system, supporting components and HP's Backup Navigator software should be installed on a physical or virtual server with the following capabilities:

Criteria	Requirements	Notes
Operating system	Redhat Enterprise Linux	Version 6.4; 64 bit
Database server	MariaDB version	Version 5.5.37; non-clustered install
Web server	Apache Tomcat	Version 7
CPU	Dual Core (Physical/Virtual) Intel or AMD	2.0 Ghz or higher
Memory	16GB DDR4	64 bit; 288-Pin; 32GB recommended
Operating System hard disk space	6GB	7.2krpm SATA, 10krpm SAS or SSD
Database Server hard disk space	2GB	7.2krpm SATA, 10krpm SAS or SSD
Web Server hard disk space	500MB	7.2krpm SATA, 10krpm SAS or SSD
HP Backup Navigator hard disk space	30GB	7.2krpm SATA, 10krpm SAS or SSD; Database size will grow depending upon cyclic change rates and should be monitored for additional capacity requirements
Network	(4) 1GB Network Interface Cards	Isolated 1GB LAN segment with jumbo frame support recommended

Deploying RedHat Enterprise Linux

Begin by configuring the server to boot from the RHEL 6.4 ISO image or from DVD media that has the RHEL 6.4 operating system boot image loaded on it. During the boot process, accept the default options associated with disk setup and allocation as appropriate. When presented with the installation type screen, choose Basic Server along with Red Hat Enterprise Linux as an additional repository. Finally, ensure the option Customize Now option is selected before pressing the Next button as shown in Figure 2 below:
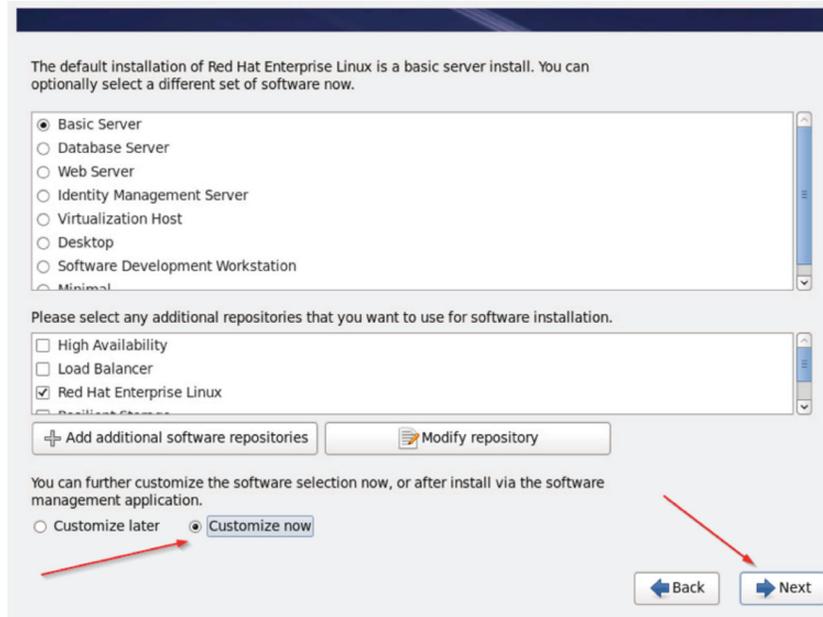
Figure 2: RHEL 6.4 - Package Installation Screen

Ensuring the Customize Now option is selected will modify the installation process and present a list of additional packages that can be installed. By default, the basic server installation type does not include a graphical user interface (GUI). While HP Backup Navigator does not require a GUI to operate, it is recommended that one is available to aid in the deployment and configuration of the product. To install a GUI, use the Customize Now screen, shown in Figure 3 below, choosing Desktops in the list on the left of the screen and Desktop and General Purpose Desktop options in the list on the right.
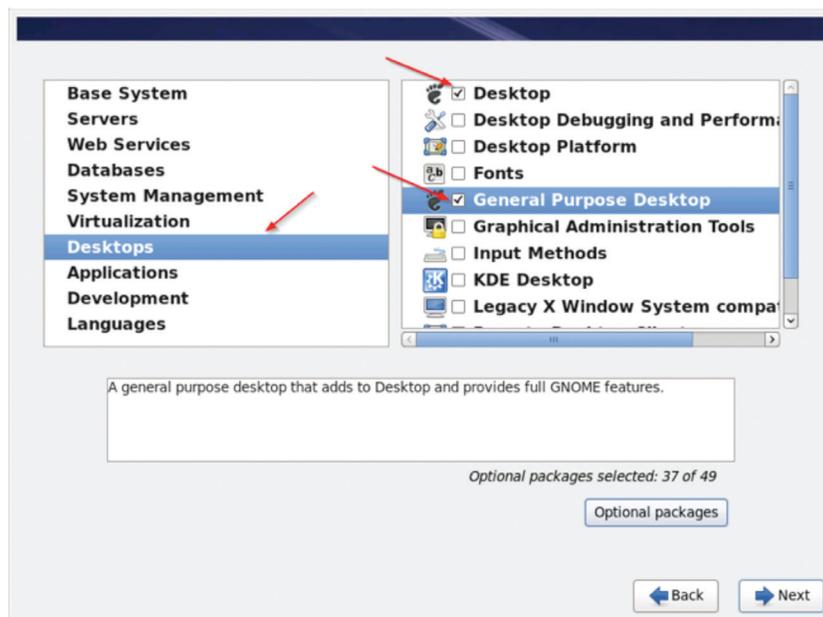
Figure 3: RHEL 6.4 - Graphical User Interface Options

Finally, to access the web-based interface of HP Backup Navigator from this server, a web browser is required. To install a web browser, select Applications in the list on the left and Internet Browser in the list on the right before pressing the Next button to complete the installation. This can be seen in Figure 4 below.
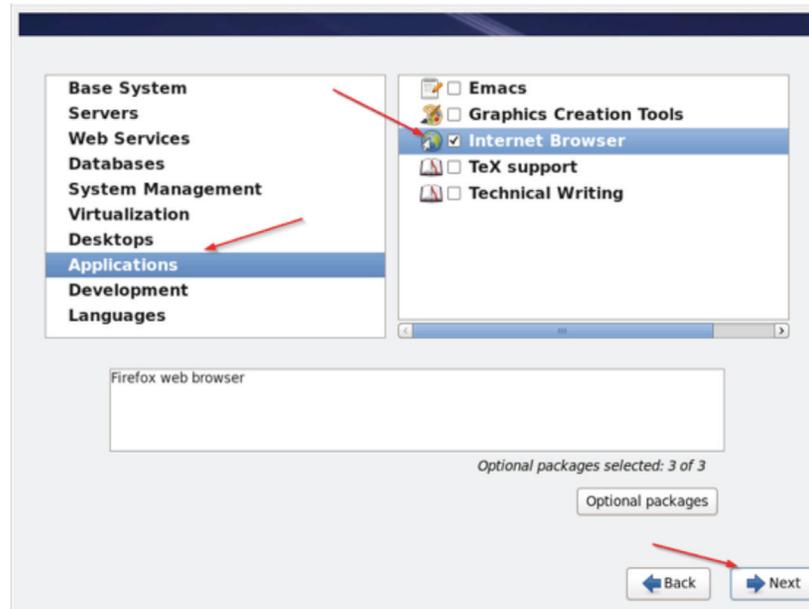
Figure 4: RHEL 6.4 - Additional Application Installation

This completes the necessary input to finalize the installation of RHEL 6.4. Upon completion of the installation, the server will indicate completion with the instructions that a reboot is required. Once the server reboots, a number of configuration steps are required before installing the additional components of HP Backup Navigator.

Configuring RedHat Enterprise Linux

To ensure a successful deployment, begin by verifying that the Domain Name System (DNS) is working correctly. Perform this verification by pinging another server on the network from the newly installed RHEL 6.4 server. Additionally, ensure server resolution occurs in both directions by using a separate server to ping the newly installed RHEL 6.4 server. It is recommended that this process validate connectivity using IP addresses, host names and fully qualified domain names. If a DNS Server is not available, the /etc/hosts file must be edited to manually add the IP address and host names for the HP Backup Navigator server and the HP Data Protector Cell Managers.

HP Backup Navigator requires port 5555 for access. Opening this port can be accomplished graphically using the Firewall Configuration Wizard (system-config-firewall) or using the command line interface (CLI). An example of the CLI code to open this port is listed below:

```
[root@localhost ~]# iptables –I INPUT –p tcp --dpport 5555 –j accept
```

Alternatively, the iptables file can be edited manually by making changes to the /etc/sysconfig/iptables file. Finally, if a firewall is not required, the firewall can be disabled by running the following commands:

```
[root@localhost ~]# service iptables save
[root@localhost ~]# service iptables stop
[root@localhost ~]# chkconfig iptables off
```

This concludes the necessary configuration steps to prepare the RHEL 6.4 operating system to host HP Backup Navigator.

Deploying MariaDB

HP Backup Navigator relies on the MariaDB relational database to store and correlate details of the HP Data Protector backup and recovery process. Before installing MariaDB, ensure there are no mysql libraries installed on the new RHEL 6.4 server by running the command:

```
[root@localhost ~]# rpm –qa | grep mysql
```

If the results of this command returns mysql-libs-5.1.71-1.el6.x86_64, or some derivate of it, the package must be removed before continuing. Removing this package can be accomplished with the following command:

```
[root@localhost ~]# sudo yum remove mysql-libs-5.1.71–1.el6.x86 _ 64
```

After ensuring that there are no instances of mysql on the new RHEL 6.4 server, it is recommended that a directory is created on the newly installed RHEL 6.4 server to store these files as they are downloaded. For example, create a root-level directory called /hp and store the files listed below in that directory.

MariaDB version 5.5.37 can be downloaded from www.mariadb.org by navigating to the Downloads page, selecting the link titled "Download 5.5.38" in the section titled "MariaDB 5.5 Series". From the list provided, selecting the "RedHat, Fedora and CentOS" RPM packages. This displays an index of the RPMs by processor type followed by subdirectories for the processor type. Select the processor type that matches the server that RHEL 6.4 was installed on. From the list of subdirectories, select RPMs and download the following files:

• MariaDB-5.5.37-centos6-x86_64-client.rpm

• MariaDB-5.5.37-centos6-x86_64-compat.rpm

• MariaDB-5.5.37-centos6-x86_64-devel.rpm

• MariaDB-5.5.37-centos6-x86_64-server.rpm

N.B. The Yellowdog Updater, Modified (YUM) service can also be used to download and install MariaDB If the newly installed RHEL 6.4 has an active internet connection. For more information on this process, refer to Appendix A.

When directly downloading the MariaDB files, change to the directory where the RPM files were downloaded and execute the following command:

```
[root@localhost ~]# sudo rpm –ivh MariaDB-*
```

An example of the output from this command is presented in the code-block below:

```
        [root@localhost ~]# cd /hp
        [root@localhost ~]# sudo rpm –ivh MariaDB-*
        Warning: MariaDB-5.5.37-centos6-x86 _ 64-client.rpm: Header V4 DSA/SHA1 Signature, key
        ID 1bb943db: NOKEY
Preparing…               #################################### [100%]
    1.  MariaDB-compat   #################################### [ 20%]
    2.  MariaDB-common   #################################### [ 40%]
    3.  MariaDB-client   #################################### [ 60%]
    4.  MariaDB-server   #################################### [ 80%]
    5.  MariaDB-devel    #################################### [100%]
[root@localhost ~]#
```

Once the MariaDB installation is complete, verify that the MariaDB configuration contains the *FederatedX Storage Engine for MySQL* by starting the mysql service and accessing the MariaDB monitor interface as shown below:

```
        [root@localhost ~]# service mysql start
        [root@localhost ~]# mysql
        MariaDB [(none)]> show engines
```

In the results that are displayed, ensure the *FEDERATEDX* engine is installed in the list from the above command, as shown in Figure 5.

```
MariaDB [(none)]> show engines;
+--------------------+---------+----------------------------------------------------------------+--------------+------+------------+
| Engine             | Support | Comment                                                        | Transactions | XA   | Savepoints |
+--------------------+---------+----------------------------------------------------------------+--------------+------+------------+
| CSV                | YES     | CSV storage engine                                             | NO           | NO   | NO         |
| MRG_MYISAM         | YES     | Collection of identical MyISAM tables                          | NO           | NO   | NO         |
| MEMORY             | YES     | Hash based, stored in memory, useful for temporary tables      | NO           | NO   | NO         |
| BLACKHOLE          | YES     | /dev/null storage engine (anything you write to it disappears) | NO           | NO   | NO         |
| MyISAM             | YES     | MyISAM storage engine                                          | NO           | NO   | NO         |
| InnoDB             | DEFAULT | Percona-XtraDB, Supports transactions, row-level locking, and foreign keys | YES | YES | YES |
| ARCHIVE            | YES     | Archive storage engine                                         | NO           | NO   | NO         |
| FEDERATED          | YES     | FederatedX pluggable storage engine                            | YES          | NO   | YES        |
| PERFORMANCE_SCHEMA | YES     | Performance Schema                                             | NO           | NO   | NO         |
| Aria               | YES     | Crash-safe tables with MyISAM heritage                         | NO           | NO   | NO         |
+--------------------+---------+----------------------------------------------------------------+--------------+------+------------+
10 rows in set (0.00 sec)
```

Figure 5: MariaDB – Show Engines Command

If the FederatedX engine is not listed, it can be manually installed using the command:

```
MariaDB [(none)]> install plugin federated soname 'ha_federated.so'
```

With the MariaDB installed and the FederatedX engine verified, the next step is to create the necessary roles within the database to support the HP Backup Navigator software.

Creating MariaDB Roles for HP Backup Navigator

HP Backup Navigator requires an administrator and additional user accounts within MariaDB. Creating this new user is done while still in the *mysql* command line context. Use the following commands to create the new user account:

```
MariaDB [(none)]> create user 'root'@'%';
MariaDB [(none)]> set password for 'root'@'%' =PASSWORD('password');
```

In the example above, the user name *root* and the password *root-password* are examples and should be replaced with the appropriate userid and password that is appropriate for the IT strategy. Passwords should be in lowercase and cannot contain the @ or = character.

To elevate the new user to an administrative level, the privileges for the new user must be set. This is accomplished using the following command:

```
MariaDB [(none)]> grant all privileges on *.* to 'root'@'%';
```

Finalizing the process requires an update and commit to the MariaDB tables by executing the following command:

```
MariaDB [(none)]> FLUSH PRIVILEGES;
```

Since MariaDB is installed on the same server as HP Backup Navigator, additional user accounts are required to be created in MariaDB for users accessing HP Backup Navigator to ensure role-based access and auditing can be supported. Creating the additional users is performed in a similar way as above:

```
MariaDB [(none)]> create user 'root'@'127.0.0.1';
MariaDB [(none)]> create user 'root'@'navigator-server-hostname';
MariaDB [(none)]> create user 'root'@'navigator-server.domainname';
```

In the above example, the root account is extended to associate it with the IP address of the local host, followed by the host name of the HP Backup Navigator server and then finally the fully qualified domain name of the HP Backup Navigator server. Additionally, these accounts can be created using a GUI. For more information on the GUI process, see Appendix B.

Updating the MariaDB Configuration File

The final step in preparing the MariaDB for use with HP Backup Navigator is to update the MariaDB configuration file. To begin, the default configuration file needs to be saved. Perform this action by renaming the existing file using the following command:

```
[root@localhost ~]# mv /etc/my.cnf /etc/my.cnf.original
```

During the setup of the MariaDB, configuration changes to the database were stored in a local configuration file that needs to be placed in the /etc directory. Perform this step by using the following command:

```
[root@localhost ~]# cp /usr/share/mysql/my-large.cnf /etc/my.cnf
```

Once the copy completes, edit the /etc/my.cnf file to add the following statements within the [mysqld] code-block of the file, as shown in Figure 6:

```
# The MariaDB server
[mysqld]
port            = 3306
socket          = /var/lib/mysql/mysql.sock
skip-external-locking
key_buffer_size = 256M
max_allowed_packet = 1M
table_open_cache = 256
sort_buffer_size = 1M
read_buffer_size = 1M
read_rnd_buffer_size = 4M
myisam_sort_buffer_size = 64M
thread_cache_size = 8
query_cache_size= 16M
# Try number of CPU's*2 for thread_concurrency
thread_concurrency = 8
federated
max_connections=1500
```

Figure 6: MariaDB - /etc/my.cnf File

```
federated
max _ connections=1500
```

Once changes are made to the /etc/my.cnf file, the MariaDB service must be restarted. This is accomplished with the following commands:

```
[root@localhost ~]# service mysql stop
[root@localhost ~]# service mysql start
```

This completes the necessary changes and modifications to complete the MariaDB deployment for use with HP Backup Navigator. The next step is to deploy and configure Apache Tomcat.

Deploying Apache Tomcat

Apache Tomcat is the web service that is required to provide access to HP Backup Navigator. Download the apache-tomcat-7.0.53.tar.gz file from the apache distribution website (*archive.apache.org/dist/tomcat/tomcat-7/v7.0.53/bin/*) and move the file into the /opt directory. Use the following commands to deploy the Tomcat service:

```
[root@localhost ~]# ln –s /opt/apache-tomcat-7.0.53 /opt/apache-tomcat
```

Once this command completes, edit the *catalina.sh* file located in /opt/apache-tomcat/bin and add the following statement:

```
JAVA _ OPTS="-Djava.awt.headless=true –Dfile.encoding=UTF-8 –server –Xms3536m –Xmx3536m –
XX:MaxPermSize=1524m –XX:+DisableExplicitGC"
```

The results are shown in Figure 7 below:

```
#               -agentlib:jdwp=transport=$JPDA_TRANSPORT,
#                   address=$JPDA_ADDRESS,server=y,suspend=$JPDA_SUSPEND
#
#   CATALINA_PID   (Optional) Path of the file which should contains the pid
#                   of the catalina startup java process, when start (fork) is
#                   used
#
#   LOGGING_CONFIG  (Optional) Override Tomcat's logging config file
#                   Example (all one line)
#                   LOGGING_CONFIG="-Djava.util.logging.config.file=$CATALINA_BASE/conf/logging.properties"
#
#   LOGGING_MANAGER (Optional) Override Tomcat's logging manager
#                   Example (all one line)
#                   LOGGING_MANAGER="-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager"
# --------------------------------------------------------------------------
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms3536m -Xmx3536m -XX:PermSize=1524m -XX:MaxPermSize=1524m -XX:
+DisableExplicitGC"

# OS specific support.  $var _must_ be set to either true or false.
```

Figure 7: Tomcat – Modified catalina.sh File

Once modified and save, the Tomcat service should be started using the following command:

```
[root@localhost ~]# cd /opt/apache-tomcat/bin
[root@localhost ~]# ./startup.sh
```

Verify that the Tomcat service is running by opening a web browser and entering the name of the server followed by the 8080 port (i.e. http://myserver:8080) as shown in Figure 8.
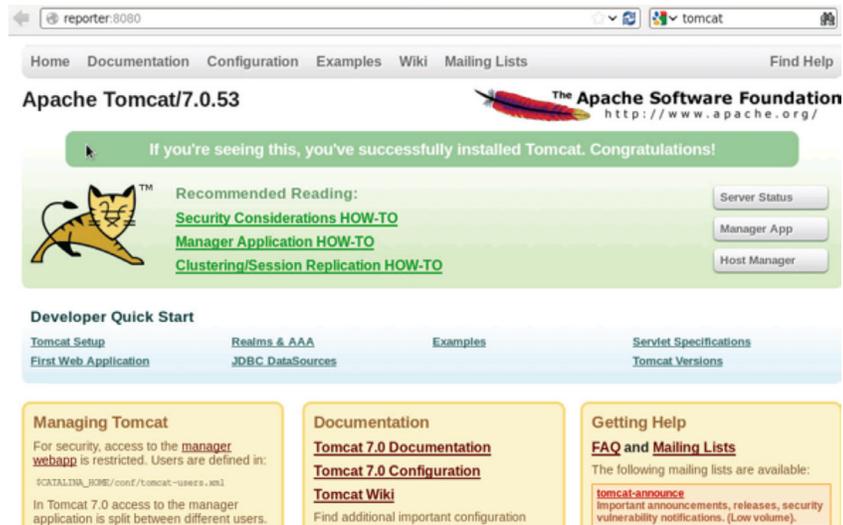
Figure 8: Tomcat – Modified catalina.sh File

With the MariaDB and the Tomcat service installed and running, the final step is the installation and configuration of HP Backup Navigator.

Deploying HP Backup Navigator

HP Backup Navigator can be downloaded from www.hp.com/go/dataprotector and should be stored on the RHEL 6.4 server it will run on. Once downloaded, mount the ISO image using the following command:

```
[root@localhost ~]# mkdir –p /mnt/iso
[root@localhost ~]# mount –o loop navigator.iso /mnt/iso
[root@localhost ~]# cd /mnt/iso
```

With the image mounted, use the following command to install HP Backup Navigator:

```
[root@localhost ~]# rpm –ivh hp-backup-navigator-8.0-1el6.x86 _ 64.rpm
```

Following the installation of Backup Navigator, the installation process displays the user name (admin) and a randomized unique password to be used for the initial login to the application. While the password can be changed later, it is recommended that the password is written down or copied to a file for later reference. Figure 9 provides an example of this point in the installation process.

Figure 9: HP Backup Navigator – Login Credentials

During the HP Backup Navigator installation, changes are made to the MariaDB and the Tomcat installation that require these services to be shutdown and restarted for the changes to take effect. Use the following commands, in the order presented, to perform these actions:

```
[root@localhost ~]# cd /opt/apache-tomcat/bin
[root@localhost ~]# ./shutdown.sh
[root@localhost ~]# service mysql stop
[root@localhost ~]# service mysql start
[root@localhost ~]# ./startup.sh
```

Following these actions, open a web browser and connect to the server using the format *hostname:8080*, where hostname is the name of the newly installed RHEL server hosting these applications. Figure 10 demonstrates the expected results from this navigation:
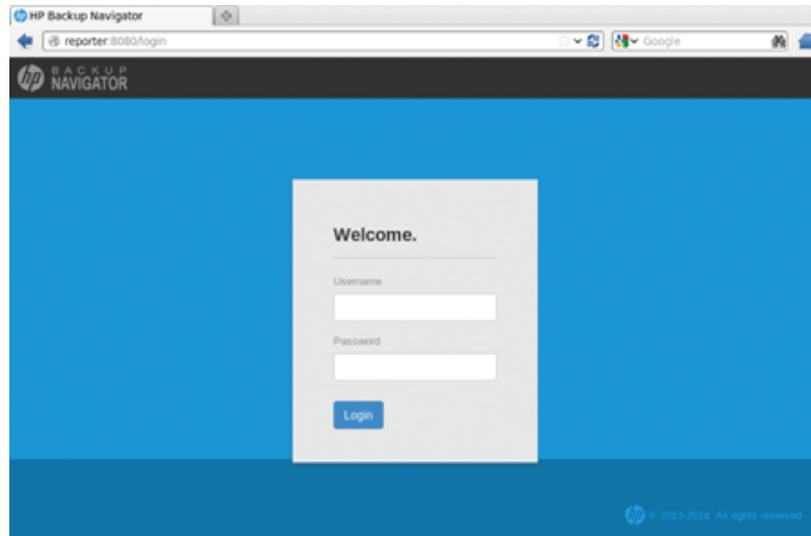
Figure 10: HP Backup Navigator – Welcome Screen

Using the user id *admin* followed by the randomly generated password, created during the installation process, login to complete the setup process as show in Figure 11.
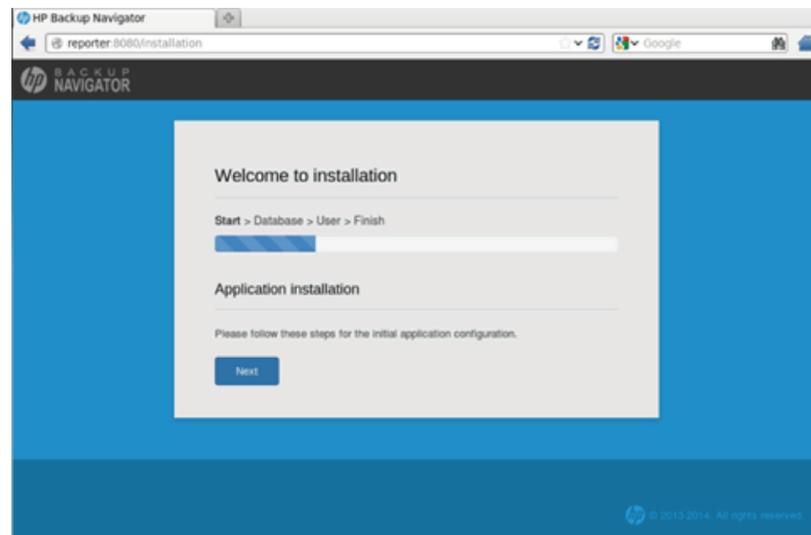
Figure 11: HP Backup Navigator – Welcome Screen

During the setup process, HP Backup Navigator will deploy the database into the MariaDB installation. Performing this action requires additional user input during installation. When prompted, the user must supply the hostname of the MariaDB server using the fully qualified domain name, the MariaDB root administrator account and password (created earlier in this document), and the name of the database that will be created to host the HP Backup Navigator data. This is demonstrated in Figure 12.
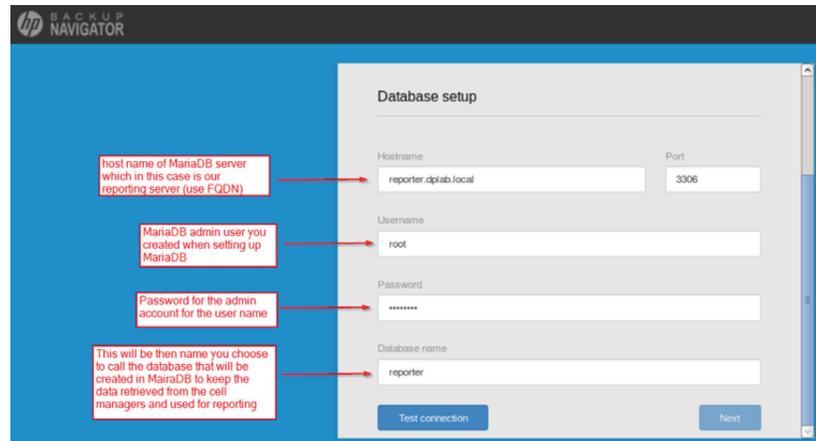
Figure 12: HP Backup Navigator – MariaDB Database Creation

Before continuing, use the Test Connection button to verify that a successful connection to the MariaDB server can be made using the credentials supplied. If a failure to connect occurs, check the hostname, username and password and try again.

If a subsequent failure occurs, ensure the MariaDB service is running on the server by using the following command:

```
[root@localhost ~]# service mysql status
```

Use the commands from the previous section to start the service if the results indicate the service is not running.

Upon successfully testing the connection, pressing the next button will complete the deployment of the database structure that HP Backup Navigator relies on. This success is displayed in the installation progress bar.

The final installation step is to create a user id for HP Backup Navigator. The admin user id, presented during the installation, is reserved and cannot be used during this step. Instead, specify a new user id and password combination (i.e. *administrator*) and use the *Create New User* button as shown in Figure 13.
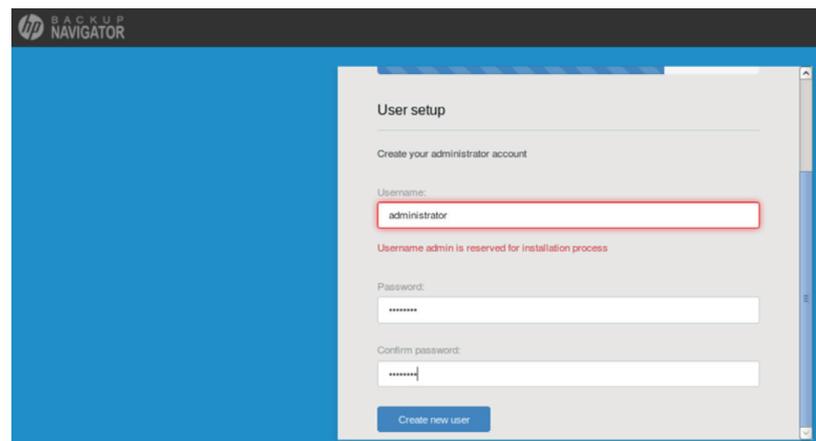
Figure 13: HP Backup Navigator – Create New User

This completes the installation and setup of HP Backup Navigator. Use the *Take Me to Application* button to end the setup and login to HP Backup Navigator as show in Figures 14 and 15.
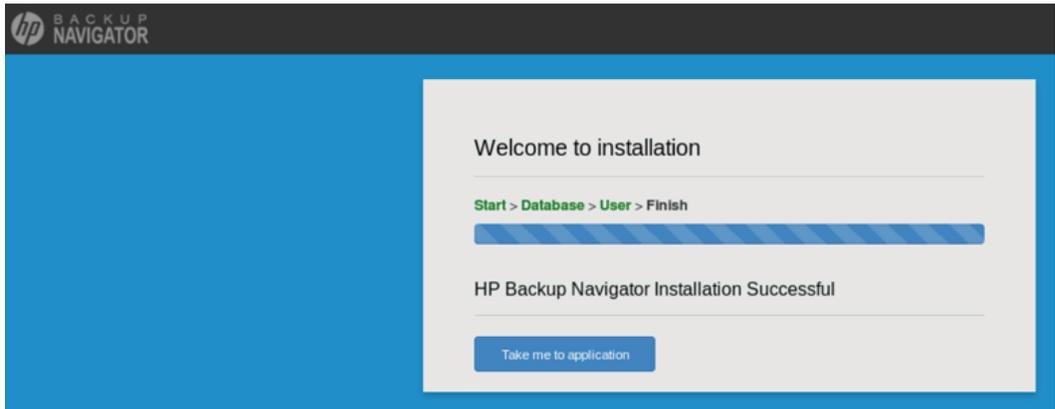
Figure 14: HP Backup Navigator – End of Setup
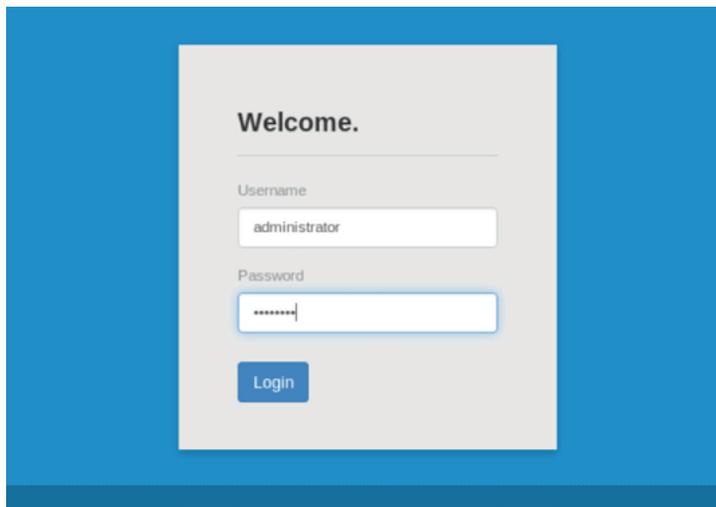
Figure 15: HP Backup Navigator – End of Setup

Successful login will display the default home screen of HP Backup Navigator shown in Figure 16.
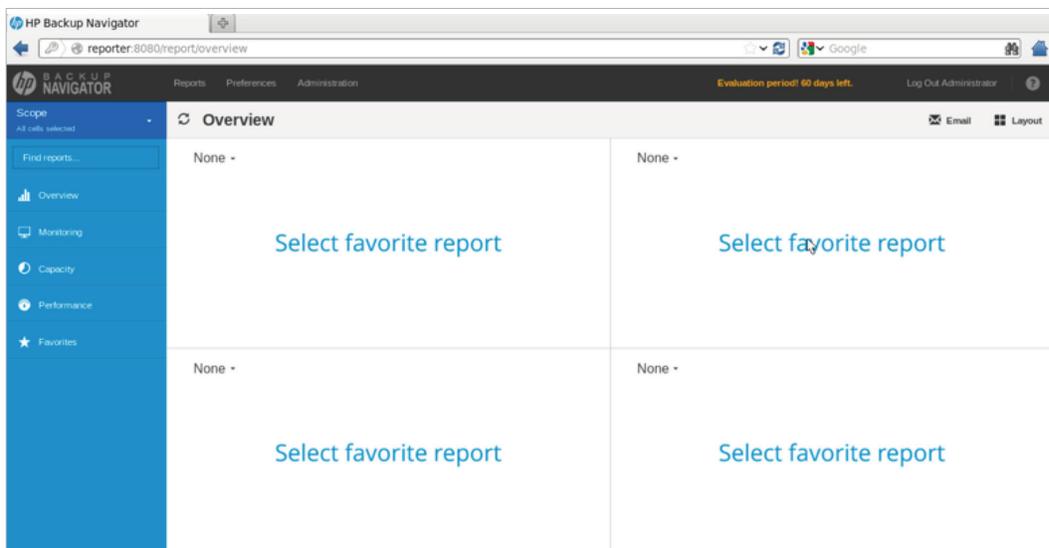
Figure 16: HP Backup Navigator – Home Page

Configuring HP Backup Navigator

With HP Backup Navigator installed, the final step is to configure the HP Data Protector Cell Manager relationship. Creating these relationships binds HP Backup Navigator to specific cells that it will begin collecting backup related information that can be used in monitoring, reporting, trending, and running simulations. To accomplish this, HP Data Protector must be updated to include the HP Backup Navigator userid and password to enable access to the internal HP Data Protector database where much of this information is stored.

As shown in Figure 17, login to the HP Data Protector interface as administrator and navigate to the Users section of Data Protector. Here, the HP Backup Navigator *Administrator* account, created during the setup process is added to the *admin* user group.
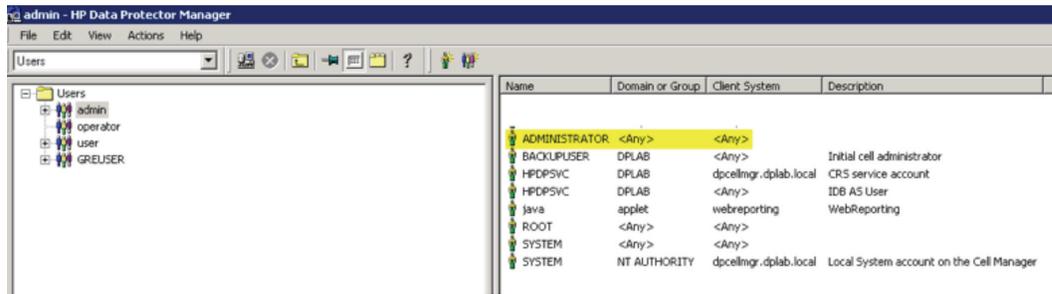
Figure 17: HP Backup Navigator – Add HP Backup Navigator Admin Account

Returning back to HP Backup Navigator, the communication with the Data Protector Cell Managers can be completed. To perform this action, use the Administration link in the title bar, as shown in Figure 18, to add the Data Protector Cells.
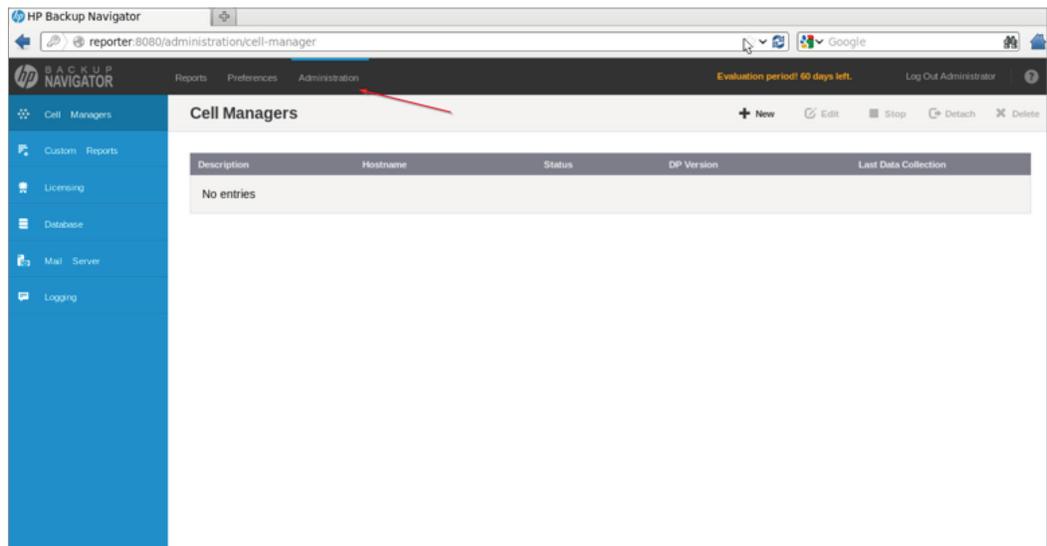
Figure 18: HP Backup Navigator – HP Data Protector Cell Details

To add a new HP Data Protector Cell Manager, use the *+New* button as shown in Figure 19.
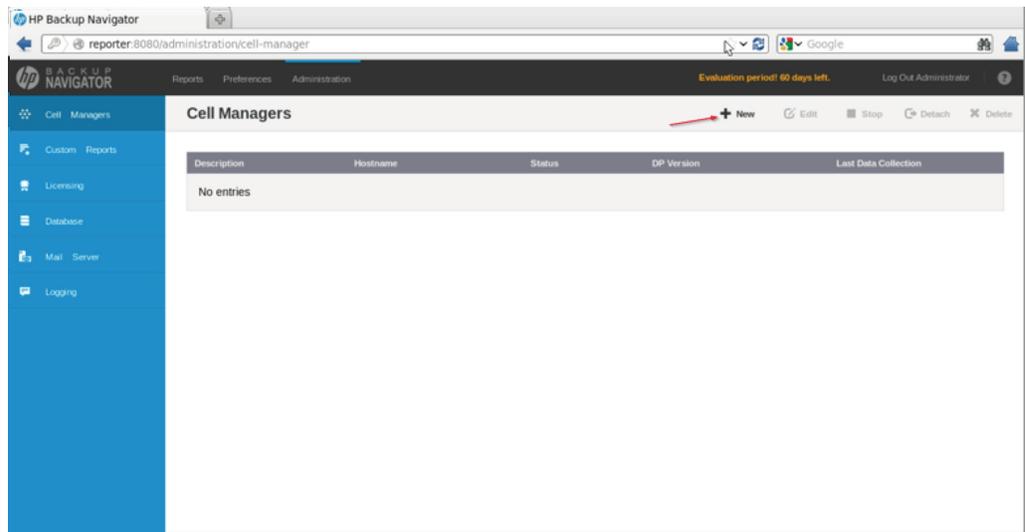
Figure 19: HP Backup Navigator – Add New Data Protector Cell Manager

Creating a new relationship with the HP Data Protector Cell Manager requires additional inputs that include the host name, a description of the Cell Manager, the HP Backup Navigator data base details, and the timeframe and interval for collecting Data Protector details. This is shown in Figure 20 below.
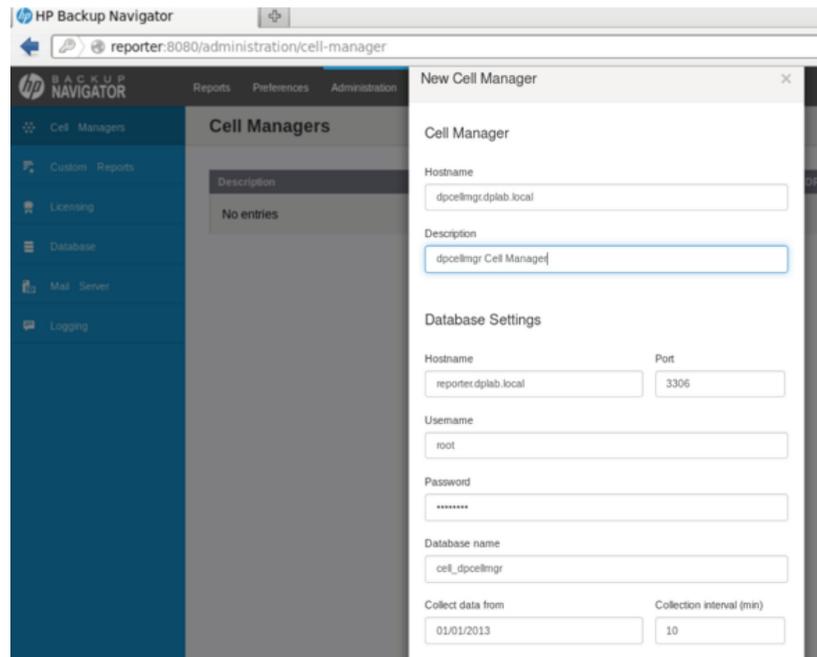
Figure 20: HP Backup Navigator – Configuring the Data Protector Cell Manager Relationship

Once configured, the list of associated Data Protector Cell Managers is updated to reflect the relationship, as shown in Figure 21 below. Perform these actions for all Data Protector Cell Managers that will be monitored by HP Backup Navigator.
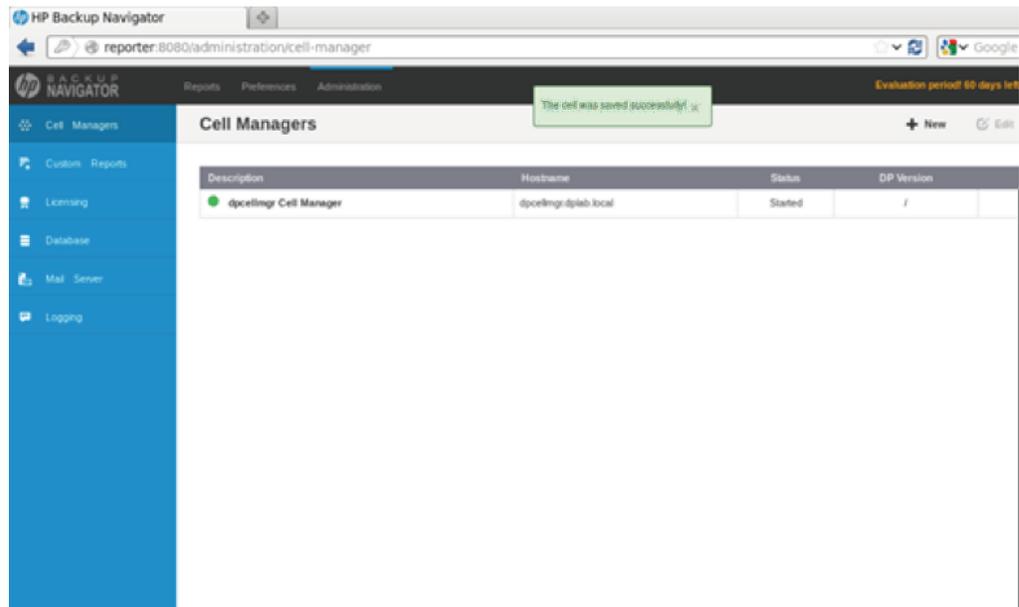
Figure 21: HP Backup Navigator – Successful Data Protector Cell Manager Relationship

With the relationships established, the monitoring scope of HP Backup Navigator can be changed to affect the default dashboard view. To accomplish this, use the *Scope* drop down control on the HP Backup Navigator main screen as shown in Figure 22.
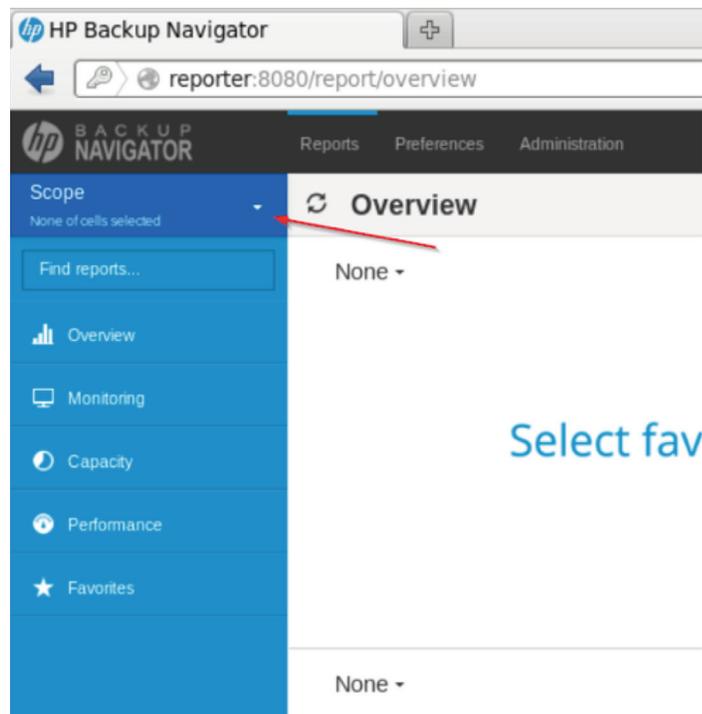
Figure 22: HP Backup Navigator – Scope Change

The monitoring scope can be inclusive or selective of the associated Data Protector Cell Managers. Select the option most appropriate to monitor *All* of the associated Cell Managers, or selectively choose which Cell Managers to monitor. Figure 23 demonstrates this option.
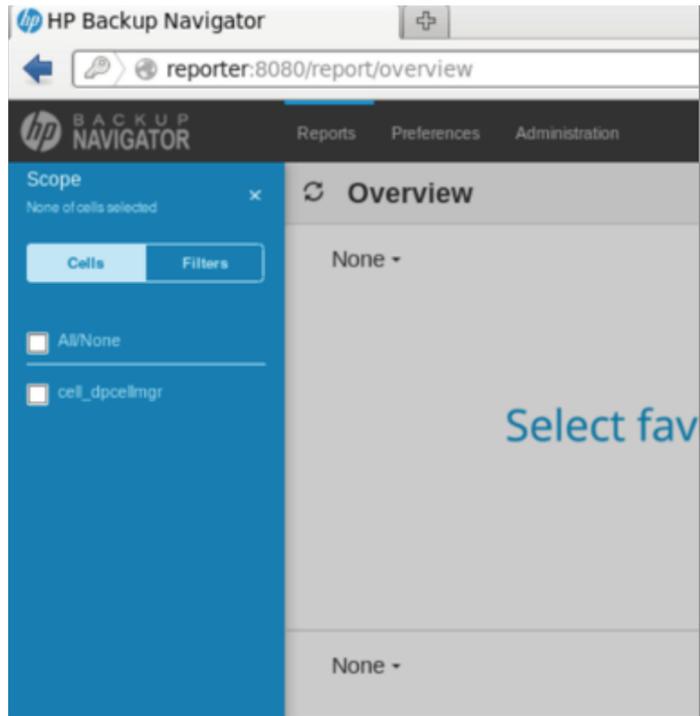
Figure 23: HP Backup Navigator – Scope Details

Once complete, HP Backup Navigator updates the reporting interface to reflect the data collected from the selected Data Protector Cell Managers, as shown in Figure 24.
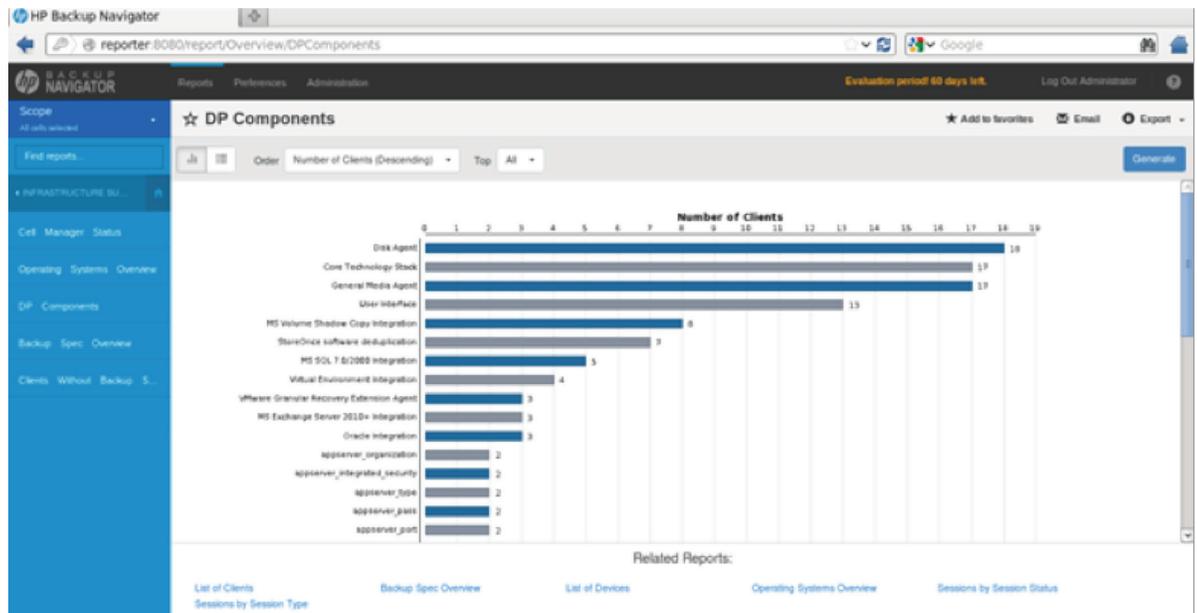
Figure 24: HP Backup Navigator – Updated Reports

Conclusion

HP Backup Navigator provides an intuitive and interactive web-based solution for correlating the details associated with HP Data Protector backup and recovery operations. Using this technical white paper, administrators can use step-by-step instructions to download and install the open source components that HP Backup Navigator relies on.

While much of this process can be seen as manual, the rules related to open source distribution are very explicit and, in this case, prevent HP from publishing Backup Navigator as a single installable form of media.

Learn more at

www.hp.com/go/convergedsystems

www.hp.com/go/3par

www.hp.com/go/burasolutions

www.adaptive-backup.com

www.autonomy.com/products/data-protector

About HP Autonomy

HP Autonomy is a global leader in software that processes unstructured human information, including social media, email, video, audio, text, web pages, and more. Using HP Autonomy's information management and analytics technologies, organizations can extract meaning in real time from data in virtually any format or language, including structured data. A range of purpose-built market offerings help organizations drive greater value through information analytics, unified information access, archiving, eDiscovery, enterprise content management, data protection, and marketing optimization.

Please visit **autonomy.com** to learn more.

Appendix A: Deploying Maria DB via Yellowdog Updater Modified (YUM)

To use the YUM service to download the MariaDB files, follow the instructions located at downloads.mariadb.org/mariadb/repositories/#mirror=syringa using the download website to specify the distribution (RedHat), the release (Red Hat EL 6 32-bit), and the version (5.5) as shown in Figure 25.
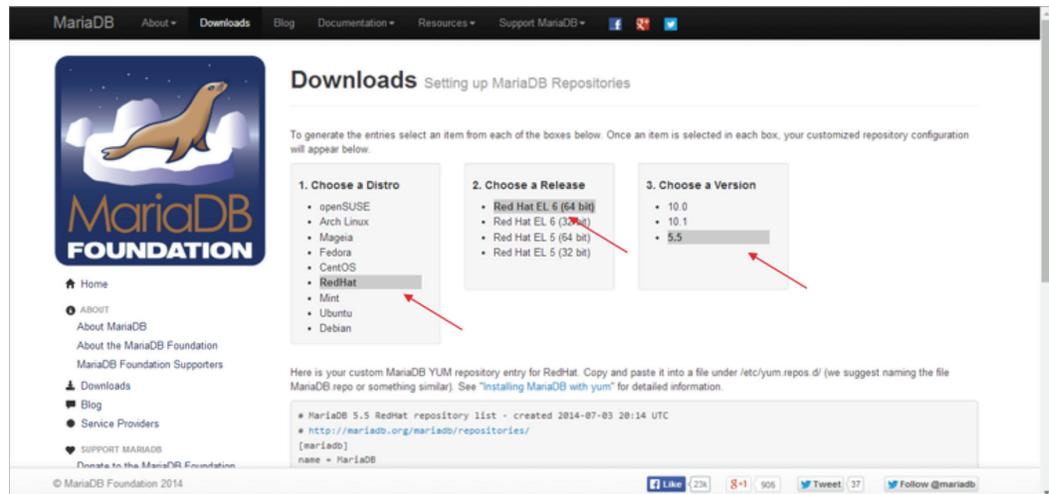
Figure 25: MariaDB Repositories for YUM Installation

Making these choices results in the specific YUM repository entries required to install the MariaDB using this service. The results generated must be copied and pasted into a new file and stored in the /etc/yum.repos.d directory on the RHEL 6.4 server. It is recommended that the output, listed below, be placed into a file titled MariaDB.repo and must be stored in the /etc/yum.repos.d/.

```
mariadb]
name=MariaDB
baseurl=http://yum.mariadb.org/5.5/rhel6-x86
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Once this file is saved, the following command can be executed to initiate the install:

```
[root@localhost ~]# sudo yum install MariaDB-server MariaDB-client MariaDB-compat
MariaDB-devel
```

Appendix B: Creating MariaDB User Account via SQLyog

SQLyog is a graphical user interface frontend for MySql. This application can be used to create the user accounts required for HP Backup Navigator and the MariaDB service. To download this application, open a web browser and navigate to the open source communities page at code.google.com/p/sqlyog. The product will need to be installed on a Microsoft Windows server that has access to the MariaDB installation. Upon successful installation, the application opens to its default view show in Figure 26 below.
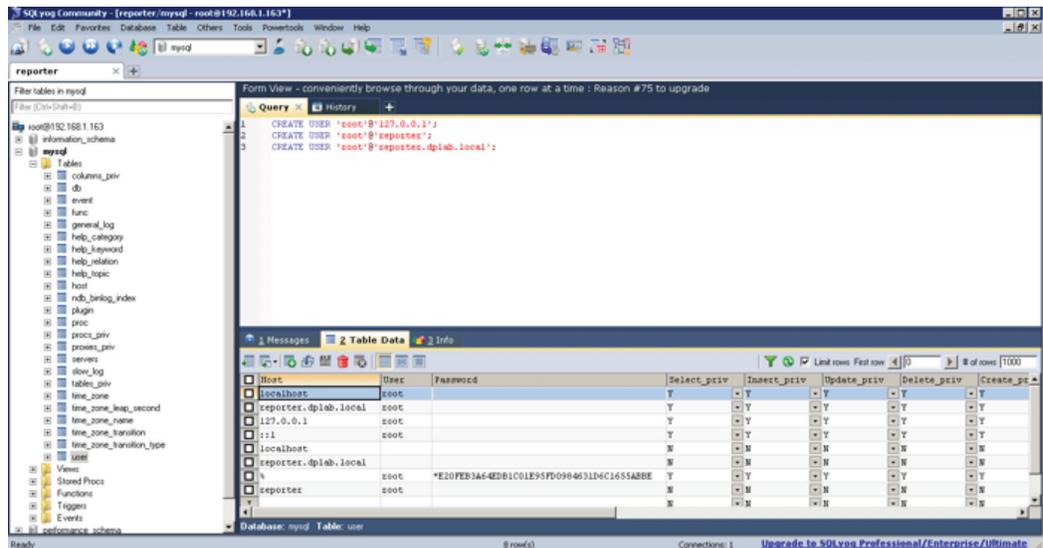
Figure 26: SQLyog – Application Main Screen

Using this application, the user accounts, passwords and privileges are created similar to the commands presented earlier in this document. Figures 27 and 28 provide additional detail on creating the user accounts and setting their passwords.
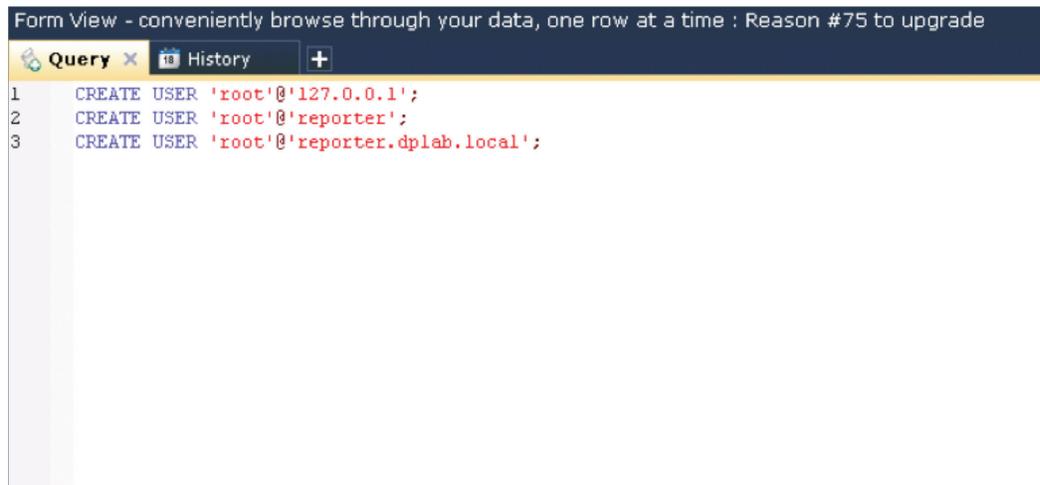
Figure 27: SQLyog – Creating User Accounts
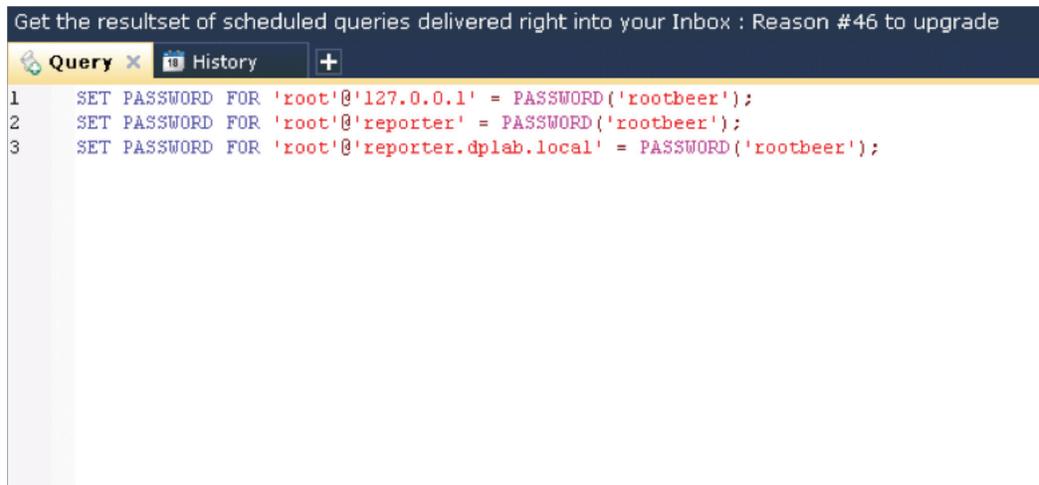
Figure 28: Lyog – Setting User Account Passwords

Finally, the privileges for these users must be set, which can be accomplished using the following commands:

```
grant all privileges on *.* to 'root'@'127.0.0.1';
grant all privileges on *.* to 'root'@'localhost';
grant all privileges on *.* to 'root'@'hostname.domainname';
```

Sign up for updates
hp.com/go/getupdated

Share with colleagues