Backup Navigator

Software Version: 10.20

Linux and Windows operating systems

User Guide

Document Release Date: November 2018
Software Release Date: November 2018

Legal notices

Warranty

Restricted rights legend

Copyright notice

Trademark notices

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

To check for recent software patches, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=.

This site requires that you register for a Passport and sign in. To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Or click the **Register** link at the top of the Micro Focus Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Micro Focus sales representative for details.

Support

Visit the Micro Focus Software Support Online web site at https://softwaresupport.softwaregrp.com/.

This web site provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Manage software licenses
- Download new versions of software or software patches
- Access product documentation
- Manage support contracts
- Look up Micro Focus support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Contents

Chapter 1: Introduction

Backup Navigator is a web-based application that provides an additional reporting functionality for your Data Protector and VM Explorer backup environments. It is a comprehensive and scalable tool, which enables you to create, generate, and deliver a wide range of reports for the web browser-based presentation and user-defined exploration.

In the web user interface you can generate numerous predefined reports on different aspects of the Data Protector and VM Explorer environments, create the reports of your choice, and export them to various formats. Predefined reports provide information on the major elements of the application specific environment, such as, infrastructure, media management, devices, sessions and tasks, capacity and performance, as well as occurred errors. For Data Protector, you can monitor active backup sessions, get a list of most unreliable media, track the backup volume growth, check the transfer rate during the restore sessions, analyze trends in backup capacity changes, make future predictions, and so on.

Backup Navigator supports multitenant Data Protector environment and can provide reports also for tenants, if you define them. A tenant is a group of users, usually related to one customer or department, who share Data Protector resources. Each tenant is represented by the dedicated Data Protector elements, such as cells, backup specification groups, backup specifications, or clients.\

Backup Navigator provides an opportunity to assign different categories to a backup application depending on its service level objective (SLO). SLO category refers to a combination of the RTO (a time period needed before an application is brought back online) and the RPO (a time period when data can be lost after an event that causes an application to go offline occurs), which are specific for your backup environment goals. SLO categories are used for monitoring your backup applications.

The key tasks of Backup Navigator are:

- Recognizing the Data Protector Cell Manager and VM Explorer Server systems that provide input data for your reports.
- Collecting data from the application environment.
- Generating reports from the collected data considering user-defined scope and parameters.
- Recognizing problems in the monitored environment and issuing alerts and notifications.

Backup Navigator benefits

- Central monitoring of multiple servers
- Simplified tracking of infrastructure changes across the entire application environment
- Overview of backup resources
- Performance, capacity trending, and future planning
- Simplified error analysis
- Customizable reporting and dashboard
- Notifications and alerts on specified events
- Multitenant environments support

Backup Navigator features

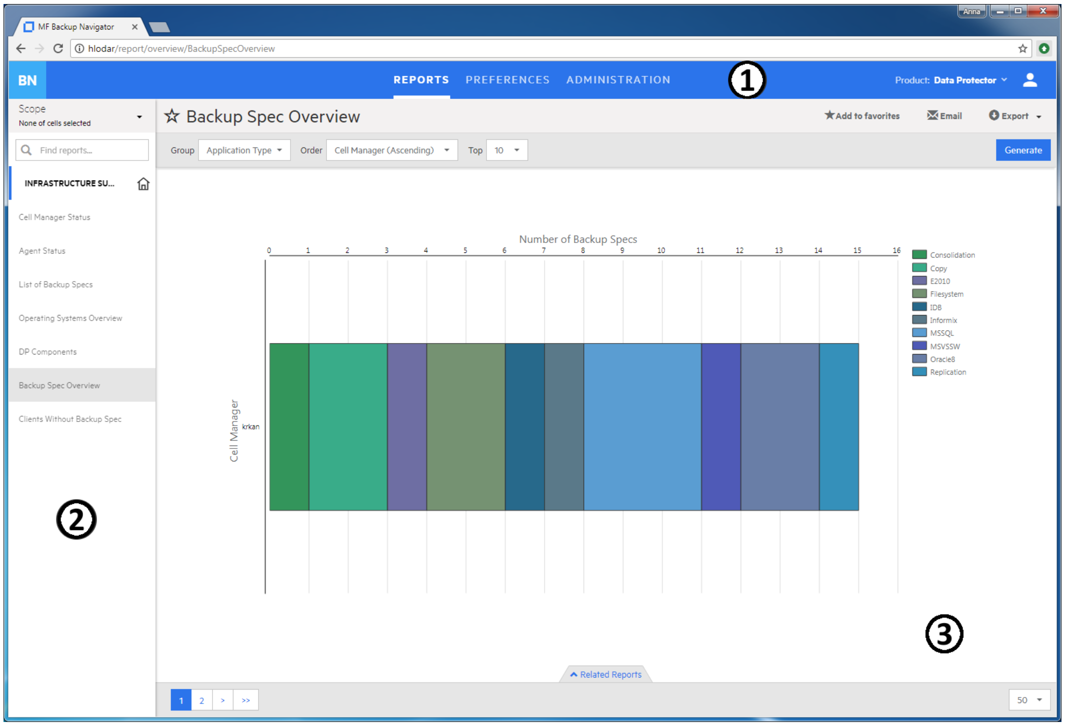
You can benefit from the following Backup Navigator features:

- Select the Data Protector and VM Explorer cells or tenants[1], from which you want to receive the input data for your reports.
- Use a remote agent to collect data from the Data Protector cells that cannot be directly accessed from Backup Navigator.
- Use a Summary dashboard for an at-a-glance overview of your Data Protector backup environment.
- Create reports of your choice with the same available options as predefined reports.
- Configure the dashboard to display the reports in the way which is convenient for you to view them.
- Switch between the chart and table presentation of the report.
- Examine report data in more detail by using the drill-down functionality.
- Add a report to your favorites to access it quicker.
- Subscribe to your favorite report to receive it regularly by email.
- Export the reports output to various formats.
- Navigate from the selected report to other reports with the related content and the same scope.
- Customize report charts by sorting data according to different available parameters.
- Group your backup applications depending on their service level objective.
- Monitor your Data Protector environment by using predefined and custom Backup Navigator monitors.
- Get alerts or event notifications on the events in Data Protector and VM Explorer, including error states and failures.
- Backup Navigator retrieves only the data, which is needed for a report presentation at the time. This enhances performance by saving the time and the resources that would be needed to load all available data.

[1] For some reports, selecting tenants is not applicable.

Backup Navigator web user interface

Figure 1: Backup Navigator web user interface



1 Menu Bar

2 Navigation Pane

3 Results Area

You can switch between the Data Protector and VM Explorer environments.

> **NOTE:** Some user interface elements may differ depending on the backup application you are switched to.

The elements of the Backup Navigator web user interface are:

- **Menu Bar**

  The Menu Bar is an upper bar of the Backup Navigator web user interface. Depending on your user rights, you can access all or only some of the following contexts:

  Reports

  The predefined reports are logically grouped in four report categories (Overview, Monitoring, Capacity, Performance). You can generate reports, add reports to your favorites, subscribe for reports, and export a report to various formats.

  Preferences

  You can configure your personal settings, specify input data filters, and manage your subscriptions.

Administration (available for users with the administrator's user rights):

You can specify from which cells you want to collect input data for your reports. Manage your input data by adding new Data Protector Cell Managers or VM Explorer Servers to the data collection, starting or stopping input data collection on the specific server, detaching the specific server from or attaching them back to the Backup Navigator. You can also create and manage your SLO categories, custom reports, perform licensing related tasks, view events and configure event monitors, configure your mail server and logging settings, view your database settings, and manage your users, tenants, and tenant groups (discover, import, and maintain them).

Notification

Access and view the Backup Navigator events. If monitors are specified for the events of a higher severity and such events occur, alarms are raised and displayed next to the icon.

Help

Access the *Backup Navigator User's Guide* with introduction to Backup Navigator and instructions on how to use it. The About dialog provides information on the Backup Navigator current version.

- **Navigation Pane**

  The Navigation Pane is a left side panel of the Backup Navigator web user interface. You can switch between different items to view them or to change them in the Results Area. When you select an item in the Navigation Pane, the corresponding information is displayed in the Results Area.

  The content of the Navigation Pane is context specific. For example, the Reports context provides scope settings, search report functionality, a list of report categories and subcategories, and favorite reports. In the Preferences and Administration contexts, you can select an item to specify or change the corresponding configuration settings, such as user profile or logging settings.

- **Results Area**

  The Results Area is a central area of the Backup Navigator web user interface. It displays information that corresponds to the item selected in the Navigation Pane.

  In the Reports context, the Results Area is represented as a dashboard with a configurable layout, or as a report output, when a specific report is selected. You can view the selected report, generate it with different parameters, switch to the table presentation of the report, see the related reports, export the report to different formats, send it by email, and subscribe to the report.

  In other contexts, you can specify or change the configuration settings of the item selected in the Navigation Pane.

Chapter 2: Installation and Configuration

The Backup Navigator environment is a set of systems that obtain, manage, and analyze the specified data from the application environment (Data Protector or VM Explorer), and present it as reports in the web-based application. The environment consists of the following parts:

- **Backup Navigator system**

  A system where Backup Navigator resides. Backup Navigator processes the data collected in the application environment and presents it as specific reports in the web user interface. A database that contains the Backup Navigator functionality related data, the data collected from the application sessions, and the Data Protector cell infrastructure related data also resides on the Backup Navigator system.
- **Backup Navigator remote agent system**

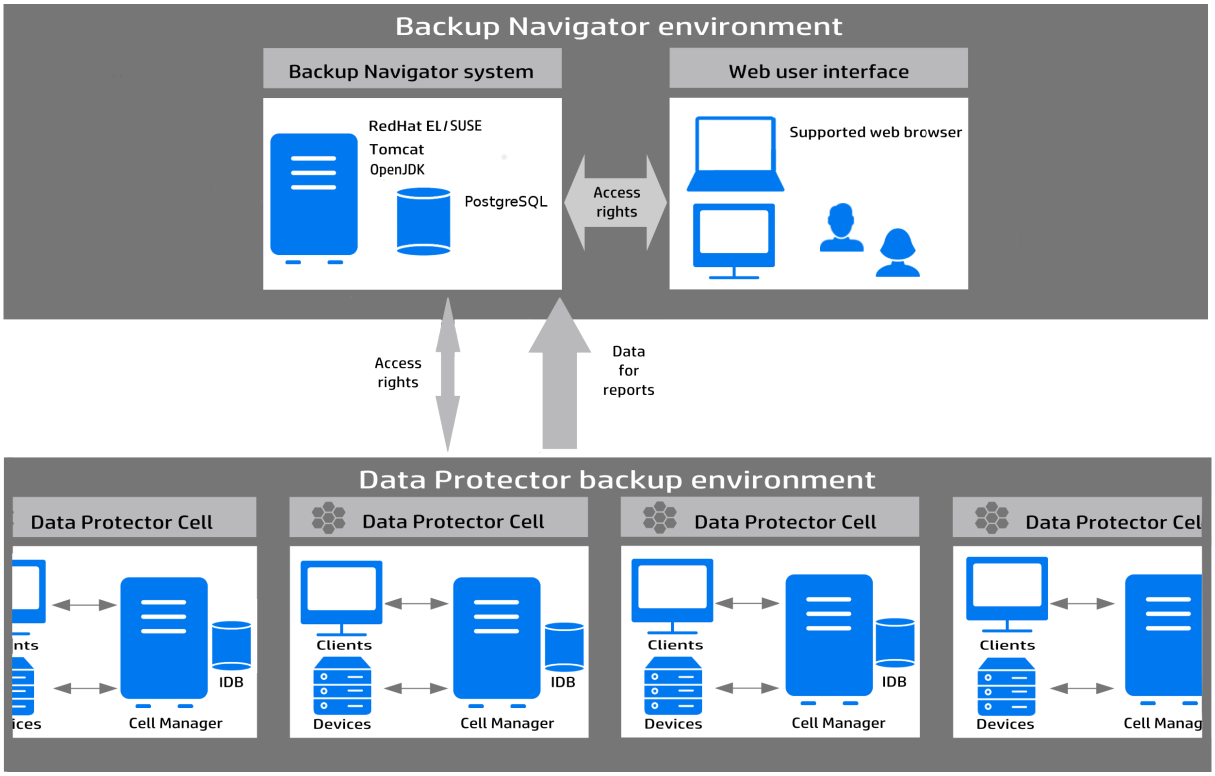
  If you want to collect data from the Data Protector cells, which you cannot or due to any reasons do not want to access from Backup Navigator, you can use a Backup Navigator remote agent to access such cells. You can install as many remote agents, as you need. Backup Navigator remote agent collects data from the Data Protector cells and provides it to Backup Navigator through HTTP protocol.
- **Backup Navigator web user interface**

  A system with a web browser, from which you access Backup Navigator. The web user interface also provides administration tools to adjust the environment to your needs. Backup Navigator web user interface has an established connection to the Backup Navigator system.
- **Application environment**

  A backup environment (Data Protector or VM Explorer), from which you collect data for your reports.

This diagram shows the Backup Navigator environment and its elements as well as how Backup Navigator interacts with Data Protector:

Figure 2: Backup Navigator environment



Prerequisites

Before installing Backup Navigator, consider the following:

Backup Navigator system prerequisites

- One of the supported operating systems. For a list of the supported operating systems, see *Backup Navigator Support Matrix*.
- System requirements

  System requirements depend on the backup application you monitor with Backup Navigator:

Size	Application environment	Minimum system requirements
Small	**100** sessions/tasks per server per day **100-500** object/task element versions per server per day	**Processor:** 64-bit two-core **RAM:** 8 GB **Hard disk:** 100 GB
Medium	**100-2000** sessions/tasks per server per day **500-10000** object/task element versions per	**Processor:** 64-bit four-core **RAM:** 16 GB

Size	Application environment	Minimum system requirements
	server per day	**Hard disk:** 160 GB
Large	**2000-4000** sessions/tasks per server per day **10000-20000** object/task element versions per server per day	**Processor:** 64-bit four+ -core **RAM:** 32 GB **Hard disk (SSD):** 320 GB
Huge	**4000 and more** sessions/tasks per server per day **20000 and more** object/task element versions per server per day	**Processor:** 64-bit eight+ -core **RAM:** 64 GB **Hard disk (SSD):** 500 GB

- When installing Backup Navigator on Linux, consider the following:
  - JDK 1.8

    JDK is installed and configured on the system automatically when running the Backup Navigator installation script.
  - Apache Tomcat 8.5.x

    Apache Tomcat is installed and configured on the system automatically when running the Backup Navigator installation script.

    It is recommended to configure Tomcat to support Transport Layer Security (TLS) versions 1.1 or 1.2 and to restrict support for TLS 1.0 to take advantage of improved secure sockets.
  - PostgreSQL 9.4-9.6

    PostgreSQL server can be installed and configured on the same system with Backup Navigator automatically when running the Backup Navigator installation script.

Backup Navigator web user interface

The Backup Navigator web user interface supports the following web browsers:

- Internet Explorer 11
- Mozilla Firefox 40 and later versions

  If you want to use Kerberos authentication, perform the following configuration steps in the browser:

  1. In the address bar, type: **`about:config`**
  2. In the Search text box, type: **`negotiate`**
  3. Double-click the **`network.negotiate-auth.trusted-uris`** string, enter the domain name of the Backup Navigator system in the pop-up text box (for example, **`company.com`**), and then click **OK**.

  When you log in to the Backup Navigator system, specify the fully qualified domain name in the address string (for example, `computer.company.com:8080`).
- Google Chrome 46 and later versions

Backup Navigator remote agent

- One of the supported operating systems. For a list of the supported operating systems, see *Backup Navigator Support Matrix.*
- JRE 1.8

Application environment

A list of prerequisites depends on the application you use with Backup Navigator.

- **Data Protector environment**

  For more information and detailed instructions, see the Data Protector documentation at the Micro Focus Support web site at: http://support.openview.hp.com/selfsolve/manuals

  - Backup Navigator can be used with Data Protector versions 9.xx, 10.02-10.20.
  - Additional detailed prerequisites for data collection are described in Establishing data collection environment, on page 39
  - To enable data collection for the Cell Manager Services, IDB Health, and Licenses related reports from the UNIX and Linux Cell Managers, create the following softlinks on such Cell Managers:

    ```
    ln -s /opt/omni/sbin/omnisv /opt/omni/lbin/omnisv
    ln -s /opt/omni/sbin/omnidbcheck /opt/omni/lbin/omnidbcheck
    ln -s /opt/omni/bin/omnicc /opt/omni/lbin/omnicc
    ln -s /opt/omni/bin/omnidownload /opt/omni/lbin/omnidownload
    ln -s /opt/omni/bin/omnirpt /opt/omni/lbin/omnirpt
    ```

  - To be able to collect data for the Data Protector virtual environment, make sure, that the Data Protector `Virtual Environment Integration` component is installed on the Cell Manager.
  - To be able to collect restore information for the reports, in the Data Protector global options file, set the variable `EnableRestoreReportStats=1`. The global options file is located at:

    Windows: *Data_Protector_program_data*`\Config\Server\Options\global`

    UNIX: `/etc/opt/omni/server/options/global`

- **VM Explorer environment**

  For more information and detailed instructions, see the VM Explorer documentation at the Micro Focus Support web site at: http://support.openview.hp.com/selfsolve/manuals

  - Backup Navigator can be used with VM Explorer Enterprise Edition 6.4.2.
  - On VM Explorer, an API key (a string token) is generated. It is used to identify and authenticate Backup Navigator and to enable data collection from VM Explorer environment. For detailed instructions, see the *VM Explorer Reporting API* documentation.

Recommendations

Before installing and configuring Backup Navigator, you should consider the factors that affect performance of the application. Backup Navigator performance mainly depends on the number of the

Data Protector objects collected from the Cell Managers for various reports. One Backup Navigator system can collect up to 1 million objects from the Data Protector environment. To calculate how many objects reside on a Cell Manager system, see Calculating the number of objects on a Data Protector Cell Manager, below.

If you have multiple Cell Managers and more than 1 million objects in your backup environment, determine how many Backup Navigator applications you need to install and from which Cell Managers each of the Backup Navigator will collect data. When planning which Cell Managers will be dedicated to a specific Backup Navigator system, consider the following:

- The number of objects residing on these Cell Managers should not exceed 1 million.
- The Cell Managers should be grouped according to their geographical location to avoid connectivity and network problems.

Calculating the number of objects on a Data Protector Cell Manager

Steps

1. On a Data Protector Cell Manager system, run the following command as an administrator:

   Windows: `omnidbutil -info > <filename>.txt`

   Linux: `/opt/omni/sbin/omnidbutil -info > <filename>.txt`
2. Open the generated `TXT` file and search for the number of objects under the `Catalog Database space usage` section > `Items Used` column > `Objects`.

Installation procedure

The Backup Navigator installation procedure depends on the operating system you want to install Backup Navigator:

- **On Linux:** Running the Backup Navigator installation script on Linux, below.
- **On Windows:** Installing Backup Navigator on Windows, on page 19.

If you want to enable Windows sessions credentials authentication, configure Kerberos on the system where you installed Backup Navigator. See Configuring Kerberos authentication, on page 23.

Running the Backup Navigator installation script on Linux

You can use the Backup Navigator installation script to install Backup Navigator with all prerequisites (PostgreSQL, Apache Tomcat, and JDK). The installation script simplifies the installation process and provides all necessary configuration specific to Backup Navigator. It is recommended to use this installation approach.

Prerequisites

- Red Hat Enterprise Linux, CentOS Linux, or SUSE Enterprise Linux operating system is installed and configured.
- If you do not have access to the internet on the Backup Navigator system, make sure, that you prepare the following packages on this system.

  You can download the prerequisite packages automatically by using the Backup Navigator installation script:

  ```
  # sh hpe-backup-navigator-install.sh --download
  ```

  The script downloads all prerequisite packages and compresses them to the `filename.tar.gz` file. It is recommended that these packages are saved in a temporary directory with write permissions, for example, `\tmp`.

  The following packages are required:

  JRE 1.8:

  Download the `jre-8u101-linux-x64.rpm` installation package from: http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

  Apache Tomcat:

  Download Tomcat from the Core Binary distribution (`tar.gz` file) from: https://tomcat.apache.org/download-80.cgi

PostgreSQL:

- On RHEL and CentOS 6.x:

  Download the following packages to your system from http://yum.postgresql.org/9.6/redhat/rhel-6-x86_64/repoview/postgresqldbserver96.group.html:

  ```
  postgresql96
  postgresql96-contrib
  postgresql96-libs
  postgresql96-server
  ```

  Download the `uuid-1.6.1-10.el6.x86_64.rpm` package to your system from: http://mirror.centos.org/centos/6/os/x86_64/Packages/

- On RHEL and CentOS 6.4, download the `openssl` package to your system from: http://mirror.centos.org/centos/6/os/x86_64/Packages/

- On RHEL and CentOS 7.x:

  Download the following packages to your system from https://yum.postgresql.org/9.6/redhat/rhel-7-x86_64/repoview/postgresqldbserver96.group.html:

  ```
  postgresql96
  postgresql96-contrib
  postgresql96-libs
  postgresql96-server
  ```

  On RHEL and CentOS 7.x, download the `openssl` package to your system from: http://mirror.centos.org/centos/7/os/x86_64/Packages

- On SUSE, download the following packages to your system from:

  http://download.opensuse.org/repositories/server:/database:/postgresql/SLE_12_SP3/x86_64/

  `libpq5` (`libpq5-10.1-10.1.x86_64.rpm`)
  `postgresql96` (`postgresql96-9.6.6-33.10.x86_64.rpm`)
  `postgresql96-contrib` (`postgresql96-contrib-9.6.6-33.10.x86_64.rpm`)
  `postgresql96-server` (`postgresql96-server-9.6.6-33.10.x86_64.rpm`)

  `postgresql-init` from http://mirror.hust.edu.cn/opensuse/distribution/openSUSE-current/repo/oss/suse/noarch/postgresql-init-9.6-15.1.noarch.rpm

Steps

1. Insert and mount the Backup Navigator installation DVD-ROM or mount the ISO image directly.

   > **NOTE:**
   > If you want to verify the rpm signature of the Backup Navigator installation package, run the following command:
   >
   > ```
   > # sh hpe-backup-navigator-install.sh -sc
   > ```

2. In the command-line console, run the following command:

   ```
   # sudo sh hpe-backup-navigator-install.sh
   ```

3. The script starts the installation and configuration of Backup Navigator and prerequisite software, such as, JDK, Tomcat, and PostgreSQL as well as firewall and network configuration. In case of the PostgreSQL installation, the database user with appropriate permissions is created.

4. You are provided with the Built-in Administrator user name (`administrator`) and password (`administrator`) for the login to the Backup Navigator web application.

When you add the Data Protector 10.xx Cell Manager, the security certificate from Data Protector are imported to Backup Navigator in the following location: `/opt/dpa-ext/conf/BNjavaKeyStore.jks`.

> **NOTE:**
> You can install Data Protector on the system where Backup Navigator is already installed. Stop Tomcat on the Backup Navigator system before the Data Protector installation and start it again after the Data Protector installation.

Installing Backup Navigator on Windows

During the Backup Navigator installation on Windows, all prerequisite software is installed automatically.

Recommendation

It is not recommended to install Backup Navigator on the same system with Data Protector. Installation on the same system may affect performance and result in issues with communication.

Steps

1. Insert and mount the Backup Navigator installation DVD-ROM or mount the ISO image directly.
2. Run the `Backup Navigator 10.20.exe` file.
3. In the Welcome to the Backup Navigator Setup Wizard window, click **Next**.
4. Accept the license agreement and then click **Next**,
5. Select the default location or browse for an alternative location where you want to install Backup Navigator, then click **Next**.
6. Select the default Tomcat port or enter an alternative port for Tomcat web server configuration, then click **Next**.
7. Select the default location of the PostgreSQL data directory or browse for an alternative location. Enter the username and password for the PostgreSQL user that will be used by Backup Navigator to access the database, then click **Next**.
8. Make sure that the port you specified for Tomcat webserver and the default PostgreSQL database port are not used by other applications, then click **Next**.
9. Review the specified settings and then click **Install**.

   During the installation, the required prerequisite software packages and Backup Navigator are installed.
10. When installation is finished, make sure that the `View initial password` check box is selected, then click **Finish**.

    The `initial_password.txt` file contains credentials for the Built-in Administrator to log in to the Backup Navigator web application.

When you add the Data Protector 10.xx Cell Manager, the security certificate from Data Protector are imported to Backup Navigator in the following location: *`BN_INSTALL_DIR`*`\dpa-ext\conf\BNjavaKeyStore.jks`.

> **NOTE:** If you upgrade Java on the Backup Navigator system, update the existing paths to Java binaries in *`BN_INSTALL_DIR`*`\webserver\bin\setenv.bat`

> **NOTE:**
> You can install Data Protector on the system where Backup Navigator is already installed. Stop Tomcat on the Backup Navigator system before the Data Protector installation and start it again after the Data Protector installation.

Configuring encrypted communication and authentication

To improve security in the Backup Navigator environment, you can configure Backup Navigator to use SSL encrypted communication and authentication.

- If you want to enable encrypted communication between Backup Navigator server and Web clients (for example, Backup Navigator web user interface connection to the server), see Configuring Backup Navigator to use SSL encrypted communication, below.
- If you use the Backup Navigator remote agent, you should perform additional steps on the system where the remote agent resides, see Configuring the remote agent to use SSL communication, on the next page.
- If you want to use LDAP authentication, you have to configuring SSL on the Backup Navigator system. See Configuring SSL for LDAP authentication, on page 22.
- If you want to use Kerberos authentication in the Backup Navigator environment, see Configuring Kerberos authentication, on page 23.

Configuring Backup Navigator to use SSL encrypted communication

To configure Backup Navigator to use SSL encrypted communication, follow these steps:

Steps

1. If you acquired a certificate for this host earlier, proceed to step 6 and import it. Otherwise, create a Certificate Signing Request (CSR):

   On Linux:

   ```
   # $JAVA_HOME/bin/keytool -certreq -keyalg RSA -alias bnjavakeystore.jks -file
   tomcat_cert_request.csr -keystore /opt/dpa-ext/conf/BNjavaKeyStore.jks
   ```

   On Windows:

   ```
   # $JAVA_HOME/bin/keytool -certreq -keyalg RSA -alias bnjavakeystore.jks -file
   tomcat_cert_request.csr -keystore BN_INSTALL_DIR/dpa-
   ext/conf/BNjavaKeyStore.jks
   ```

2. Submit the created `tomcat_cert_request.csr` file to the Certificate Authority (CA). For instructions, see the CA documentation.
3. The CA issues a certificate and sends it to you.
4. Import the acquired certificate to the Backup Navigator keystore:

   On Linux:

```
# $JAVA_HOME/bin/keytool -import -alias tomcat -keystore /opt/dpa-ext/conf/BNjavaKeyStore.jks -file <certificate_filename>
```

On Windows:

```
# $JAVA_HOME/bin/keytool -import -alias tomcat -keystore BN_INSTALL_DIR/dpa-ext/conf/BNjavaKeyStore.jks -file <certificate_filename>
```

When the `keytool` command requests a password, provide the one that is stored in `/opt/dpa-ext/conf/admin.properties`.

5. Configure Apache Tomcat webserver config file to start using the SSL connector:

   ```
   # vi /opt/apache-tomcat/conf/server.xml
   ```

   > **NOTE:**
   > An example of the `connector` element for an SSL connector is included in the Apache Tomcat web server `config` file.

6. Remove the comments and edit the `connector` element as follows:

   ```
   <Connector port="443"
   protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200"
   SSLEnabled="true"
   scheme="https"
   secure="true"
   clientAuth="false"
   sslProtocol="TLS"
   keystoreFile="<keystore_filename>"
   keystorePass="<keystore_password>" />
   ```

   The `port` attribute is the TCP/IP port number, on which Tomcat will listen for secure communication. The default port for https is 443, but you can change it.

7. Comment the old `connector` element which is not configured for SSL (by default, the port is 80 or 8080).
8. Make sure that the newly specified connector port is open in the firewall. Check, which ports are open in your firewall:

   On RHEL and CentOS: `service iptables status`

   On SUSE: `cat /etc/sysconfig/scripts/SuSEfirewall2-custom`

9. Restart Apache Tomcat:

   ```
   # service tomcat restart
   ```

Configuring the remote agent to use SSL communication

When the Backup Navigator server is configured to use SSL for secure communication, ensure that the CA of the certificate installed on the Backup Navigator server is also trusted on the remote agent. Perform this procedure on the system where the Backup Navigator remote agent resides.

Prerequisite

The root certificate (public certificate) of the same CA issuer that is registered in the certificate installed on the Backup Navigator server.

Step

By sing the `keytool` command, import the root certificate into the Backup Navigator keystore located at:

On Linux: `/opt/dpa-ext/conf/BNjavaKeyStore.jks`

On Windows: *`BN_INSTALL_DIR`*`/dpa-ext/conf/BNjavaKeyStore.jks`

The password required by the Java keystore tool is stored in `/opt/dpa-ext/conf/admin.properties`. During the import, mark the certificate as trusted.

Example:

```
keytool -import -keystore /opt/dpa-ext/conf/BNjavaKeyStore.jks -file
<certificate_filename>
```

After the certificate is properly imported the remote agent can connect to the Backup Navigator server using a secure communication channel.

Configuring SSL for LDAP authentication

On the Backup Navigator system, configure SSL to enable LDAP authentication.

Steps

1. On the Backup Navigator system, import your CA root certificate into the Backup Navigator keystore file:

   On Linux:

   ```
   keytool -import -alias <alias_description> -keystore /opt/dpa-
   ext/conf/BNjavaKeyStore.jks -file <certificate_filename>
   ```

   On Windows :

   ```
   keytool -import -alias <alias_description> -keystore BN_INSTALL_DIR/dpa-
   ext/conf/BNjavaKeyStore.jks -file <certificate_filename>
   ```

   Example:

   ```
   keytool -import -alias BN_PEM -keystore /opt/dpa-ext/conf/BNjavaKeyStore.jks
   -file "/tmp/BN-CA.PEM.crt"
   ```

   When the `keytool` command requests a password, provide the one that is stored in `/opt/dpa-ext/conf/admin.properties`.

2. Type **`yes`** to add the new certificate as trusted.
3. Restart the Tomcat server on the Backup Navigator system:

   ```
   # service tomcat restart
   ```

Configuring Kerberos authentication

To enable Windows sessions credentials authentication, configure Kerberos on the system where you installed Backup Navigator.

Prerequisite

Make sure that the time on the system where you want to install Backup Navigator is synchronized with NTP of your network.

Steps

1. Set up the `/etc/krb5.conf` file as follows:

   ```
   # cat /etc/krb5.conf
   [logging]
   default = FILE:/var/log/krb5libs.log
   kdc = FILE:/var/log/krb5kdc.log
   admin_server = FILE:/var/log/kadmind.log
   [libdefaults]
   default_tkt_enctypes = aes128-cts rc4-hmac des3–cbc–sha1 des–cbc–md5 des–cbc–crc
   default_tgs_enctypes = aes128-cts rc4-hmac des3–cbc–sha1 des–cbc–md5 des–cbc–crc
   permitted_enctypes = aes128-cts rc4-hmac des3–cbc–sha1 des–cbc–md5 des–cbc–crc
   default_realm = COMPANY.COM
   dns_lookup_realm = true
   dns_lookup_kdc = true
   ticket_lifetime = 24h
   forwardable = yes
   [realms]
   COMPANY.COM = {
   kdc = dc_computer.company.com
   admin_server = dc_computer.company.com
   default_domain = company.com
   }
   [domain_realm]
   .company.com = COMPANY.COM
   company.com = COMPANY.COM
   [appdefaults]
   pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
   }
   ```

   where:

   dc_computer.company.com is the company Key distribution center host.
   company.com is the company domain name.

2. Test the Kerberos configuration as follows:

```
# kinit user@COMPANY.COM
Password for user@COMPANY.COM:
```

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: user@COMPANY.COM
```

```
Valid starting Expires Service principal
03/18/14 11:10:19 03/18/14 21:10:23 krbtgt/COMPANY.COM@COMPANY.COM
renew until 03/19/14 11:10:19
```

where:

user@COMPANY.COM is your user account, which is already in AD and has permissions to add a system to AD.
company.com is the domain name of the system, where you want to install Backup Navigator.

3. Make sure that the Samba server is installed:

   ```
   # rpm -qa | grep -i samba-
   samba-3.6.9-167.el6_5.x86_64
   samba-winbind-clients-3.6.9-167.el6_5.x86_64
   samba-winbind-3.6.9-167.el6_5.x86_64
   samba-client-3.6.9-167.el6_5.x86_64
   samba-common-3.6.9-167.el6_5.x86_64
   ```

4. Stop the Samba services (`smb`, `nmb`, and `winbind`):

   ```
   # service smb stop
   # service nmb stop
   # service winbind stop
   ```

5. Configure the Samba server as follows:

   ```
   # cat /etc/samba/smb.conf
   [global]
   workgroup = WORKGROUP
   security = ads
   realm = COMPANY.COM
   kerberos method = dedicated keytab
   create krb5 conf = no
   dedicated keytab file = /etc/krb5.keytab
   ```

   ```
   wins support = no
   preferred master = no
   local master = no
   domain master = no
   ```

   where:

   workgroup is the name of your workgroup.
   company.com is the domain name of the system, where you want to install Backup Navigator.

6. Join Samba to the Active Directory (AD). Make sure that:

   - Your Kerberos ticket is valid or initialize it again.
   - No old Kerberos keytab is specified by the Samba config.
   - You have the root user permissions.

- The hostname of the system is not joined in domain. If it is joined, ensure that it is removed from domain.

Run the following commands:

```
# rm -f /etc/krb5.keytab

# kinit user@COMPANY.COM
Password for USER@COMPANY.COM:

# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: user@COMPANY.COM

Valid starting Expires Service principal
03/18/14 11:21:37 03/18/14 21:21:40 krbtgt/COMPANY.COM@COMPANY.COM
renew until 03/19/14 11:21:37

# net ads join -k COMPANY.COM
Using short domain name -- NAME
Joined 'computer' to dns domain 'company.com'

# net ads testjoin
Join is OK
```

where:

user@COMPANY.COM is your user account, which is already in AD and has permissions to add a system to AD.
company.com is the domain name of the system, where you want to install Backup Navigator.
NAME is a shortened form of the domain name.

7. Start Samba services (`smb`, `nmb`, and `winbind`):

   ```
   # service smb start
   # service nmb start
   # service winbind start
   ```

8. Create the Kerberos Keytab HTTP Principal to communicate through the security channel, as follows:

   ```
   # net ads keytab create
   # net ads keytab add HTTP
   # net ads keytab list | grep -i http
   4 DES cbc mode with CRC-32 HTTP/computer.company.com@COMPANY.COM
   4 DES cbc mode with RSA-MD5 HTTP/computer.company.com@COMPANY.COM
   4 ArcFour with HMAC/md5 HTTP/computer.company.com@COMPANY.COM
   4 AES-128 CTS mode with 96-bit SHA-1 HMAC HTTP/computer.company.com@COMPANY.COM
   4 AES-256 CTS mode with 96-bit SHA-1 HMAC HTTP/computer.company.com@COMPANY.COM
   ```

   where:

   computer.company.com is the hostname of the system, where you want to install Backup Navigator.
   company.com is the domain name of the system, where you want to install Backup Navigator.

9. Create a dedicated group for accessing the Kerberos keytab and set up permissions accordingly:

   ```
   # grep 200 /etc/group
   # groupadd -g 200 krb5keytab
   # chgrp krb5keytab /etc/krb5.keytab
   # chmod g+r /etc/krb5.keytab
   ```

10. In `/opt/dpa-ext/conf` create the `kerberos.properties` file with the following content:

    ```
    grails.plugin.springsecurity.kerberos.ticketValidator.servicePrincipal =
    HTTP/computer.company.com@COMPANY.COM
    grails.plugin.springsecurity.kerberos.ticketValidator.keyTabLocation =
    file:///etc/krb5.keytab
    ```

    where:

    computer.company.com is the hostname of the system, where you want to install Backup Navigator.
    company.com is the domain name of the system, where you want to install Backup Navigator.
    pathname is the path to the keytab location.

11. Restart Tomcat on the Backup Navigator system:

    ```
    # service tomcat restart
    ```

Configuring Data Protector secure communication for Backup Navigator

If the secure communication is enabled on the Data Protector Cell Manager you can provide secure communication for Backup Navigator.

- You can configure Backup Navigator to use secure communication with the single Cell Manager or the Cell Managers, members of the MoM environment, if MoM secure communication was enabled in Data Protector 9.03 and newer versions (with the `omnicc -encryption -enable_mom -all` command). See Configuring secure communication for single Cell Manager and for MoM server, on the next page.
- You can configure Backup Navigator to use secure communication for multiple Cell Managers, see Configuring secure communication for multiple Cell Managers, on page 28.

Prerequisite

- Ensure that the following OpenSSL libraries reside on the Backup Navigator server:

  On Windows:

  ```
  omnissleay32.dll
  omnilibeay32.dll
  ```

  You can copy them from *`Data_Protector_home`*`\lib\x8664\` on any Data Protector Windows client or Cell Manager to *`BN_INSTALL_DIR`*`\agent\util_cmd\lib\x8664\` on the Backup Navigator server.

  On Linux:

  ```
  libgcc_s.so.1
  libomnicrypto.so.1.0.0
  libomnissl.so.1.0.0
  ```

  You can copy them from `/opt/omni/lib64/` on any Data Protector Linux client or Cell Manager copy the following files to `/opt/omni/lib64` on the Backup Navigator server.

Data Protector 10.xx:

- Data Protector client with the User Interface component is installed on the Backup Navigator system.
- Replace the existing `util_cmd` with the `util_cmd` for Data Protector 10.xx. Before doing so, make sure to back up the existing one.

  On Windows:

  Copy *BN_INSTALL_DIR*`\agent\dp10\util_cmd.exe` to *BN_INSTALL_DIR*`\agent\util_cmd.exe`

  On Linux:

  Copy `/opt/agent/dp10/util_cmd` to `/opt/agent/util_cmd`
- To redistribute certificates, run the following commands:

  On the Data Protector client installed on the Backup Navigator system:

  ```
  # omnicc -secure_comm -configure_peer <CM hostname>
  ```

  On the Data Protector Cell Manager:

  ```
  # omnicc -secure_comm -configure_peer <BN_hostname> -accept_host
  ```

Configuring secure communication for single Cell Manager and for MoM server

Configure Backup Navigator to use secure communication with the single Cell Manager or the Cell Managers, members of the MoM environment, if MoM secure communication was enabled in Data Protector 9.03 and newer versions.

Steps

1. On the Cell Manager, create the certificates for Backup Navigator server by using the Certificate Generation Utility (`omnigencert.pl`). The utility is available at the following location:

   On Windows: *Data_Protector_home*`\bin`

   On HP-UX and Linux: `/opt/omni/sbin`

   To generate the certificates for Backup Navigator, run the following command from the `omnigencert.pl` location:

   On Windows:

   ```
   # Data_Protector_home\bin\perl omnigencert.pl -pem_client -user_id BN_hostname
   ```

   On HP-UX and Linux:

   ```
   # /opt/omni/bin/perl omnigencert.pl -pem_client -user_id BN_hostname
   ```

   Certificates are generated at the following location:

   On Windows: *Data_Protector_program_data*`\Config\Server\certificates`

   On HP-UX and Linux: `/etc/opt/omni/server/certificates`

   For information on the utility, see the *Data Protector documentation*.

   The Cell Manager uses three certificate files for secure communication:

   BN_hostname`_cert.pem` -certificate for the Backup Navigator server

   BN_hostname`_key.pem` - private key for the Backup Navigator server

*CM_hostname*_cacert.pem -trusted certificate list, containing CA certificate of the cell

2. Copy three certificate files from the Data Protector Cell Manager to the following location on the Backup Navigator server:

   On Windows: *BN_INSTALL_DIR*\agent\util_cmd\config\client\certificates\

   On Linux: /etc/opt/omni/client/certificates

3. Create the config file in the following location:

   On Windows: *%Program Files%*\MF Backup Navigator\agent\util_cmd\config\client\

   On Linux: /etc/opt/omni/client/

   in the UTF16 LE format with the following content:

   ```
   encryption={
   enabled=1;
   certificate_chain_file='/etc/opt/omni/client/certificates/BN_hostname_
   cert.pem';
   private_key_file='/etc/opt/omni/client/certificates/BN_hostname_key.pem';
   trusted_certificates_file='/etc/opt/omni/client/certificates/Cell_Manager_
   hostname_cacert.pem';
   };
   ```

Configuring secure communication for multiple Cell Managers

You can configure Backup Navigator to use secure communication with multiple Data Protector Cell Managers.

Steps

1. On Backup Navigator, create the OpenSSL config file (for example, `myopenssl.cnf`) with the following content:

   ```
   [req]
   default_bits = 4096
   encrypt_key = no
   default_md = sha256
   distinguished_name = dn
   req_extensions = san
   [dn]
   [san]
   ```

2. Create the self-signed certificate and key, by running the following command:

   ```
   # openssl req -x509 -newkey rsa:4096 -keyout BN_hostname_key.pem -out BN_hostname_cert.pem -days 3650 -nodes -config myopenssl.cnf -subj "/CN=bn/O=HEWLETT PACKARD ENTERPRISE/C=US/ST=CA"
   ```

3. Copy the generated `BN_hostname_cert.pem` and `BN_hostname_key.pem` to `/etc/opt/omni/client/certificates` (creat the directory, if missing).

4. Create the `/etc/opt/omni/client/config` file with the following content:

   ```
   encryption={
   enabled=1;
   certificate_chain_file='/etc/opt/omni/client/certificates/BN_hostname_cert.pem';
   private_key_file='/etc/opt/omni/client/certificates/BN_hostname_key.pem';
   trusted_certificates_file='/etc/opt/omni/client/certificates/BN_hostname_cert.pem';
   };
   ```

5. Update *every* Data Protector Cell Manager to establish secure communication with Backup Navigator as follows:

   a. Copy `BN_hostname_cert.pem` to the Cell Manager.

   b. Join the trusted certificate file residing on the Cell Manager with `BN_hostname_cert.pem`. The trusted certificate file resides on the Cell Manager at:

      On Windows: *Data_Protector_program_data*`\Config\Server\certificates`

      On HP-UX and Linux: `/etc/opt/omni/server/certificates`

      Run the following command:

      On Windows:

      ```
      # type CM_hostname_cacert.pem BN_hostname_cert.pem 2> nul > CM_BN_hostname_cacerts.pem
      ```

      On HP-UX and Linux:

      ```
      # cat CM_hostname_cacert.pem BN_hostname_cert.pem > CM_BN_hostname_cacerts.pem
      ```

   c. In the Cell Manager local `config` file (located at *Data_Protector_program_data*`\Config\client\config` on Windows and `/etc/opt/omni/client/config` on HP-UX and Linux), in the line `trusted_certificates_file`, replace the name of the trusted certificate file as follows:

Change `CM_hostname_cacert.pem` to `CM_hostname_BN_hostname_cacert.pem`.

6. Update the Backup Navigator configuration to establish secure communication with the Data Protector Cell Managers as follows:

   a. Copy the Cell Managers trusted certificate files (`CM_hostname_cacert.pem`) to the Backup Navigator server to the `/etc/opt/omni/client/certificates` directory.

   b. In the `/etc/opt/omni/client/certificates` directory, join the (`CM_hostname_cacert.pem` files with `BN_hostname_cert.pem`. For example:

   ```
   # cat CM1_hostname_cacert.pem CM2_hostname_cacert.pem CM3_hostname_
   cacert.pem bn_cert.pem > All_CM_BN_hostname_cacerts.pem
   ```

   When you add more Cell Managers, make sure that you join their (`CM_hostname_cacert.pem` files with the cumulative trusted certificate file on the Backup Navigator server (`All_CM_BN_hostname_cacerts.pem`).

   c. In the `/etc/opt/omni/client/config` file, in the line `trusted_certificates_file`, replace the name of the trusted certificate file as follows:

   Change `BN_hostname_cert.pem` to `All_CM_BN_hostname_cacerts.pem`.

Chapter 3: Upgrading Backup Navigator

You can upgrade Backup Navigator from earlier versions.

> **IMPORTANT:**
> After upgrading Backup Navigatorfrom version 9.10 and earlier, you also need to upgrade your Backup Navigator licenses to the new format. Contact your Sales Representative.

Prerequisites

If you do not have access to the internet on the Backup Navigator system, make sure, that you prepare the following packages on this system.

You can download the prerequisite packages automatically by using the Backup Navigator installation script:

```
# hpe-backup-navigator-install.sh --download
```

The script downloads all prerequisite packages and compresses them to the `filename.tar.gz` file. It is recommended that these packages are saved in a temporary directory with write permissions, for example, `\tmp`.
The following packages are required:
JRE 1.8:

Download the `jre-8u101-linux-x64.rpm` installation package from:
http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

Apache Tomcat:

Download Tomcat from the Core Binary distribution (`tar.gz` file) from: https://tomcat.apache.org/download-80.cgi

PostgreSQL 9.6:

- On RHEL and CentOS 6.x:

  Download the following packages to your system from http://yum.postgresql.org/9.6/redhat/rhel-6-x86_64/repoview/postgresqldbserver96.group.html:

  ```
  postgresql96
  postgresql96-contrib
  postgresql96-libs
  postgresql96-server
  ```

  Download the `uuid-1.6.1-10.el6.x86_64.rpm` package to your system from:
  http://mirror.centos.org/centos/6/os/x86_64/Packages/
- On RHEL and CentOS 6.4, download the `openssl` package to your system from:
  http://mirror.centos.org/centos/6/os/x86_64/Packages/
- On RHEL and CentOS 7.x:

  Download the following packages to your system from https://yum.postgresql.org/9.6/redhat/rhel-7-x86_64/repoview/postgresqldbserver96.group.html:

  ```
  postgresql96
  postgresql96-contrib
  postgresql96-libs
  postgresql96-server
  ```

On RHEL and CentOS 7.x, download the `openssl` package to your system from: http://mirror.centos.org/centos/7/os/x86_64/Packages

On SUSE, download the following packages to your system from:

http://download.opensuse.org/repositories/server:/database:/postgresql/SLE_12_SP3/x86_64/

`libpq5` (`libpq5-10.1-10.1.x86_64.rpm`)
`postgresql96` (`postgresql96-9.6.6-33.10.x86_64.rpm`)
`postgresql96-contrib` (`postgresql96-contrib-9.6.6-33.10.x86_64.rpm`)
`postgresql96-server` (`postgresql96-server-9.6.6-33.10.x86_64.rpm`)

`postgresql-init` from http://mirror.hust.edu.cn/opensuse/distribution/openSUSE-current/repo/oss/suse/noarch/postgresql-init-9.6-15.1.noarch.rpm

Limitation

If you upgrade from versions earlier than 9.40, the custom reports are not migrated to the new database during the upgrade.

Steps

1. Insert and mount the Backup Navigator installation DVD-ROM or mount the ISO image directly.
2. In the command-line console, run the following command:

   ```
   # sudo sh hpe-backup-navigator-install.sh
   ```
3. The script starts and checks all the prerequisite software. It prompts you to update to a newer version, when it discovers the respective installation packages in a local directory or on the internet. If you want to upgrade the software and have the installation packages, type **y** and follow the instructions.
4. The script discovers that Backup Navigator is already installed. When the script prompts you to upgrade the existing version, type **y** and follow the instructions.

If you have any imported certificates in their default keystores, you need to import them manually to the Backup Navigator keystore located at: `/opt/dpa-ext/conf/BNjavaKeyStore.jks`.

As soon as the upgrade procedure is completed successfully, upgrade your Backup Navigator licenses to the new format in the following cases:

- If you upgraded from the version 9.10 and earlier. See Licensing, on page 34. Then, you can start using the application.
- If you are using the Lite Backup Navigator licenses, contact Backup Navigator support, because this license type is not supported with Backup Navigator 9.50. In the meantime, Backup Navigator treats Lite license as the Standard 10 TB.

Chapter 4: Removing Backup Navigator

To remove Backup Navigator, run the following command:

```
# rpm –e `rpm –qa | grep backup-navigator`
```

To remove the Backup Navigator remote agent, do the following:

On Windows:

In Windows Control Panel -> Programs and Features, right-click **Backup Navigator Remote Agent**, and then select **Uninstall**.

On Linux:

Run the following command:

```
# rpm -e `rpm –qa | grep remote-agent`
```

Chapter 5: Licensing

After you install and configure Backup Navigator, you can start using it immediately. An Instant-On password is built in to the product when first installed. You can use the software for 60 days and buy the permanent license within this period. If you don't buy a permanent license, new data will not be collected after 60 days.

The following types of Backup Navigator licenses exist:

- **Standard Backup Navigator licenses**

  Standard Backup Navigator licenses are capacity based and are applicable for use with Data Protector environment. You should estimate the capacity of your backup environment to purchase an appropriate number of licenses. The Capacity Based License (CBL) product structure is based on the volume of primary data protected by Data Protector. The capacity is measured in Front End Terabytes. The total amount of Front End Terabytes is defined as the aggregate amount of source data being backed up from all systems. Per system it is measured as the largest full backup. That is, the total amount of source data backed up. The licensing in this product structure is perpetual and covers existing or new infrastructure and applications.

  Capacity calculation details:

  - For a full and incremental backup concept, only full is considered.
  - For an incremental forever, a synthetic full is used.
  - Only objects with a status of `Completed` or `Completed with errors` are included in the calculation.
  - Only objects which are still under protection are included in the calculation.
  - The capacity per system is calculated as an aggregation of the largest size of each unique object for that system still under protection.

  Limitations:

  - Backup of the same database with multiple agents will be counted multiple times. Some examples of scenarios where capacity will be counted multiple times:
    - A filesystem backup of a database using VSS and an application integration agent of the same database.
    - A virtual environment integration backup of a virtual machine and a file system backup of the same data within that virtual machine.
  - When an Oracle backup object name format is externally reconfigured in such a way that Data Protector is not be able to resolve the Oracle database name from the object name, the unique capacity will be counted multiple times. To avoid this the reconfigured object name must include the Oracle database name and be in the format `<DBID_*.dbf`.

  The source data should reside on the Cell Managers monitored by Backup Navigator. If the capacity of your backup environment grows, you should buy additional licenses.

- **Traditional Backup Navigator licenses**

  Traditional Backup Navigator license is dependent on your application environment.

  - Data Protector environment:

    The number of license tokens depends on the amount and types of Data Protector licenses installed on the Cell Managers for which Backup Navigator is collecting data.

  - VM Explorer environment

The number of license tokens depends on the amount of sockets in the VM Explorer environment for which Backup Navigator is collecting data.

The calculation of the Backup Navigator price is incorporated in the product licensing functionality. Data Protector licenses and VM Explorer sockets are represented as the Backup Navigator tokens using an in-built algorithm. You purchase the number of license tokens required by Backup Navigator.

How licensing works

Backup Navigator takes advantage of integration with the Micro Focus Autopass to implement the licensing policy.

To implement licensing for Backup Navigator, follow this procedure:

Steps

1. Buy a needed number of Backup Navigator licenses. For information on the needed number, contact your Sales Representative.

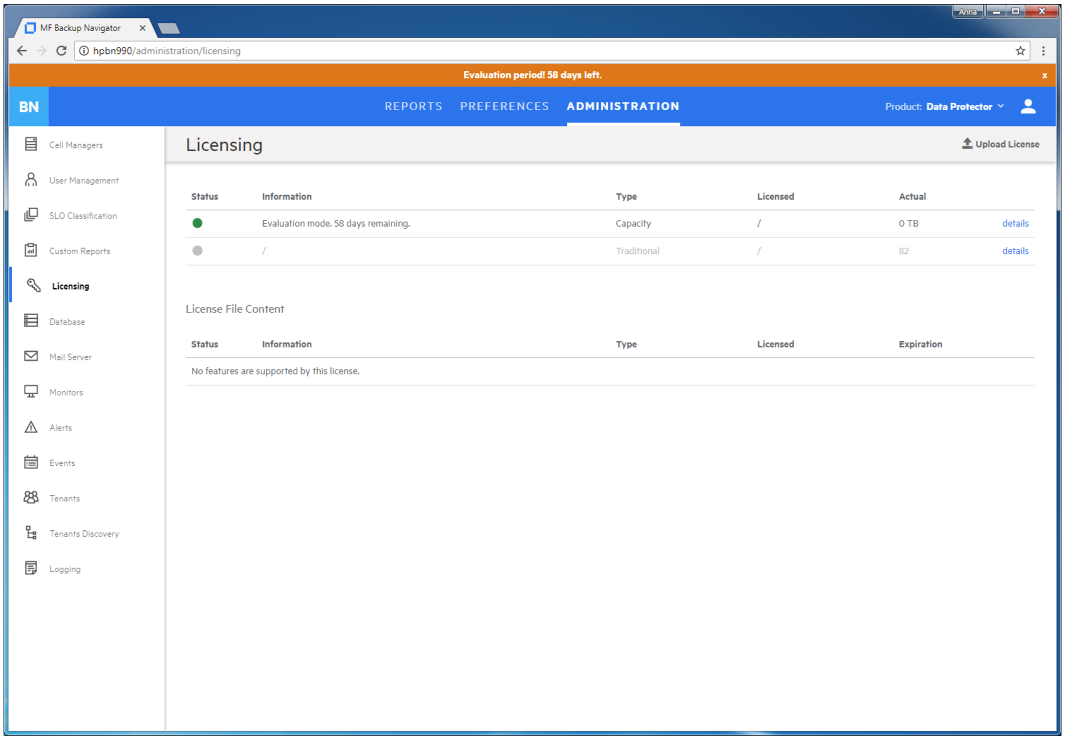
   You can also view the needed number of Standard and Traditional licenses in the Backup Navigator web user interface after you added all the Cell Managers for which Backup Navigator is collecting data:

   a. Select the **Administration** context.

   b. In the Navigation Pane, click **Licensing**.

   c. Click **details**, opposite the Capacity or Traditional license type.

   Figure 3: Viewing the needed number of licenses



Evaluation period! 58 days left.

Licensing

Status	Information	Type	Licensed	Actual	
●	Evaluation mode. 58 days remaining.	Capacity	/	0 TB	details
●	/	Traditional	/	82	details

License File Content

Status	Information	Type	Licensed	Expiration
No features are supported by this license.				

2. After you buy a needed number of licenses, you receive the a license file (`Backup Navigator-licfile.xml`). Copy it to a temporary location.
3. Log in to Backup Navigator and activate the licenses:
   a. Select the **Administration** context.
   b. In the Navigation Pane, click **Licensing**.
   c. Click **Upload License**, browse for the license file received by email, and then click **Upload**.

   After the licenses are activated, the licensing related information is updated.

When the protected data capacity of your backup environment grows, you can purchase additional licenses to cover your new needs. Contact your Sales Representative.

If you upgraded Backup Navigator from an earlier release, upgrade your licenses to a new format. Contact your Sales Representative.

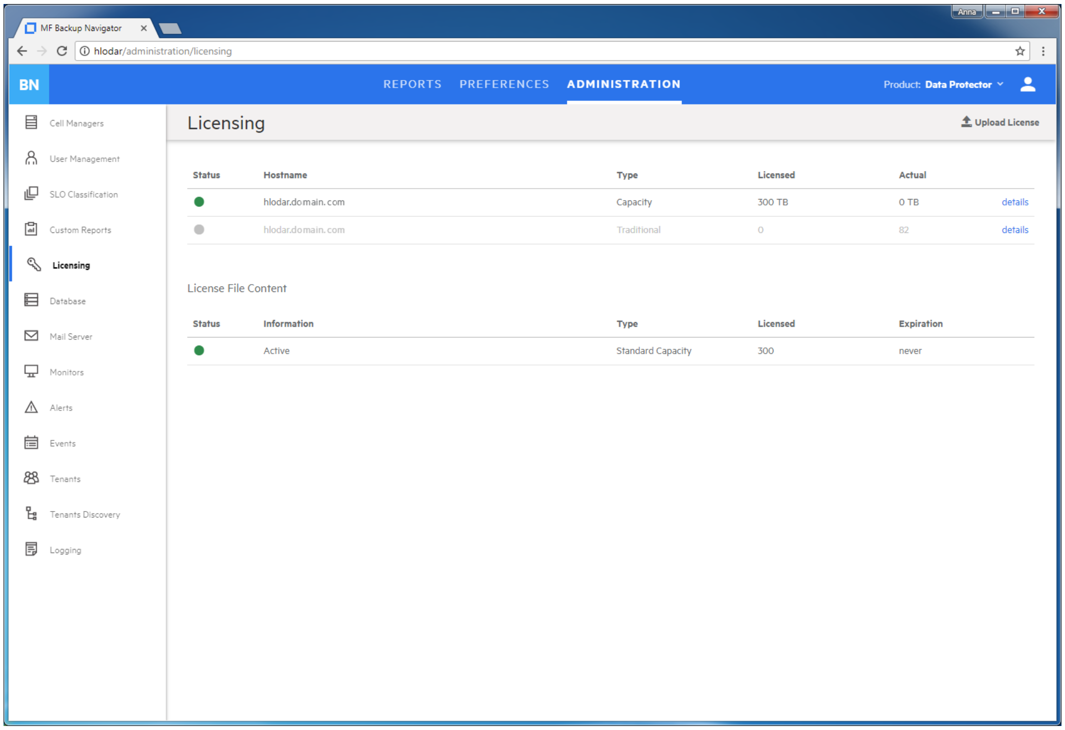
Verifying licenses

You can check the licensing related information at any time.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Licensing**.

Figure 4: Licensing information



Licensing

Status	Hostname	Type	Licensed	Actual	
●	hlodar.domain.com	Capacity	300 TB	0 TB	details
●	hlodar.domain.com	Traditional	0	82	details

License File Content

Status	Information	Type	Licensed	Expiration
●	Active	Standard Capacity	300	never

The current licensing related information is displayed:

- company name
- hostname

- status
- licensed volume (capacity or token based)
- actual volume (capacity or token based)
- number of Cell Managers covered by the current licensing
- list of all purchased licenses with their properties

Chapter 6: Administration Tasks for Data Protector Environment

This chapter is intended for Backup Navigator administrators and refers to using Backup Navigator only with the Data Protector environment. If you use Backup Navigator to collect data from the VM Explorer environment, refer to the administration tasks described in Administration Tasks for VM Explorer Environment, on page 74.

Before you can start using the Backup Navigator functionality, perform the following administration and configuration tasks in the web user interface:

- To start collecting input data from Data Protector cells, add these cells to the Backup Navigator list. For a detailed procedure, see Establishing data collection environment, on the next page.
- After you select the Data Protector cells to collect data for your reports, you can update the cell settings and perform other related tasks. For more information, see Administering cells, on page 41.

  > **IMPORTANT:** If you upgraded Data Protector to 10.03 from an earlier 10.xx version, ensure that you change the Web User name to the new one created in Data Protector 10.03 in the respective cell settings.

- Start the remote agent to collect data from the remote Cell Managers (Cell Managers that cannot be directly accessed from Backup Navigator). See Installing remote agent, on page 43.
- You can perform the following configuration tasks to better adjust Backup Navigator functionality to your environment's needs.
  - To create new users with different permissions as well as edit and delete the existing user accounts in Backup Navigator, see Managing users and user roles, on page 44.
  - See the recommendations on the database maintenance in Maintaining database, on page 52.
  - To be able to receive emails from the Backup Navigator, configure the mail server. See Configuring mail server, on page 54.
- To manage the Service level objective categories, see Managing Service level objective categories, on page 47.
- To create and handle the custom reports, perform the following tasks:
  - Creating custom reports, on page 50.
  - Downloading custom reports, on page 51.
  - Uploading custom reports, on page 52.
- You can monitor different aspects of the Data Protector environment by using the predefined Backup Navigator monitors or configuring custom monitors to trigger alerts or to log events for the specified conditions:
  - To monitor your Data Protector environment with the predefined Backup Navigator monitors, see Predefined monitors, on page 55.
  - To trigger notifications on specific events, configure the related monitors, see Creating and using monitors, on page 60.

- To handle the problems reported in the triggered alerts, see Handling alerts, on page 61.
  - To view the event log, see Viewing events, on page 62.
- To be able to generate reports based on the tenant related data, see Managing tenants and tenant groups, on page 63.
- To analyze and troubleshoot potential problems and provide an appropriate input to Micro Focus Support, see Backup Navigator logging, on page 71.

Establishing data collection environment

Select a new Data Protector cell to collect the input data for your reports from it.

Prerequisites

- Ensure that the hostnames of your Backup Navigator system and remote agent systems, are defined as a fully qualified domain name (FQDN). For details, see the operating system documentation.
- Make sure that your network is configured so that the Cell Manager and Backup Navigator are visible to each other.
- To access and collect data from the newly selected Data Protector cell, add the Backup Navigator user to the Data Protector Admin user group on the Cell Manager. For detailed instructions on how to add a user, see the Data Protector online help. When adding this user to the Data Protector Admin user group, provide the following information:
  - **Name:** The logon name under which Backup Navigator is running on the Backup Navigator server or Backup Navigator remote agent system.
  - **Group/Domain or UNIX Group:** The Windows domain or UNIX group to which the Backup Navigator user belongs.
  - **Client:** The Backup Navigator server or remote agent system name (FQDN or IP address).

Data Protector 10.xx:

- Make sure that the Backup Navigator user in the Data Protector Admin user group on the Cell Manager has enabled web service access (`Webaccess`) to get advantages provided with this product version (Schedule Data reports). On Data Protector 10.02, when creating a user account, make sure to enable the **Webaccess** option. On Data Protector 10.03, Web User name is generated automatically during the account creation.
- To enable data collection from the Data Protector cell *without* using encrypted communication between the Data Protector and Backup Navigator, run the following command on the Data Protector Cell Manager:

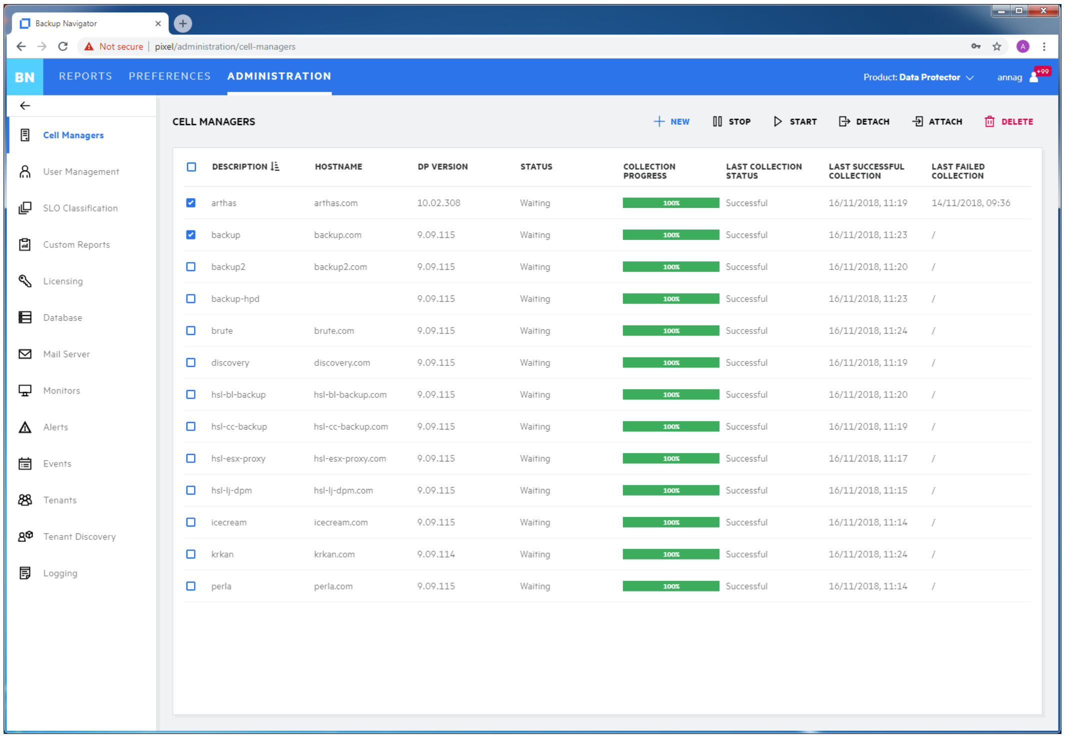
  ```
  # omnicc -secure_comm -configure_for_gui <BN_hostname>
  ```

  If you will use encrypted communication, perform additional configuration steps described in Configuring Data Protector secure communication for Backup Navigator , on page 26.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Cell Managers**.

Figure 5: Adding new Cell Managers

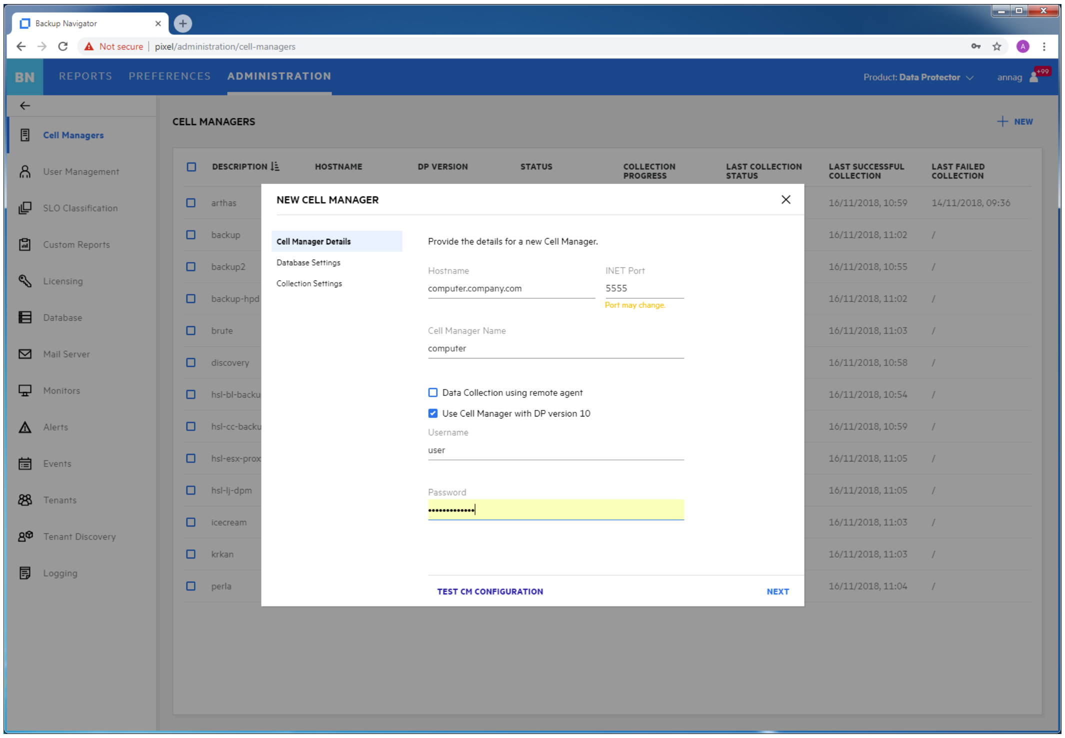


CELL MANAGERS

□	DESCRIPTION	HOSTNAME	DP VERSION	STATUS	COLLECTION PROGRESS	LAST COLLECTION STATUS	LAST SUCCESSFUL COLLECTION	LAST FAILED COLLECTION
☑	arthas	arthas.com	10.02.308	Waiting	100%	Successful	16/11/2018, 11:19	14/11/2018, 09:36
☑	backup	backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:23	/
□	backup2	backup2.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:20	/
□	backup-hpd		9.09.115	Waiting	100%	Successful	16/11/2018, 11:23	/
□	brute	brute.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:24	/
□	discovery	discovery.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:19	/
□	hsl-bl-backup	hsl-bl-backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:20	/
□	hsl-cc-backup	hsl-cc-backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:19	/
□	hsl-esx-proxy	hsl-esx-proxy.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:17	/
□	hsl-lj-dpm	hsl-lj-dpm.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:15	/
□	icecream	icecream.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:14	/
□	krkan	krkan.com	9.09.114	Waiting	100%	Successful	16/11/2018, 11:24	/
□	perla	perla.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:14	/

3. In the Tool bar of the Results Area, click **New**. The New Cell Manager configuration window opens.

Figure 6: New Cell Manager Configuration window



NEW CELL MANAGER

Provide the details for a new Cell Manager.

Hostname: computer.company.com

INET Port: 5555

Port may change.

Cell Manager Name: computer

□ Data Collection using remote agent

☑ Use Cell Manager with DP version 10

Username: user

Password: ••••••••••••••

4. In the Cell Manager Details window, enter a Cell Manager hostname or its IP address, INET port (by default, `5555` and, on the Data Protector 10.xx, `5565`) and a Cell Manager name.

   If this Cell Manager cannot be directly accessed from Backup Navigator, select the **Data collection using remote agent** option.

   If the Cell Manager has Data Protector 10.xx installed, select **Data Protector version is 10.x** to be able to access Data Protector web services.

   Enter the user name and password to access the Cell Manager.
5. Click **Test Configuration** to verify that the Cell Manager is configured appropriately. Then click **Next**.
6. In the Database Settings window, configure the database of the new cell by specifying the following:
   - *Enabled with the **Data Protector version is 10.x** option*: the Web User name and password. If you use Data Protector 10.02, enter an `admin` user account with enabled web service access you created . If you use Data Protector 10.03, enter a web user name generated by Data Protector during the creation of the `admin` user account in the following format: *`username|domain|hostname`*
   - the hostname of the system where the database resides (by default, the system where you installed Backup Navigator)
   - the port of the system where the database resides (by default, `5432`)
   - the user name and the password of the PostgreSQL admin user with the `SUPERUSER` permissions
   - the database name of your choice

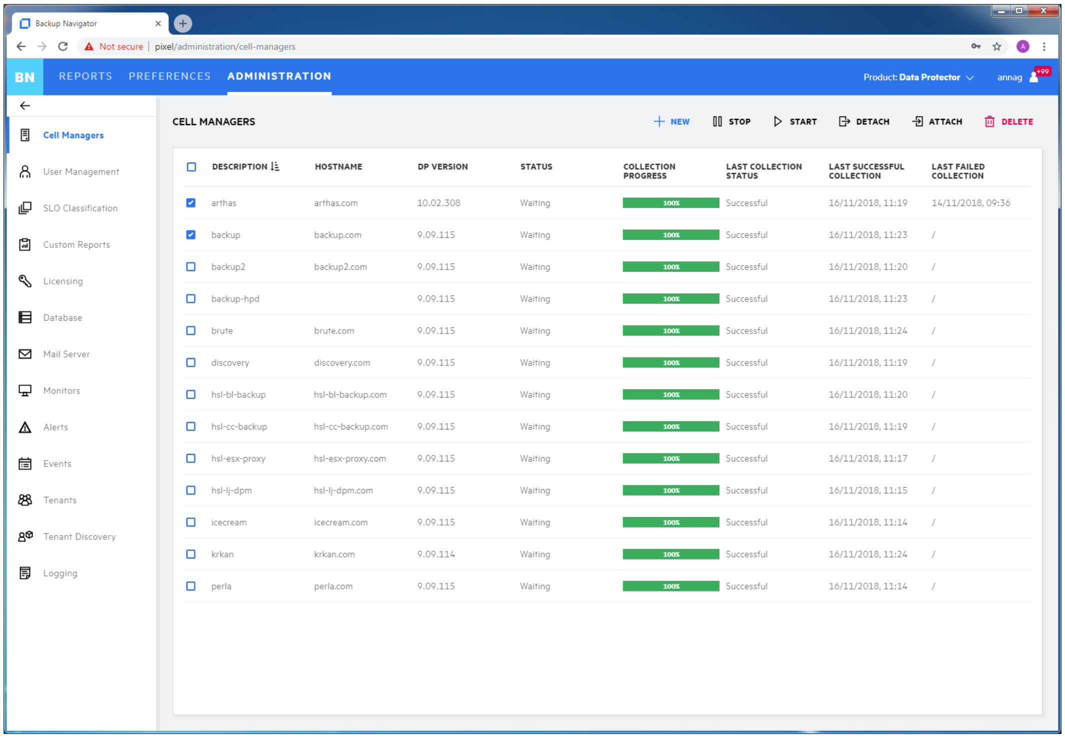
     The maximum number of characters for the database name is 25. The default name is `cell_`*`<description>`*, which you can change to another one.
7. In the Collection Settings window, specify the following:
   - the period for which you want to collect data for your reports (you can select the custom starting date or all existing data)
   - the time interval in which you want to collect the changed input data for your reports (for example, every 10 minutes)
8. Click **Save**. A new cell is added to Scope and is visible in the Navigation Pane.

You can always update your settings later.

Administering cells

After you selected the Data Protector cells to collect data for your reports, they are listed in the Cell Managers window of the Administration context.

Figure 7: Administering cells



□	DESCRIPTION	HOSTNAME	DP VERSION	STATUS	COLLECTION PROGRESS	LAST COLLECTION STATUS	LAST SUCCESSFUL COLLECTION	LAST FAILED COLLECTION
☑	arthas	arthas.com	10.02.308	Waiting	100%	Successful	16/11/2018, 11:19	14/11/2018, 09:36
☑	backup	backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:23	/
□	backup2	backup2.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:20	/
□	backup-hpd		9.09.115	Waiting	100%	Successful	16/11/2018, 11:23	/
□	brute	brute.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:24	/
□	discovery	discovery.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:19	/
□	hsl-bl-backup	hsl-bl-backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:20	/
□	hsl-cc-backup	hsl-cc-backup.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:19	/
□	hsl-esx-proxy	hsl-esx-proxy.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:17	/
□	hsl-lj-dpm	hsl-lj-dpm.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:15	/
□	icecream	icecream.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:14	/
□	krkan	krkan.com	9.09.114	Waiting	100%	Successful	16/11/2018, 11:24	/
□	perla	perla.com	9.09.115	Waiting	100%	Successful	16/11/2018, 11:14	/

You can change the Cell Manager's settings or status by clicking on it and selecting one of the following actions:

- **Edit**: Change the Cell Manager and database settings.

  If you moved the database to a new server or performed any other database configuration changes that affect the Backup Navigator functionality, make the necessary database setting updates on every related Cell Manager.

  If you upgraded Data Protector to 10.03 from an earlier 10.xx version, ensure that you change the Web User name to the new one created in Data Protector 10.03 in the respective cell settings.
- **Stop/Start**: Pause data collection from the selected cell by stopping it, when you temporarily do not need to include its data to your reports. When stopped, the cell is still present in the scope and to the reports. Start data collection from the selected cell, when you need this data for your reports.
- **Download**: Download package for the Backup Navigator remote agent installation. Applicable for the remote Cell Managers.
- **Detach/Attach**: Pause data collection from the selected cell by detaching it, when you want to have access to the collected data in the database, but do not need to include this data in your reports. When detached, the cell is not visible in the scope and in the reports. Attach the selected cell and then start data collection from it, when you need its data for your reports.
- **Delete**: Delete the selected cell from the Backup Navigator list. The database of this cell with all previously collected data is deleted. You can always add this cell to the list later. Note, that a filter that contains only this cell, will be also deleted.

Installing remote agent

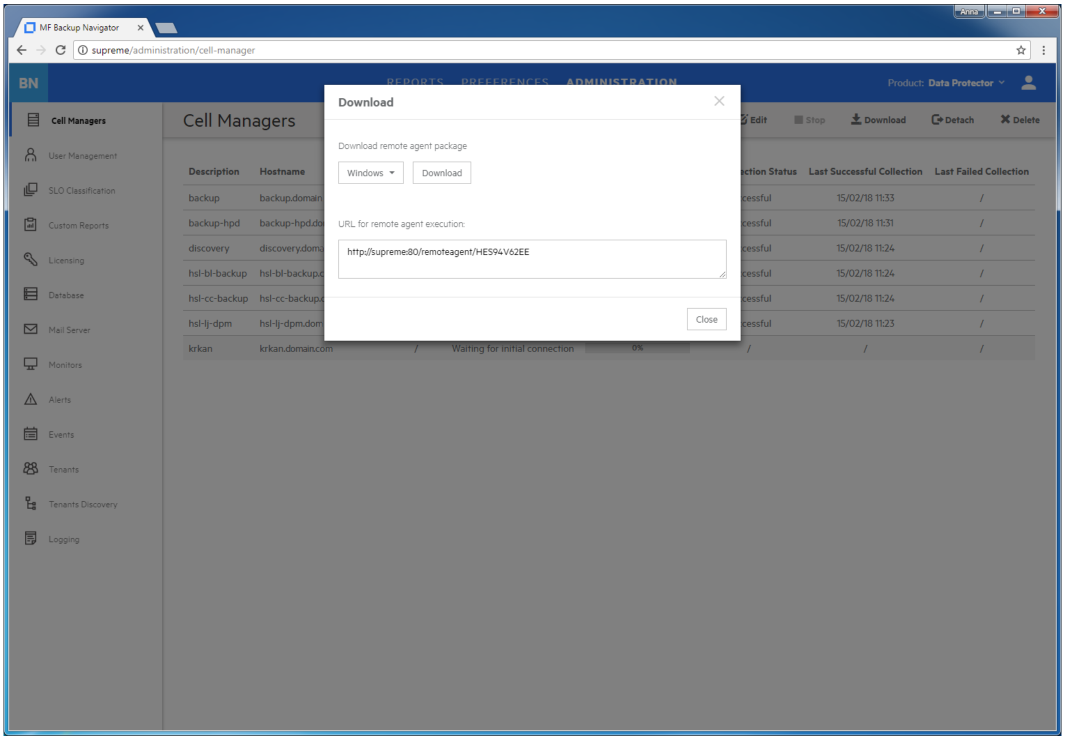
You need to install a remote agent only if you want to collect data from the remote Cell Managers (the Cell Managers that cannot be directly accessed from Backup Navigator).

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Cell Managers**.
3. From the list of the Cell Managers, select the remote Cell Managers, from which you will collect data using the remote agent. In the Tool bar of the Results Area, click **Download**.
4. In the Download Remote Agent window, select **Windows** or **Linux** depending on the operating system you want to install the remote agent and then click **Download** to download the remote agent package.

> **NOTE:**
> The URL provided in this window will be used on a remote system to start the remote agent.

Figure 8: Download Remote Agent Window



Download

Download remote agent package

Windows ▾ | Download

URL for remote agent execution:

http://supreme:80/remoteagent/HES94V62EE

Close

Description	Hostname	ction Status	Last Successful Collection	Last Failed Collection
backup	backup.domain	cessful	15/02/18 11:33	/
backup-hpd	backup-hpd.do	cessful	15/02/18 11:31	/
discovery	discovery.doma	cessful	15/02/18 11:24	/
hsl-bl-backup	hsl-bl-backup.c	cessful	15/02/18 11:24	/
hsl-cc-backup	hsl-cc-backup.c	cessful	15/02/18 11:24	/
hsl-lj-dpm	hsl-lj-dpm.dom	cessful	15/02/18 11:23	/
krkan	krkan.domain.com / Waiting for initial connection 0%	/	/	/

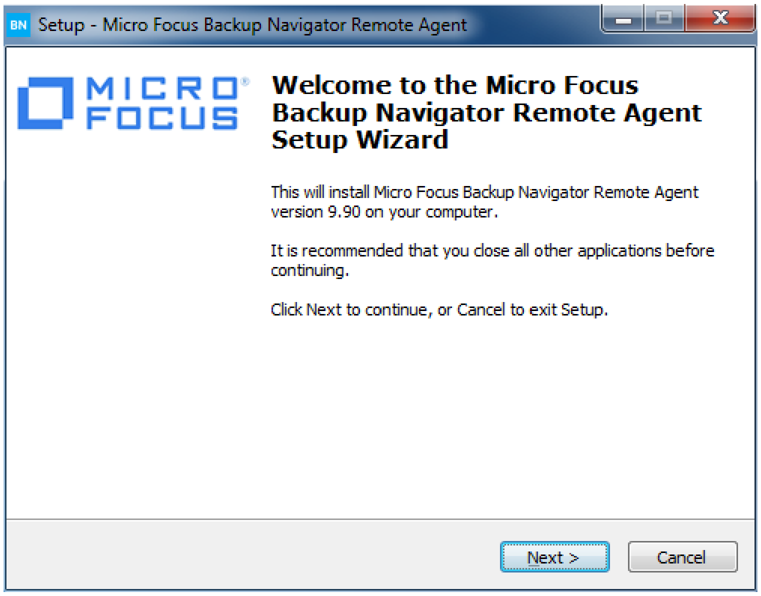
5. Transfer the remote agent installation package to the remote Cell Manager or another system, from which you can access the remote Cell Manager.
6. On the target system, install the remote agent.

On Windows:

a. Start the `bn-remote-agent-10.20.exe` file. When the installation wizard starts, click **Next**.

b. In the Java `HOME` directory text box, specify the path to the Java `HOME` directory. In the URL to Backup Navigator, specify the URL from step 4. Click **Next**.

Figure 9: Remote Agent Installation



Setup - Micro Focus Backup Navigator Remote Agent

Welcome to the Micro Focus Backup Navigator Remote Agent Setup Wizard

This will install Micro Focus Backup Navigator Remote Agent version 9.90 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

c. Specify the location where you want to install the remote agent and then click **Next**.

d. Review the settings and click **Install** to start installation. After the installation process is complete, click **Finish**.

After the installation is complete, the `BNAgentService` process is running. You can start and stop it from the Services page of the Windows Task Manager.

On Linux:

a. Run the installation of the `bn-remote-agent-10.20.rpm` file:

```
# rpm -ivh bn-remote-agent-10.20.rpm
```

b. Edit the remote agent configuration file with the URL provided in step 4:

```
# vi /opt/remote-agent/agent_cfg.properties
```

After the installation is complete, you can use the following commands on the Linux remote agent:

- To start data collection on remote agent: `# service remote-agent start`
- To stop data collection on remote agent: `# service remote-agent stop`
- To check if any remote agent is running: `# service remote-agent status`

Managing users and user roles

Depending on their role, users have different permissions. Backup Navigator supports the following user roles:

- **Built-in Administrator**

  This user role is created during installation. There is only one Built-in Administrator in the Backup Navigator environment and it cannot be deleted or changed. The Built-in Administrator has permissions to generate reports on all Data Protector cells and to perform administration tasks in Backup Navigator.

- **Administrator**

  The Administrator has permissions to generate reports on all Data Protector cells and to perform administration tasks in Backup Navigator. Administrator accounts can be created, edited, and deleted by the Built-in Administrator or Administrator.

- **Standard User**

  An Administrator can create, edit, and delete the Standard User account and grant it permissions for all or selected Data Protector cells. The Standard User can change the profile, manage subscriptions and filters, and generate reports on the Data Protector cells, for which the permissions were granted by the Administrator.

If you configured LDAP authentication (see Configuring SSL for LDAP authentication, on page 22), you can specify users that can be authenticated with the LDAP server. Before you can add LDAP users, you need to specify an LDAP server that will be used by Backup Navigator. For detailed procedure, see Adding LDAP Server, below.

To create a new user, see Creating new users, on the next page.

Adding LDAP Server

Add LDAP server, if you want to create users with LDAP authentication.

Prerequisite

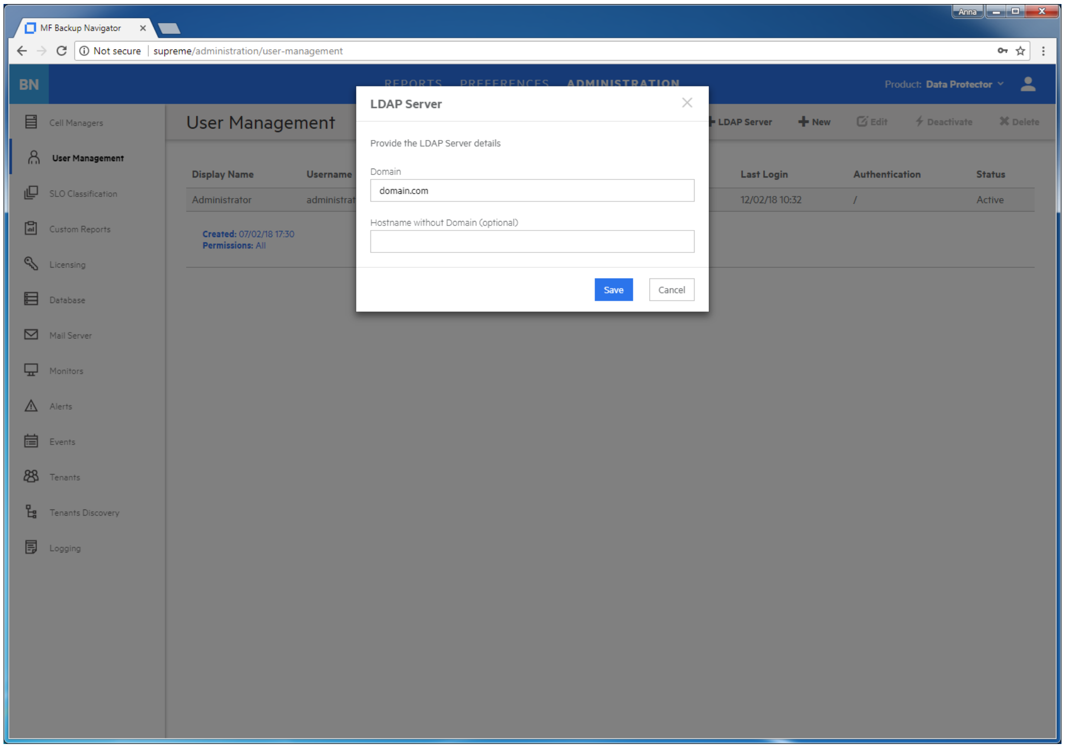
LDAP authentication is configured on the Backup Navigator server.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **User Management**.
3. In the Tool bar of the Results Area, click **LDAP Server**.
4. In the LDAP Server properties window, specify the domain name that should be recognized by the LDAP server.

   You can also specify the hostname, if you want that the LDAP server recognizes the specific host.

Figure 10: Specifying LDAP server



LDAP Server

Provide the LDAP Server details

Domain: domain.com

Hostname without Domain (optional):

Click **Save**.

The LDAP server is added successfully.

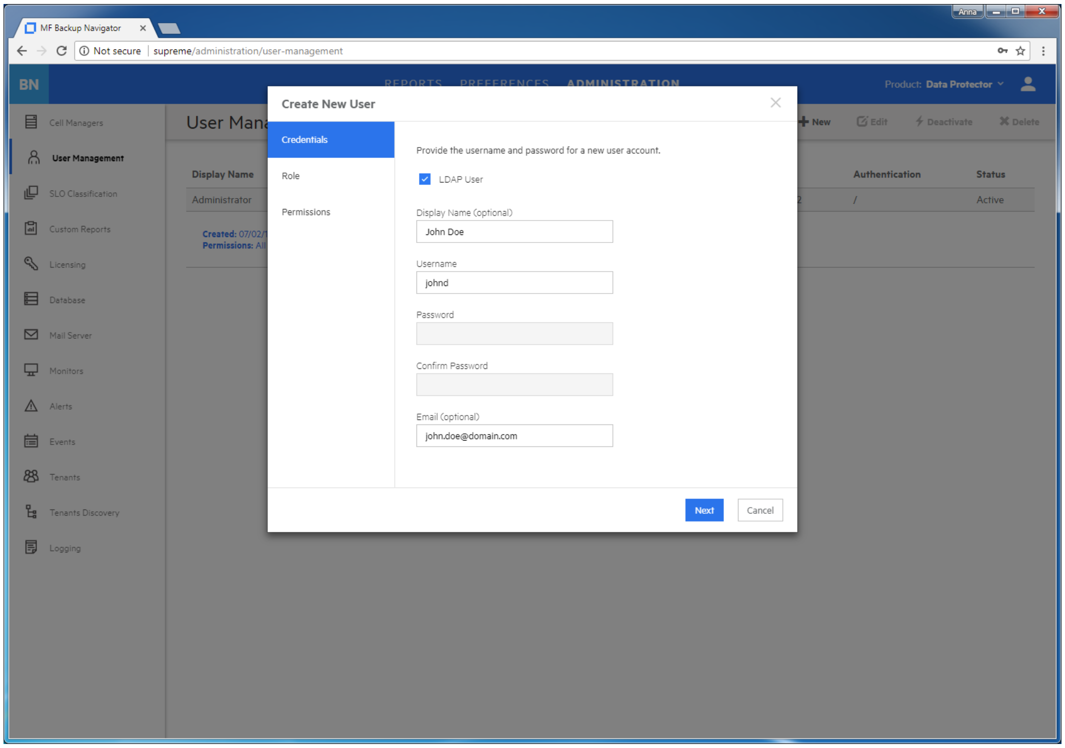
Creating new users

Create new users with the specific user roles.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **User Management**.
3. In the Tool bar of the Results Area, click **New**. The Create New User wizard displays.
4. If you added an LDAP server, select the **LDAP User** option. Enter the user display name, username, and password (for the LDAP user, the password from the LDAP server is used) of the user that you add to Backup Navigator and, optionally, the email. Click **Next**.

Figure 11: Creating a new user



Create New User

Provide the username and password for a new user account.

☑ LDAP User

Display Name (optional): John Doe

Username: johnd

Password:

Confirm Password:

Email (optional): john.doe@domain.com

5. Select **Administrator** or **Standard User** as a user role for this user account.

   If you selected `Administrator`, click **Finish**. If you selected `Standard User`, click **Next**.

6. For the Standard User, select the Data Protector Cell Managers the user can access to generate reports. Click **Finish**.

A new user account is added to the User Management table. You can later edit, deactivate or delete it.

> **IMPORTANT:** You cannot perform any actions on the account with which you are currently logged in to Backup Navigator.

Managing Service level objective categories

Backup Navigator provides an opportunity to assign different categories to a backup application depending on its service level objective (SLO). SLO category refers to a combination of the RTO (a time period needed before an application is brought back online) and the RPO (a time period when data can be lost after an event that causes an application to go offline occurs), which are specific for your backup environment goals. SLO categories are used for monitoring your backup applications.

There are three predefined SLO categories available within Backup Navigator:

SLO category	RPO	RTO
Gold	The maximum tolerable data loss interval, a time period in which data can be lost after an event that causes	The maximum tolerable time of disruption, a time period that is needed before an application is brought back

SLO category	RPO	RTO
	an application to go offline occurs, is up to 6 hours.	online, is less than 1 hour.
Silver	The maximum tolerable data loss interval, a time period in which data can be lost after an event that causes an application to go offline occurs, is from 6 to 12 hours.	The maximum tolerable time of disruption, a time period that is needed before an application is brought back online is less than 2 hours.
Bronze	The maximum tolerable data loss interval, a time period in which data can be lost after an event that causes an application to go offline occurs, is from 12 to 24 hours.	The maximum tolerable time of disruption, a time period that is needed before an application is brought back online is less than 4 hours.

You can change the predefined parameters within these categories and create the categories that mostly suit your backup environment goals.

Backup Navigator assigns a predefined SLO category to a backup application automatically during the initial data collection, if it is possible to retrieve data on RPO and RTO. If no SLO category is assigned during the initial collection, you can assign it later. You can recognize the backup applications without assigned SLO category in the Application Overview report and in the SLO Classification page.

- To create SLO categories, see Creating and editing SLO categories, below.
- To assign SLO categories, see Assigning SLO categories , on the next page.

Creating and editing SLO categories

Create a new SLO category or change the predefined one to meet the needs of your backup environment.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **SLO Classification**.
3. In the Results Area, click **Assign Category**.
4. In the Assign Category window, click **manage categories**.
5. In the Manage Categories window, do one of the following:
   - If you want to change parameters of the predefined SLO category, click on this category. Update the settings in the properties page and then click **Save**.
   - If you want to create a new category, click Create a New Category. Specify parameters in the properties page and then click **Save**.
6. Close the Manage Categories window you can now assign a new SLO category to backup applications.

Assigning SLO categories

Assign an SLO category to backup applications if you want to change their current SLO category or if no SLO category is currently assigned to them.

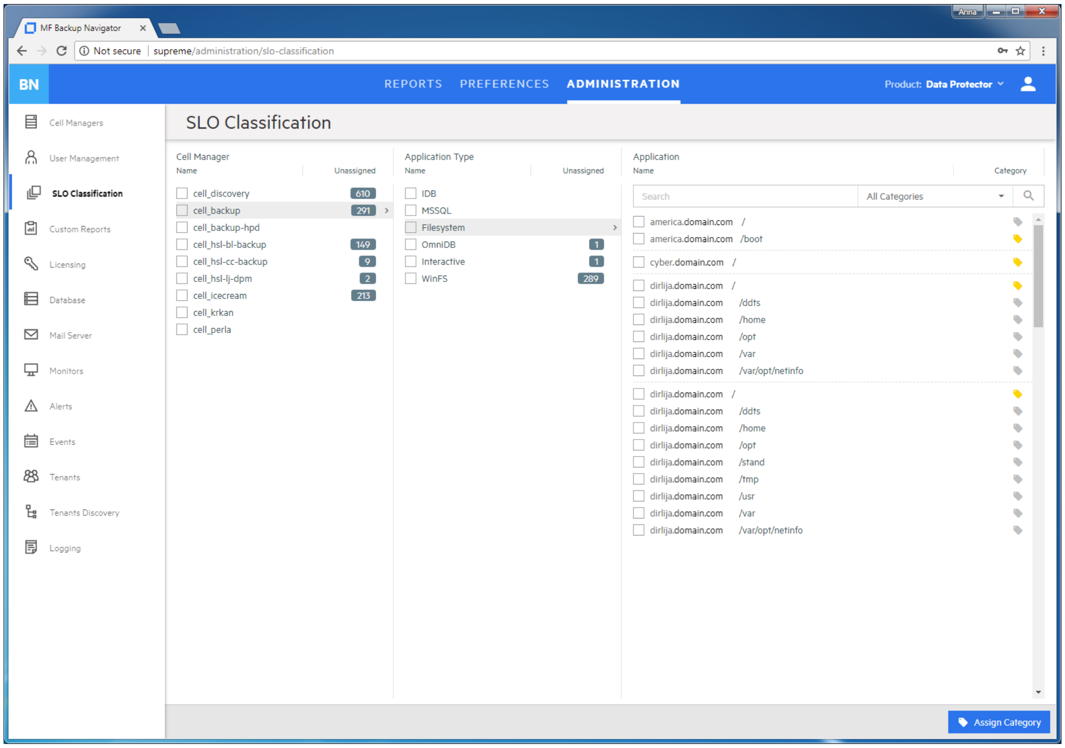
Prerequisite

The initial data collection was performed successfully.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **SLO Classification**.
3. In the Results Area, navigate to the backup applications, to which you want to assign an SLO category. Select the items to which you want to assign an SLO category.

> **IMPORTANT:** Click on the item to navigate to the child items. Select the check box, to select the item and its child items for assigning a category.



Cell Manager

Name	Unassigned
□ cell_discovery	610
□ cell_backup	291
□ cell_backup-hpd	
□ cell_hsl-bl-backup	149
□ cell_hsl-cc-backup	9
□ cell_hsl-lj-dpm	2
□ cell_icecream	213
□ cell_krkan	
□ cell_perla	

Application Type

Name	Unassigned
□ IDB	
□ MSSQL	
□ Filesystem	
□ OmniDB	1
□ Interactive	1
□ WinFS	289

Application

Name		Category
□ america.domain.com	/	
□ america.domain.com	/boot	
□ cyber.domain.com	/	
□ dirlija.domain.com	/	
□ dirlija.domain.com	/ddts	
□ dirlija.domain.com	/home	
□ dirlija.domain.com	/opt	
□ dirlija.domain.com	/var	
□ dirlija.domain.com	/var/opt/netinfo	
□ dirlija.domain.com	/	
□ dirlija.domain.com	/ddts	
□ dirlija.domain.com	/home	
□ dirlija.domain.com	/opt	
□ dirlija.domain.com	/stand	
□ dirlija.domain.com	/tmp	
□ dirlija.domain.com	/usr	
□ dirlija.domain.com	/var	
□ dirlija.domain.com	/var/opt/netinfo	

4. Click **Assign Category** to open the Assign Category window.
5. Select one of the available category. If you do not that a backup application belongs to any of the SLO categories, select `Excluded`.

   The selected SLO category is assigned to the selected backup applications. You can later unassign categories by clicking **Assign Category > clear category**.

Creating custom reports

Create a custom report to collect and analyze data of your choice.

Requirement

To create and manage custom reports, knowledge of SQL is required. For more information, see the related documentation.

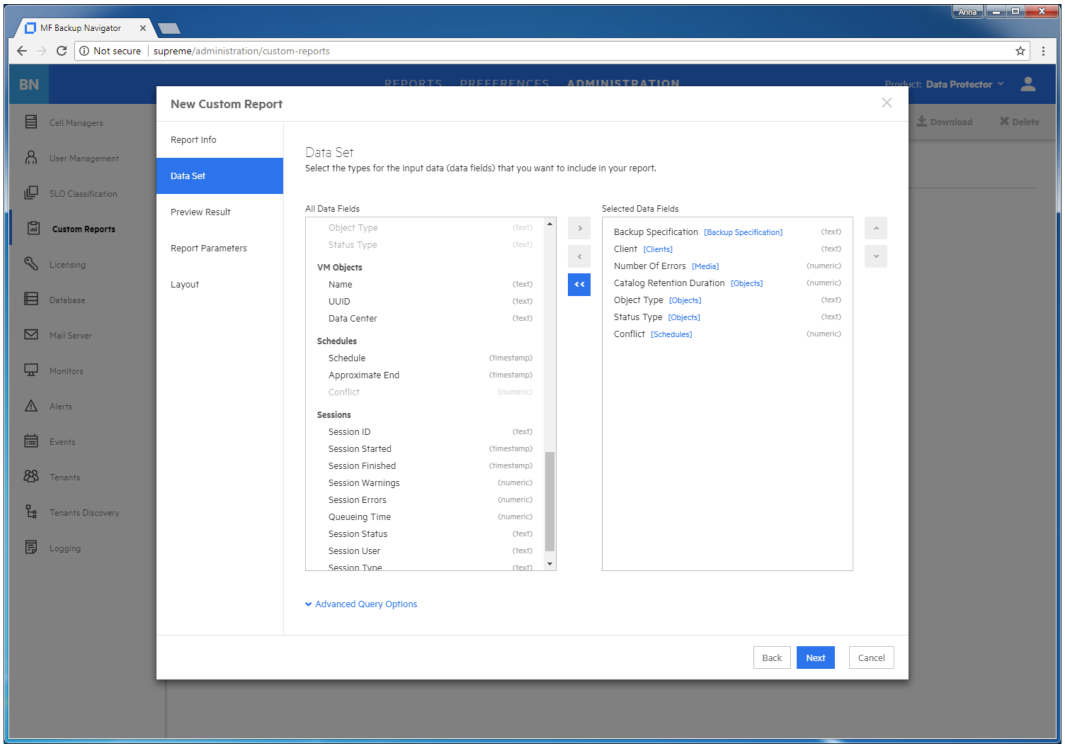
Limitation

You cannot specify the preferred unit values in the custom reports, the default Data Protector values are used.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Custom Reports**.
3. In the Results Area, click **New**. The New Custom Report wizard opens.
4. In the Report Info window, specify the custom report name and description, and select the report folder where you want to place your report. Click **Next**.
5. In the Data Set window, select the types for the input data (data fields) that you want to include in your report. The parameters are grouped by a subject of the report: backup specification, groups, clients, client type, libraries, media, media location, objects, VM objects, schedules, and sessions. The input data is collected and arranged in the report tables, each column representing the specified parameter.

Figure 12: Configuring custom reports



New Custom Report

Data Set

Select the types for the input data (data fields) that you want to include in your report.

All Data Fields

Object Type	(text)
Status Type	(text)
VM Objects	
Name	(text)
UUID	(text)
Data Center	(text)
Schedules	
Schedule	(timestamp)
Approximate End	(timestamp)
Conflict	(numeric)
Sessions	
Session ID	(text)
Session Started	(timestamp)
Session Finished	(timestamp)
Session Warnings	(numeric)
Session Errors	(numeric)
Queueing Time	(numeric)
Session Status	(text)
Session User	(text)
Session Type	(text)

Selected Data Fields

Backup Specification [Backup Specification]	(text)
Client [Clients]	(text)
Number Of Errors [Media]	(numeric)
Catalog Retention Duration [Objects]	(numeric)
Object Type [Objects]	(text)
Status Type [Objects]	(text)
Conflict [Schedules]	(numeric)

If you want to fine tune the query by aggregating columns and creating conditions and sorting rules, click the **Advanced Query Options** link and then specify the Aggregate and Group By options for each selected column. Specify the sorting, limit, and other options for your report.

Click **Next**.

6. In the Preview Result window, verify whether the query you specified meets your requirements. If you want to [preview the report, click the **SQL Editor** link and click **Run**.
7. In the Report Parameters page, you can enable and select the default time range for your report. To enable the default date range, select **Enable Date Range** and then select one of the available options from the drop-down list. Otherwise, the last 7 days range is used. Click **Next**.
8. In the Layout window, select a presentation type of your report. Select **Table**, if you want to view your report as a table. Select **Chart**, if you want to view your report in graphical presentation *and* a table.

   Select the table columns for the table presentation type. Select the chart orientation, specify X and Y axis for a chart. Click **Finish**.

The report is added to the selected report subcategory in the Navigation Pane. You can later make modifications to a custom report by selecting a specific report and then clicking **Edit**.

Downloading custom reports

Save a custom report to a preferred location to be able to upload it later to another server. You can share the saved custom reports between different Backup Navigator environments later.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Custom Reports**.
3. In the Results Area, select the custom report that you want to download.
4. In the Tool bar of the Results Area, click **Download**.
5. Save the report as a ZIP file in a specified location.

Uploading custom reports

Upload a report created on a different Backup Navigator server.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Custom Reports**.
3. In the Tool bar of the Results Area, click **Upload**.
4. In the Upload Custom Report window, name your report and browse for the report file that you want to upload. select the report category and subcategory where you want to place the uploaded report.
5. Click **Upload**.
6. When the upload process is finished, close the dialog box. The report is added to the selected report subcategory.

Maintaining database

Ensure regular backups, archiving, and clean-up of the Backup Navigator database. Be prepared for a potential recovery. For the related procedures, see the PostgreSQL documentation.

You can use pgAdmin GUI to administer PostgreSQL. You can download this tool from: http://www.pgadmin.org/download/

To view the database settings in the web user interface, see Viewing database settings, below.

You can perform the following database maintenance tasks in Backup Navigator:

- Purging the database. See Purging database, on the next page.
- Performance tuning. See Tuning database performance, on the next page.

Viewing database settings

You can view the database settings information.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Database**. The database settings information is displayed. To

change these settings perform the procedure described in Maintaining database, on the previous page.

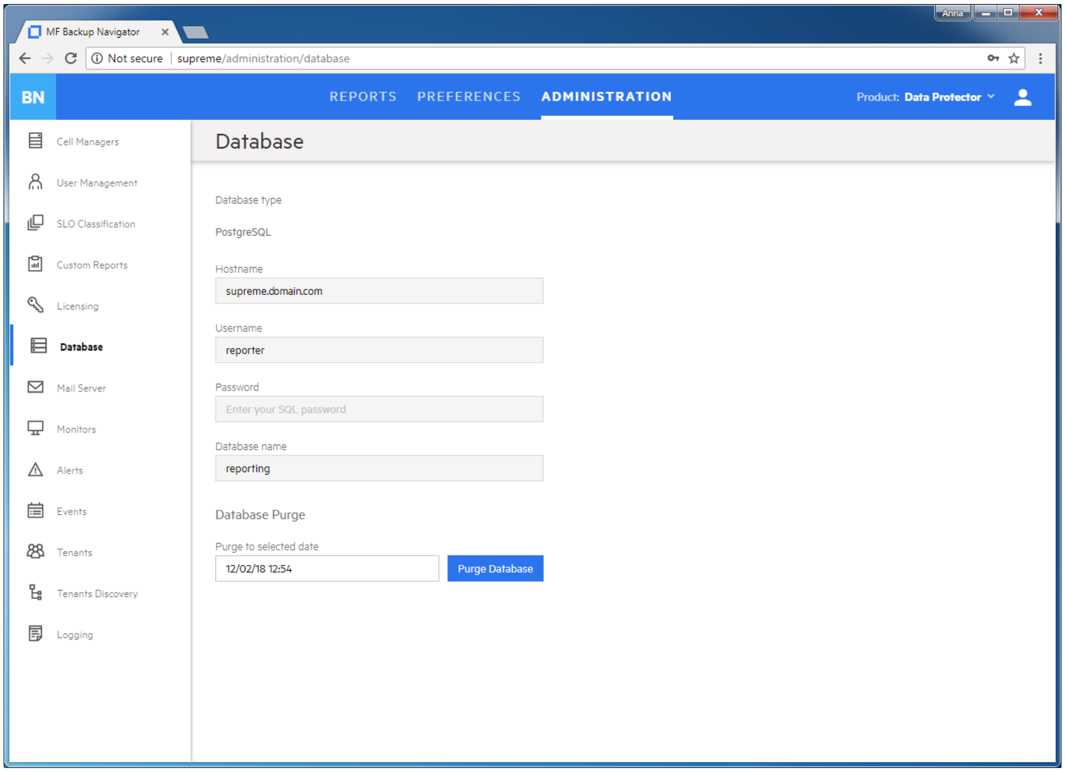
Purging database

You can use the Backup Navigator web user interface to clean up the database.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Database**. The database settings information is displayed. Under Database Purge, specify the date, up to which you want to purge the Backup Navigator database and then click **Purge Database**.

   Figure 13: Database settings



Database

Database type
PostgreSQL

Hostname
supreme.domain.com

Username
reporter

Password
Enter your SQL password

Database name
reporting

Database Purge

Purge to selected date
12/02/18 12:54

3. In the Purge Database window, select to purge all cells or specify the cells you want to purge. Click **Purge** and then click **Confirm**.

   During the database cleanup, the data older than the specified date is deleted.

Tuning database performance

When you install and configure Backup Navigator, PostgreSQL database server is also configured. The provided default settings related to the database performance correspond to the minimum system requirements and are as follows:

```
shared_buffers = 1000MB
effective_cache_size = 2000MB
```

```
work_mem = 64MB
maintenance_work_mem = 256MB
```

If the memory resources of your Backup Navigator allow, you can allocate more memory resources to improve performance. If you consider that the Backup Navigator performance is not sufficient, you can change the performance related settings to tune the performance to the needs of your specific environment. For the description of these settings and detailed procedures, see the PostgreSQL documentation.

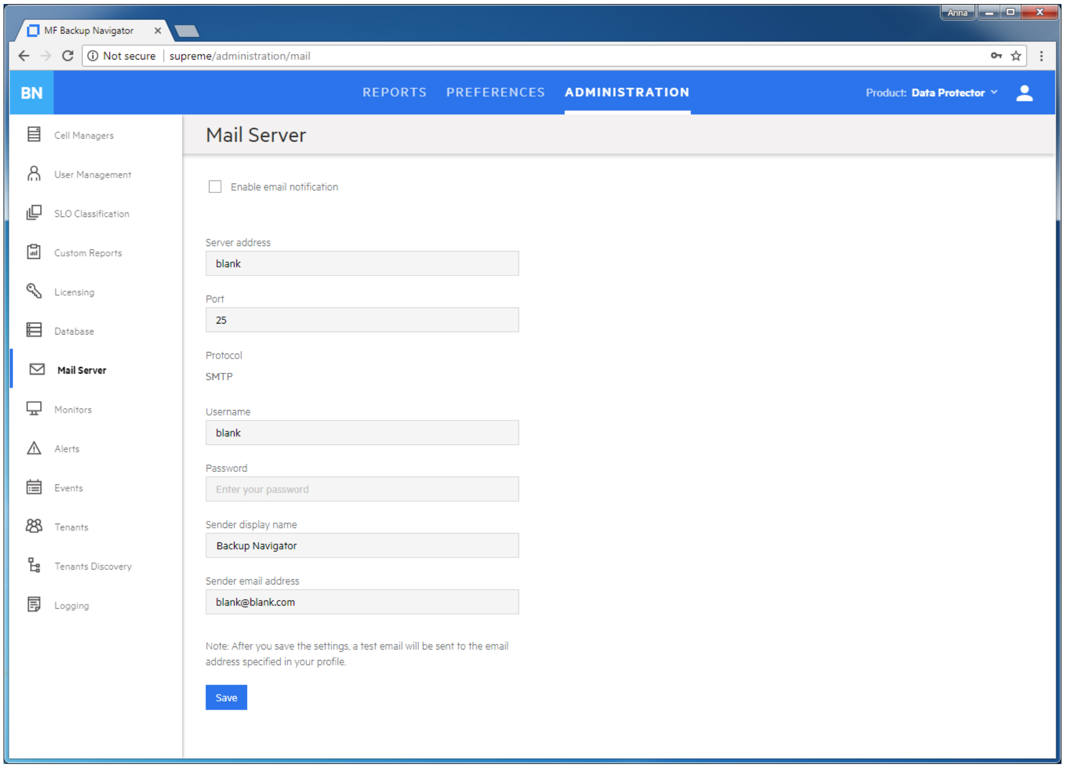
Configuring mail server

Configure your mail server to be able to receive emails.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Mail Server**.

Figure 14: Configuring Mail Server



Mail Server

□ Enable email notification

Server address
blank

Port
25

Protocol
SMTP

Username
blank

Password
Enter your password

Sender display name
Backup Navigator

Sender email address
blank@blank.com

Note: After you save the settings, a test email will be sent to the email address specified in your profile.

3. In the Results Area, select **Enable email notification**.
4. Enter the web address of the server, which you want to use for sending emails.
5. Enter the server port, username, and password.
6. Enter the sender's display name and email address (mandatory).
7. Click **Save**. A test email is sent to the specified email address.

You can always change these settings later.

Monitoring the Data Protector environment

You can use the data collected for reports from the Data Protector cells to monitor different aspects of the Data Protector environment. Use the Backup Navigator monitoring functionality to be notified about the specified events and conditions in the Data Protector environment.

Backup Navigator provides predefined monitors for the data protection basic functionality, such as backup success, device utilization, media quality, and so on. For the complete list and description of the predefined monitors, see Predefined monitors, below.

You can use the predefined monitors and create the monitors that cover your needs. For the detailed procedure, see Creating and using monitors, on page 60

You get notified about the conditions and events specified in the monitors by alerts or event notifications. Use alerts to ensure the priority handling of the detected problem. An alert requires user acknowledgment and resolution. Alert messages contain a potential cause of the event or condition and offer a resolution. For more information on handling the triggered alerts and logged events, see Handling alerts, on page 61 and Viewing events, on page 62.

Predefined monitors

Backup Navigator provides the predefined monitors for your Data Protector environment. You can view this monitors in the Backup Navigator, enable, disable, and edit them. You can edit the scope of the monitored entities as well as parameters, values, and action types.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Monitors**.

A list of the following default monitors displays:

Application without retention	
Description	Monitors applications and detects those not protected with backup.
Monitored category	Application
Metric Type	Retention
Parameters	n/a
Actions	Trigger `EVENT` metric value = 0 Event level: `Critical`

Backup session failure after backup specification modification	
Description	Monitors backup session after the backup specification modification. Issues an event notification, if the backup session fails.

Backup session failure after backup specification modification	
Monitored category	Backup specification
Metric Type	Session failure count after modification
Parameters	n/a
Actions	Trigger `EVENT` metric value > 0 Event level: `Warning` metric value > 1 Event level: `Critical`

Backup session without objects	
Description	Monitors the backup session. When a backup session has no specified objects, issues a critical alert.
Monitored category	Session
Metric Type	Object count
Parameters	Session type = `Backup`; Backup Type = `All`
Actions	Trigger `ALERT` Alert level: `Critical` **Cause:** Can indicate that the backed up client or application instance is not available. **Resolution:** Check the client or instance availability.

Backup specification expected session duration exceeded	
Description	Monitors the duration of a backup session. Issues an alert, when the expected duration for this backup session is exceeded.
Monitored category	Backup specification
Metric Type	Estimated percentage session duration change
Parameters	Session type = `Backup`
Actions	Trigger `ALERT` 20% < metric value < 40 % Alert level: `Warning` 40 % < metric value Alert level: `Critical` **Cause:** Can be caused by recent backup specification changes. **Resolution:** Check if there are any recent changes for the backup specification.

Data Protector IDB RPO	
Description	Monitors time since the last successful backup of the Data Protector internal database. Issues alert, when the last IDB backup was performed more than the specified number of days or hours.
Monitored category	Cell
Metric Type	Data Protector IDB RPO
Parameters	n/a
Actions	Trigger `ALERT` metric value > `X days|hours` Alert level: `Warning` **Cause:** Cannot find a successful Data Protector internal database backup for cell within the specified period of time. **Resolution:** Perform a successful Data Protector internal database backup. metric value > `Y days|hours` Alert level: `Critical` **Cause:** Cannot find a successful Data Protector internal database backup for cell within the specified period of time. **Resolution:** Perform a successful Data Protector internal database backup.

Device daily utilization too low	
Description	Monitors device utilization in the last 7 days. Issues an event notification, if the device utilization is lower than 90%.
Monitored category	Device
Metric Type	Daily utilization
Parameters	Time range = Last 7 days
Actions	Trigger `EVENT` 80% < metric value < 90% Event level: `Warning` metric value < 80% Event level: `Critical`

Media pool quality	
Description	Monitors the media pools quality. Issues an event notification if less than 10% of media in the pool is of a `Good` condition.
Monitored category	Media
Metric Type	Quality

Media pool quality	
Parameters	n/a
Actions	Trigger `Event` 5% < metric value < 10% Event level: `Warning` metric value < 5% Event level: `Critical`

RPO	
Description	Monitors backup applications with an assigned SLO category. The monitor compares the time between the last and previous successful application backups (RP) with the maximum tolerable data loss interval (RPO) specified in the assigned SLO category.
Monitored category	Application
Metric Type	RPO
Parameters	SLO category.
Actions	Trigger `EVENT` RP exceeds the RPO specified in the SLO category. **Cause:** Application backups are scheduled too seldom. **Resolution:** Reschedule your application backups to align the schedule with the RPO.

RTO	
Description	Monitors backup applications with an assigned SLO category. The monitor compares the estimated time needed for successful application recovery (RT) with the time acceptable for restore the backed up data (RTO) specified in the assigned SLO category.
Monitored category	Application
Metric Type	RTO
Parameters	SLO category
Actions	Trigger `EVENT` RT exceeds the RTO specified in the SLO category. **Cause:** Application backups chain is too long and it takes more time to restore it. **Resolution:** Consider rescheduling your application backups to decrease the backup chain and consequently the RT. For example, you can decrease the number of incremental backups by scheduling the full backups more frequently.

Session queuing time too long	
Description	Monitors the duration of backup session queuing time. Issues an alert, if a session is in the queue for more than 30 minutes.
Monitored category	Session
Metric Type	Queuing time
Parameters	Session type = Backup; Backup Type = All
Actions	Trigger `ALERT` metric value > 30 min Alert level: `Warning` metric value > 30 min Alert level: `Warning` **Cause:** Can indicate that the resources, devices, or application required by session are not available. **Resolution:** If this is a scheduled operation, check schedule conflicts.

Session overlapping	
Description	Monitors backup sessions started for the same backup specification and identifies the sessions overlapping.
Monitored category	Session
Metric Type	Overlapping
Parameters	n/a
Actions	Trigger `ALERT\` **Cause:** The backup session is running longer than expected (for example, because of unavailable target device) or backups are scheduled too frequently. **Resolution:** Identify the cause of overlapping and resolve the issue accordingly.

Session success rate	
Description	Monitors backup session success rate and issues notification, when the success rate is 98 % or lower.
Monitored category	Cell
Metric Type	Success rate
Parameters	Time range = `Last 24h`; Session type = `ALL`; Type = `Backup`
Actions	Trigger `EVENT` metric value >= 98% Event level: `Normal`

Session success rate	
	98% > metric value >= 96% Event level: `Warning` metric value < 96% Event level: `Critical`

Media pool low free space	
Description	Monitors the media pools free space. Issues an event notification, when the free space is lower than 10%
Monitored category	Media
Metric Type	Free space
Parameters	n/a
Actions	Trigger `EVENT` 5% < metric value < 10% Event level: `Warning` metric value < 5% Event level: `Critical`
Unexpected backup size	
Description	Monitors the backup size. Issues alert, if the backup transfer size differs from what was expected.
Monitored category	Backup specification
Metric Type	Predicted percentage backup size change
Parameters	n/a
Actions	Trigger `EVENT` `20%` > metric value > `10%` Event level: `Warning` metric value > `20%` Event level: `Critical`

Creating and using monitors

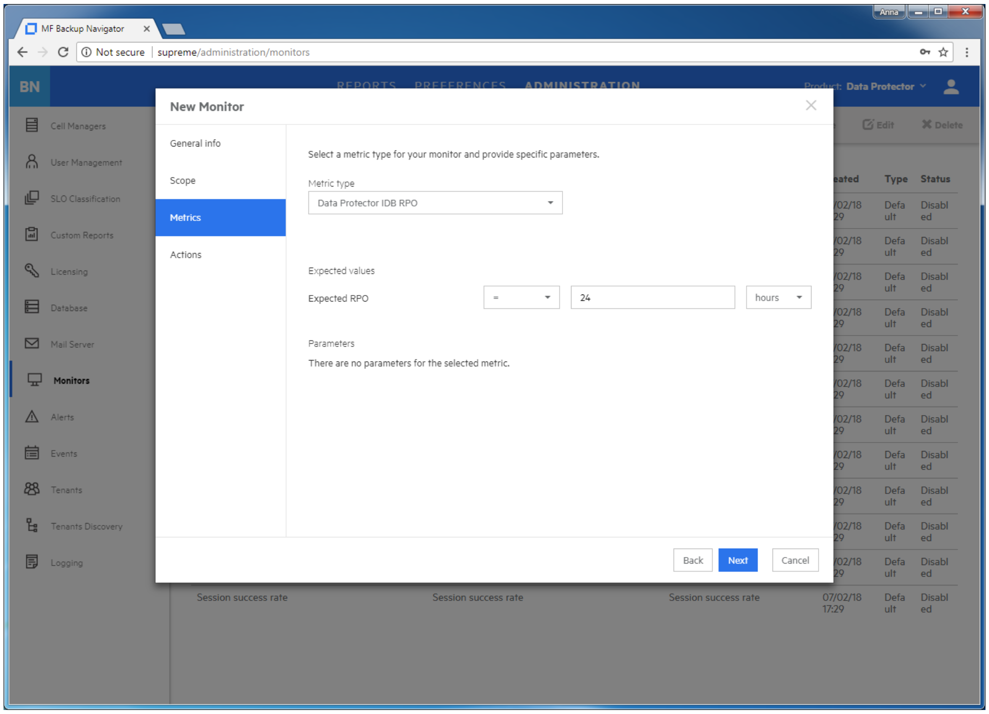
To get notifications on the specific events or alerts, you can create Backup Navigator monitors.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Monitors**.
3. In the Results Area, click **New**. The New Monitor wizard opens.
4. In the General info window, specify the monitor name and description. Click **Next**.
5. In the Scope window, select a category you want to monitor. You can select one of the following categories: application, backup specification, cell, device, media, session. Select a scope of entities related to the specified category. Click **Next**.

6. In the Metrics window, select the metric type available for the specified category and parameters, if applicable. Click **Next**.

   Figure 15: Creating monitors



Select a metric type for your monitor and provide specific parameters.

Metric type: Data Protector IDB RPO

Expected values

Expected RPO = 24 hours

Parameters

There are no parameters for the selected metric.

7. In the Actions window, specify one or more conditions by selecting parameters, operators, and setting values. If you want to specify more than one condition, click **Add condition**.

   Select **Alert** or **Event** as an Action type and the severity level. You can specify both action types in the same monitor for different conditions or values. To specify the more action types, click **Add action**.

   To be notified about the occurred alert or event by email, select **Send email notification**.

   Click **Finish**.

The newly created monitor appears on the monitors list. You can enable or disable monitors.

Handling alerts

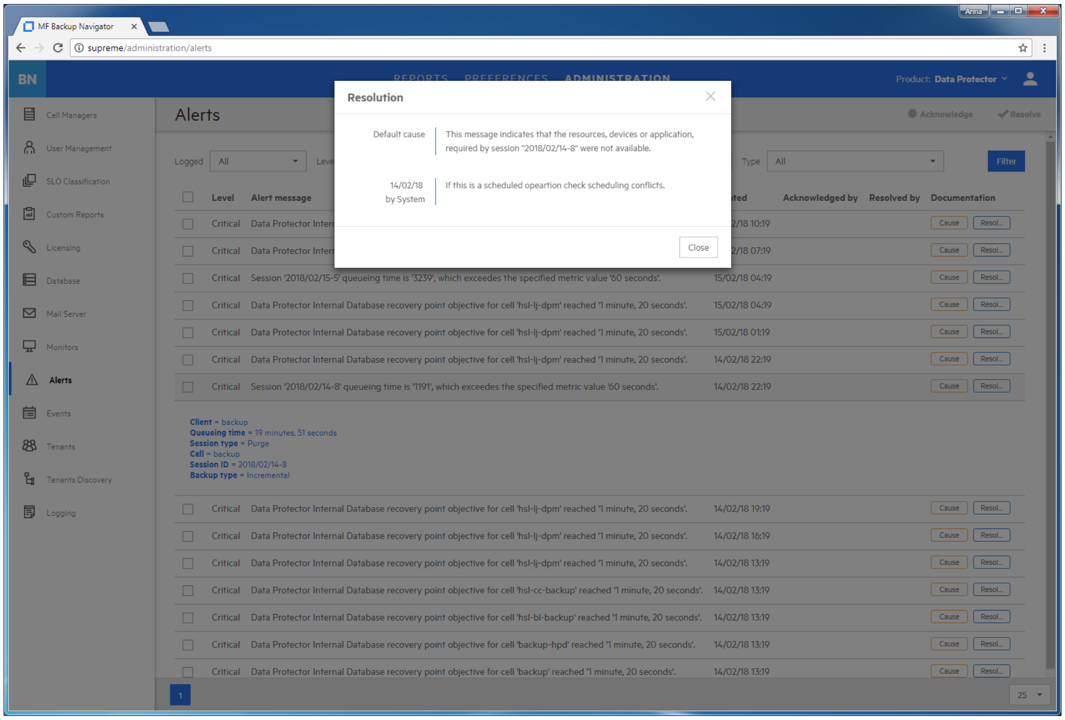
You can view the alerts triggered in Backup Navigator. An alert is logged when the conditions specified in the monitors are met.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Alerts**. A table with the Backup Navigator alerts displays. You can filter and sort the table by name, severity level, and timeframe. To apply the specified filter, click **Filter**.
3. To view the specific alert details, double-click it. Alert provides a description of a potential cause and offers a resolution.

4. Select the alert and then click **Acknowledge**. By acknowledging an alert, you confirm that you are notified about the event or specified conditions, and start troubleshooting actions.
5. After you handle the reported problem appropriately, select the alert and then click **Resolve**. You can add your resolution comments, click **Resolve**.

Figure 16: Resolving alerts



Resolution

Default cause	This message indicates that the resources, devices or application, required by session "2018/02/14-8" were not available.
14/02/18 by System	If this is a scheduled opeartion check scheduling conflicts.

Close

☐	Level	Alert message	ted	Acknowledged by	Resolved by	Documentation
☐	Critical	Data Protector Inter	2/18 10:19			Cause Resol...
☐	Critical	Data Protector Inter	2/18 07:19			Cause Resol...
☐	Critical	Session '2018/02/15-5' queueing time is '3239', which exceedes the specified metric value '60 seconds'.	15/02/18 04:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	15/02/18 04:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	15/02/18 01:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	14/02/18 22:19			Cause Resol...
☐	Critical	Session '2018/02/14-8' queueing time is '1191', which exceedes the specified metric value '60 seconds'.	14/02/18 22:19			Cause Resol...
		Client = backup **Queueing time** = 19 minutes, 51 seconds **Session type** = Purge **Cell** = backup **Session ID** = 2018/02/14-8 **Backup type** = Incremental				
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	14/02/18 19:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	14/02/18 16:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-lj-dpm' reached '1 minute, 20 seconds'.	14/02/18 13:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-cc-backup' reached '1 minute, 20 seconds'.	14/02/18 13:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'hsl-bl-backup' reached '1 minute, 20 seconds'.	14/02/18 13:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'backup-hpd' reached '1 minute, 20 seconds'.	14/02/18 13:19			Cause Resol...
☐	Critical	Data Protector Internal Database recovery point objective for cell 'backup' reached '1 minute, 20 seconds'.	14/02/18 13:19			Cause Resol...

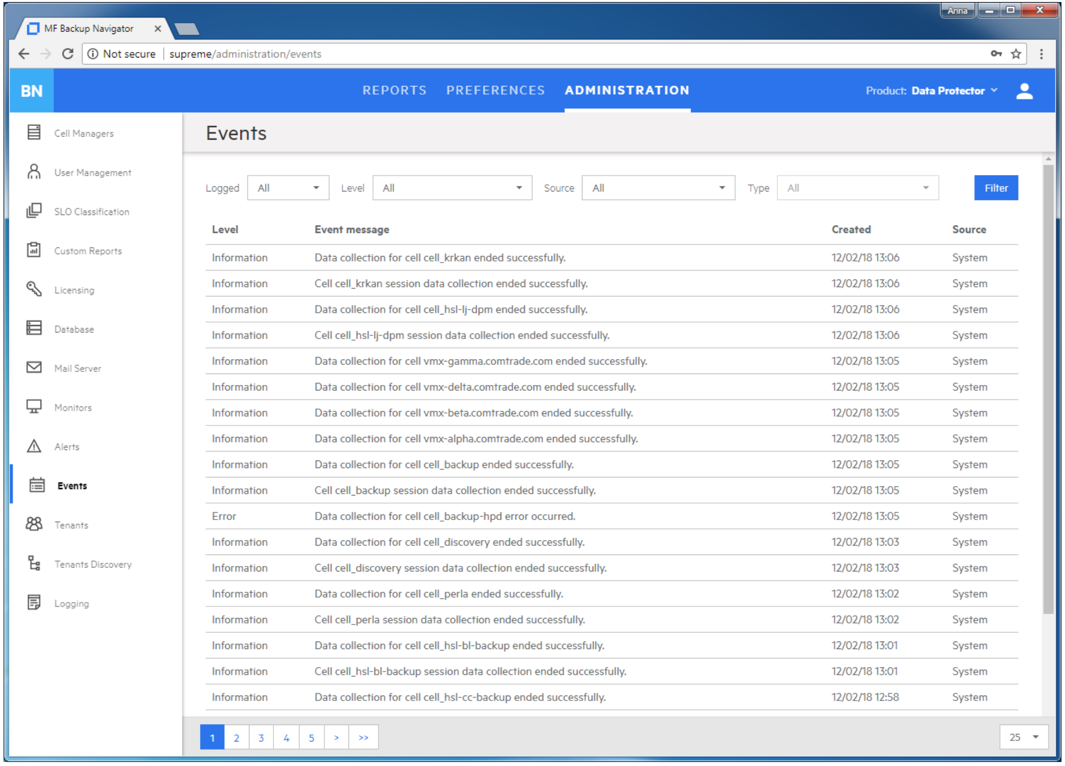
Viewing events

You can view the events occurred in Backup Navigator. An event is logged, when the conditions specified in the monitors are met.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Events**. A table with the Backup Navigator events displays. You can filter and sort table by name, severity level, and timeframe. To apply the specified filter, click **Filter**.
3. To view the specific event details, double-click it.

Figure 17: Events list



Events

Logged: All | Level: All | Source: All | Type: All

Level	Event message	Created	Source
Information	Data collection for cell cell_krkan ended successfully.	12/02/18 13:06	System
Information	Cell cell_krkan session data collection ended successfully.	12/02/18 13:06	System
Information	Data collection for cell cell_hsl-lj-dpm ended successfully.	12/02/18 13:06	System
Information	Cell cell_hsl-lj-dpm session data collection ended successfully.	12/02/18 13:06	System
Information	Data collection for cell vmx-gamma.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-delta.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-beta.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-alpha.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell cell_backup ended successfully.	12/02/18 13:05	System
Information	Cell cell_backup session data collection ended successfully.	12/02/18 13:05	System
Error	Data collection for cell cell_backup-hpd error occurred.	12/02/18 13:05	System
Information	Data collection for cell cell_discovery ended successfully.	12/02/18 13:03	System
Information	Cell cell_discovery session data collection ended successfully.	12/02/18 13:03	System
Information	Data collection for cell cell_perla ended successfully.	12/02/18 13:02	System
Information	Cell cell_perla session data collection ended successfully.	12/02/18 13:02	System
Information	Data collection for cell cell_hsl-bl-backup ended successfully.	12/02/18 13:01	System
Information	Cell cell_hsl-bl-backup session data collection ended successfully.	12/02/18 13:01	System
Information	Data collection for cell cell_hsl-cc-backup ended successfully.	12/02/18 12:58	System

Managing tenants and tenant groups

A tenant is a group of users, usually related to one customer or department, who share Data Protector resources. Each tenant is represented by the dedicated Data Protector elements, such as cells, backup specification groups, backup specifications, or clients.

Tenants are logical organizational structures and they cannot be specifically defined in the Data Protector environment. However, a good practice is to follow naming conventions to structure your backup environment in logical order. You can use certain tenant related prefixes or postfixes with tenant names in the names of backup groups, backup specifications, or clients to easily recognize to which tenant these elements belong. For recommendations on naming conventions, see Tenant naming conventions, on the next page.

Before you can generate reports based on tenants related data, you should discover which tenants already exist in the Data Protector environment, and add them to the Backup Navigator. Perform the following tasks:

- Define one or more rules (depending on the approach you use to identify your tenants) to be able to discover tenants in the Data Protector environment. See Discovering tenants, on the next page.
- Import tenants from the Data Protector environment using the created discovery rules. See Importing tenants, on page 68.
- You can add new tenants and tenant groups, and add tenants to tenant groups. See Creating tenants, on page 69 and Creating tenant groups, on page 70.

Tenant naming conventions

You can use the following approach to name the elements of your backup environment to be able to discover tenants:

- If you allocate one or more cells per tenant, you can discover such tenants without using naming conventions.
- If you use one or more backup groups per tenant:
  - For a backup group per tenant configuration, use the tenant ID (tenant name) as a backup group name. For example, if you have tenants Customer1, Customer2, and Customer3, name backup groups as follows: `customer1`, `customer2`, and `customer3`. Ensure, that names of the backup specifications from such groups contain the parent backup group name.
  - For multiple backup groups per tenant configuration, use the tenant ID (tenant name) as a part of the backup group name delimited with one of the supported characters (for example, "_" (underscore)). If a tenant owns backup groups in different cells, ensure that the tenant ID is unique across the related cells.

    For example, if you have tenants Customer1 and Customer2, name your backup groups as follows: `customer1_backupgroup1`, `customer1_backupgroup2`, `customer1_backupgroup3`, `customer2_backupgroup1`, and `customer2_backupgroup2`.
- If you use several backup specifications per tenant:

  Ensure, that the backup specification names contain the tenant ID (tenant name) and the backup group name delimited with one of the supported characters (for example, "_" (underscore)). If a tenant owns backup specifications in different cells, ensure that the tenant ID is unique across the related cells.

  For example, if you have tenants Customer1 and Customer2, name your backup specifications as follows: `customer1_backupgroup1_full`, `customer1_backupgroup1_incr`, `customer1_backupgroup1_sap`, `customer2_backupgroup1_full`, and `customer2_backupgroup1_incr`.
- If you allocate one or more clients per tenant:

  Use the tenant ID (tenant name) as a part of the client name or as a prefix of the client delimited with one of the supported characters (for example, "_" (underscore)). If tenants own clients in different cells, ensure that the tenant ID is unique across the related cells. For example, if you have tenants Customer1 and Customer2 with two clients each, name the clients as follows: `customer1_host1.com`, `customer1_host2.com`, `customer2_host3.com`, and `customer2_host4.com`.

> **NOTE:**
> Using delimiters in the tenant makes the tenant discovery easier. Without delimiters, you need to create regular expressions to identify tenant IDs.

Discovering tenants

Before you can generate reports for specific tenants, you should first create a tenant discovery rule for discovering tenants in your Data Protector backup environment.

Prerequisites

- You use tenant naming conventions in your Data Protector backup environment.
- You added the Data Protector cells that you want to use for tenant discovery to the Backup Navigator environment.

Considerations

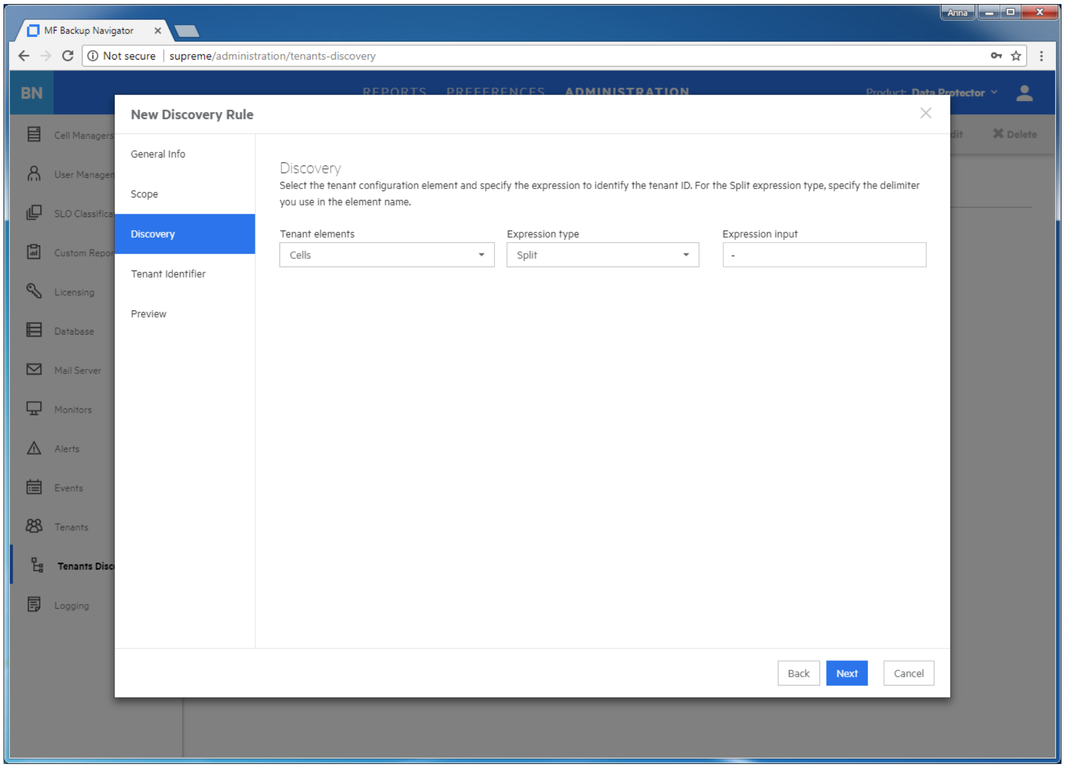
- You can use one discovery rule to discover multiple tenants, if you use the same approach to identify them.
- You can use a Data Protector cell in one discovery rule only. If multiple tenants share one cell, you can use one discovery rule for them and then use this rule to import different tenants.
- When you add a new Data Protector cell to the Backup Navigator environment and you want to collect tenant related reports from it, add this cell to an existing discovery rule, or create a new discovery rule for this cell.
- You cannot use the same tenant ID in different rules and for different tenant types (backup specification, backup groups, or clients).

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Tenants Discovery**.
3. In the Tool bar of the Results Area, click **New**.
4. In the New Discovery Rule wizard, enter a tenant discovery rule name and description. Click **Next**.
5. Select the cells you want to use for this tenant discovery rule. Click **Next**.
6. Specify the discovery rule you want to use for this tenant discovery. In the Tenant elements drop-down list, select the Data Protector element you allocate for the tenants you want to discover. In the Expression type drop-down list, select **Split** (if you use characters to delimit a tenant ID in the respective element name) or **Regular expression**. In the Expression input text box, specify one of the following:
   - For the **Split** expression type, specify the character you use as a tenant ID delimiter (for example. "_", underscore).

     If you do not specify any delimiter, all the elements specified in the Group drop-down list will be discovered.

Figure 18: Creating discovery rule using Split expression type



New Discovery Rule

Discovery

Select the tenant configuration element and specify the expression to identify the tenant ID. For the Split expression type, specify the delimiter you use in the element name.

Tenant elements: Cells

Expression type: Split

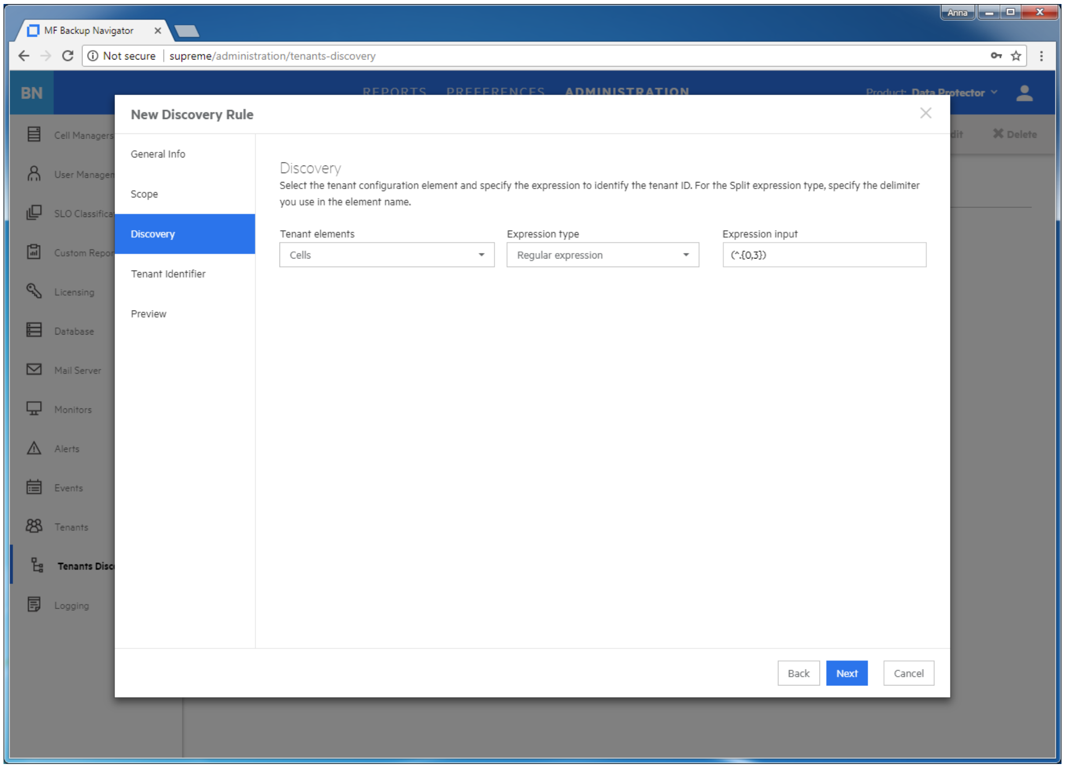
Expression input: -

- For the **Regular expression** expression type, specify the regular expression using Java syntax.

Example of the regular expression

To specify the first three characters as a tenant ID, use the expression: `(^.{0,3})`.

Figure 19: Creating discovery rule using Regular expression



New Discovery Rule

Discovery

Select the tenant configuration element and specify the expression to identify the tenant ID. For the Split expression type, specify the delimiter you use in the element name.

Tenant elements: Cells

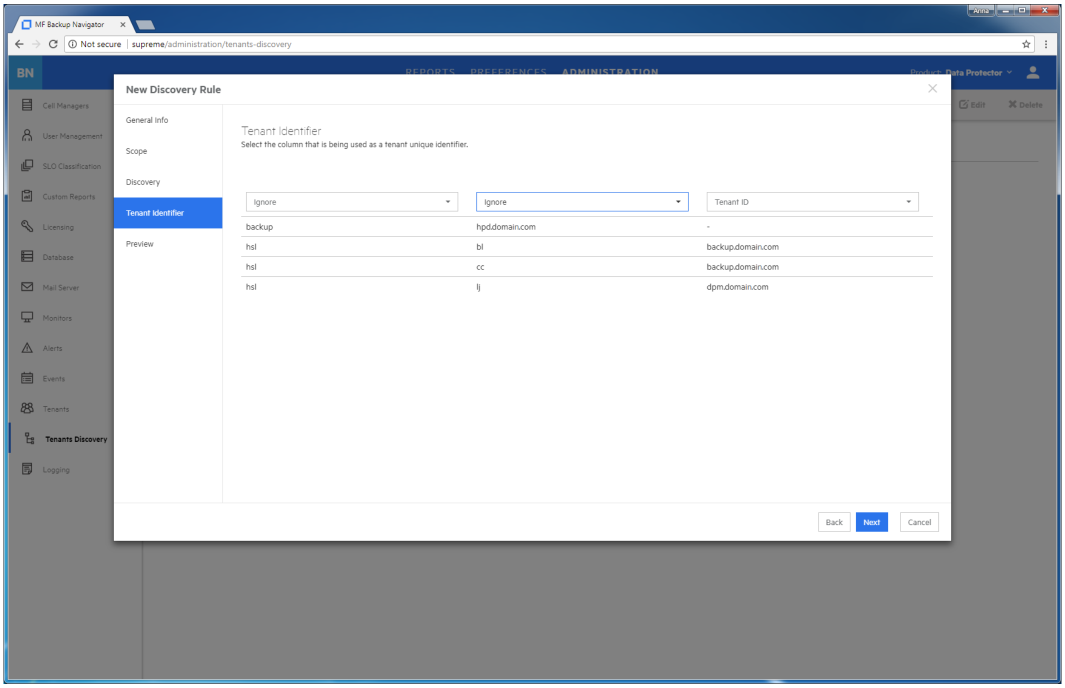
Expression type: Regular expression

Expression input: (^.{0,3})

Click **Next**.

7. In the Tenant Identifier page, a list of the discovered tenant elements displays. If you split the elements names and more than one potential tenant ID is recognized, a table lists all potential tenant IDs. Select the column with the tenant ID you specified and in the column header drop-down list, select **Tenant ID**, other column headers will contain `Ignore`. Click **Next**.

Figure 20: Selecting Tenant identifier in the tenant name



Tenant Identifier

Select the column that is being used as a tenant unique identifier.

Ignore	Ignore	Tenant ID
backup	hpd.domain.com	-
hsl	bl	backup.domain.com
hsl	cc	backup.domain.com
hsl	lj	dpm.domain.com

8. The Preview page lists the discovered tenants. You can preview the list of tenants and the content of each tenant by clicking **Preview** while hovering over it. Click **Finish** to save the tenant discovery rule.

   A newly created tenant discovery rule is added to the discovery rules list in the Tenants Discovery page.

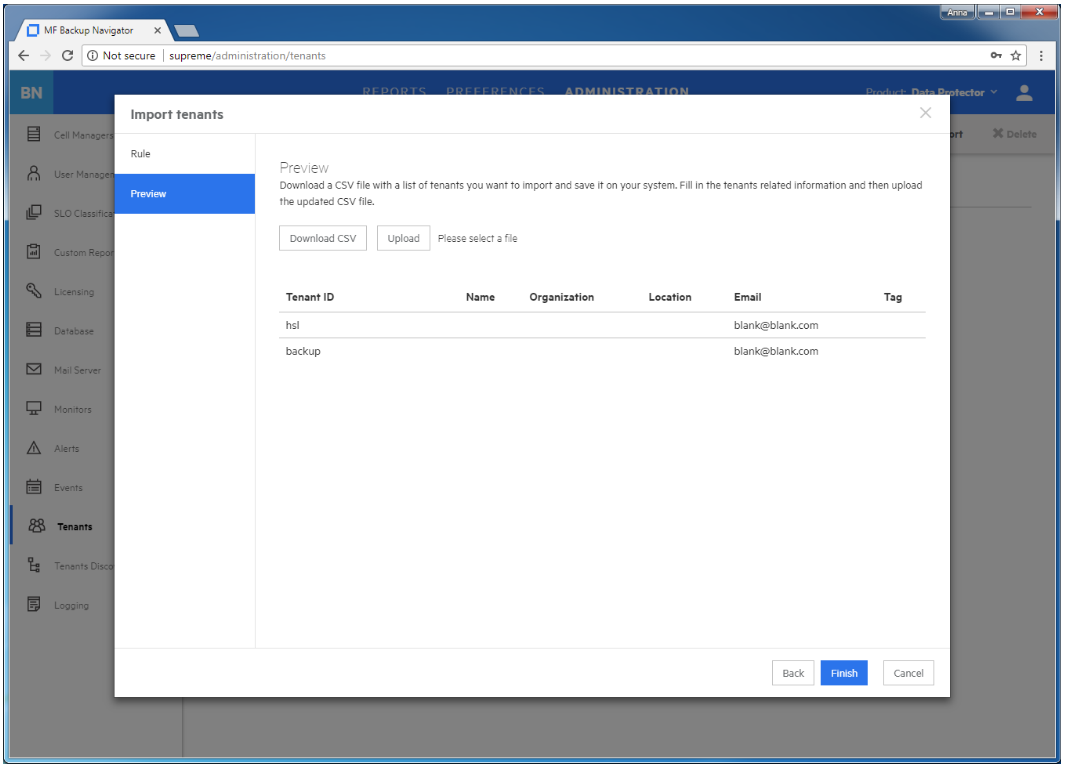
Importing tenants

After you create a rule for the tenants discovery and discover tenants, you can add them to the Backup Navigator environment. Use the import functionality when you add the tenants for the first time and when you add a great number of tenants. If you want to add one or a small number of tenants, see Creating tenants, on the next page.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Tenants**.
3. In the Tool bar of the Results Area, click **Import**.
4. In the Import tenant wizard, select a tenant discovery rule. Click **Next**.
5. In the Preview page, view a list of tenants you will import. Click **Download CSV** to download a `tenants.csv` file with a list of tenants you want to import and save it on your system. Fill in the tenants related information (organization, location, e-mail, and so on) and then upload the updated file to the Backup Navigator by clicking **Upload**. Then click **Finish**.

Figure 21: Importing tenants



Import tenants

Preview

Download a CSV file with a list of tenants you want to import and save it on your system. Fill in the tenants related information and then upload the updated CSV file.

Please select a file

Tenant ID	Name	Organization	Location	Email	Tag
hsl				blank@blank.com	
backup				blank@blank.com	

> **NOTE:**
> You can delete the `tenants.csv` file from your system after uploading it to Backup Navigator.

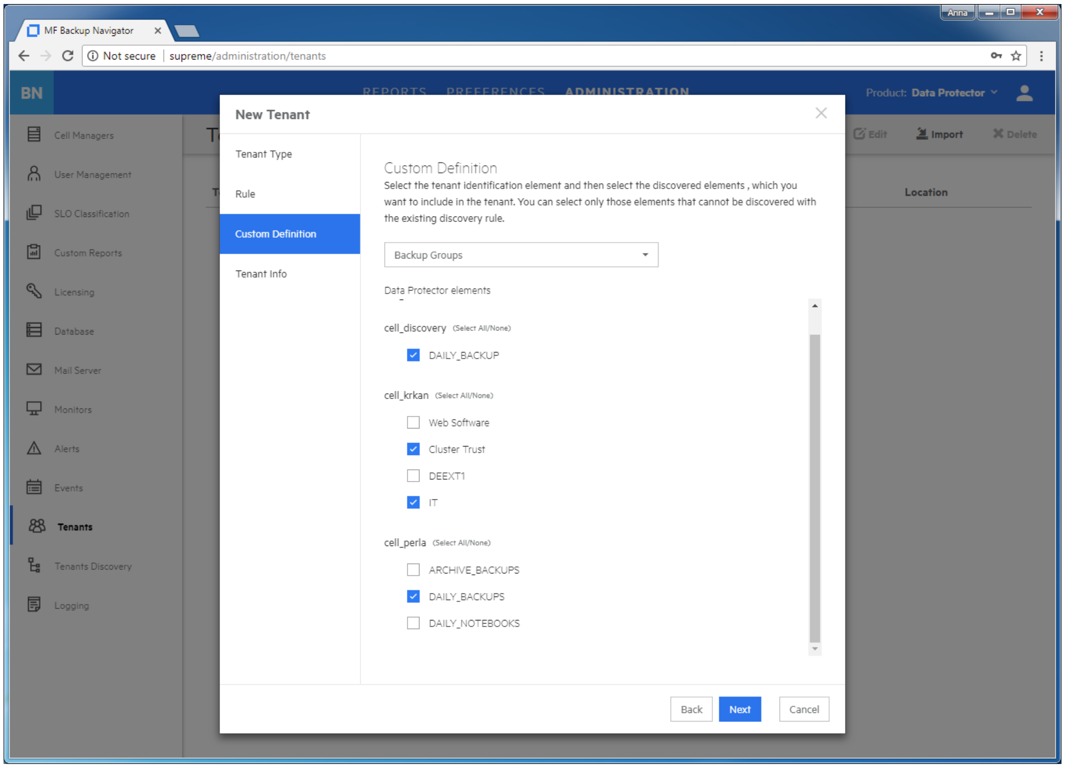
Creating tenants

You can add one or more tenants using the existing tenants discovery rule or your custom definition.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Tenants**.
3. In the Tool bar of the Results Area, click **New**.
4. In the New tenant wizard, select **New tenant**. Click **Next**.
5. In the Discovery rule page, select **Discovery rule** and the existing tenants discovery rule from the drop-down list, if you want to use the existing rule for creating a tenant. If you want to use your custom definition to create a new tenant, select **Custom definition**. Click **Next**.

Figure 22: Creating new tenants with custom definition



New Tenant

Tenant Type
Rule
Custom Definition
Tenant Info

Custom Definition

Select the tenant identification element and then select the discovered elements , which you want to include in the tenant. You can select only those elements that cannot be discovered with the existing discovery rule.

Backup Groups

Data Protector elements

cell_discovery (Select All/None)

☑ DAILY_BACKUP

cell_krkan (Select All/None)

☐ Web Software
☑ Cluster Trust
☐ DEEXT1
☑ IT

cell_perla (Select All/None)

☐ ARCHIVE_BACKUPS
☑ DAILY_BACKUPS
☐ DAILY_NOTEBOOKS

Back | Next | Cancel

6. If you select custom definition, the Custom Definition page displays.Select the Data Protector element identifying a new tenant, then select the discovered elements that you want to include in the tenant.

   > **NOTE:**
   > The list includes only those elements that cannot be discovered with the existing discovery rules.

   Click **Next**.

7. In the Tenant Info page, provide the tenant related information in the input text boxes. You can add a new tenant to an existing tenant group by selecting a tenant group name from the Tenant group drop-down list. Click **Finish**.

   The newly created tenant is added to the tenants list. It is also added to the Scope settings and is visible in the Navigation Pane. You can later add it to a tenant group, edit its properties, or delete it.

Creating tenant groups

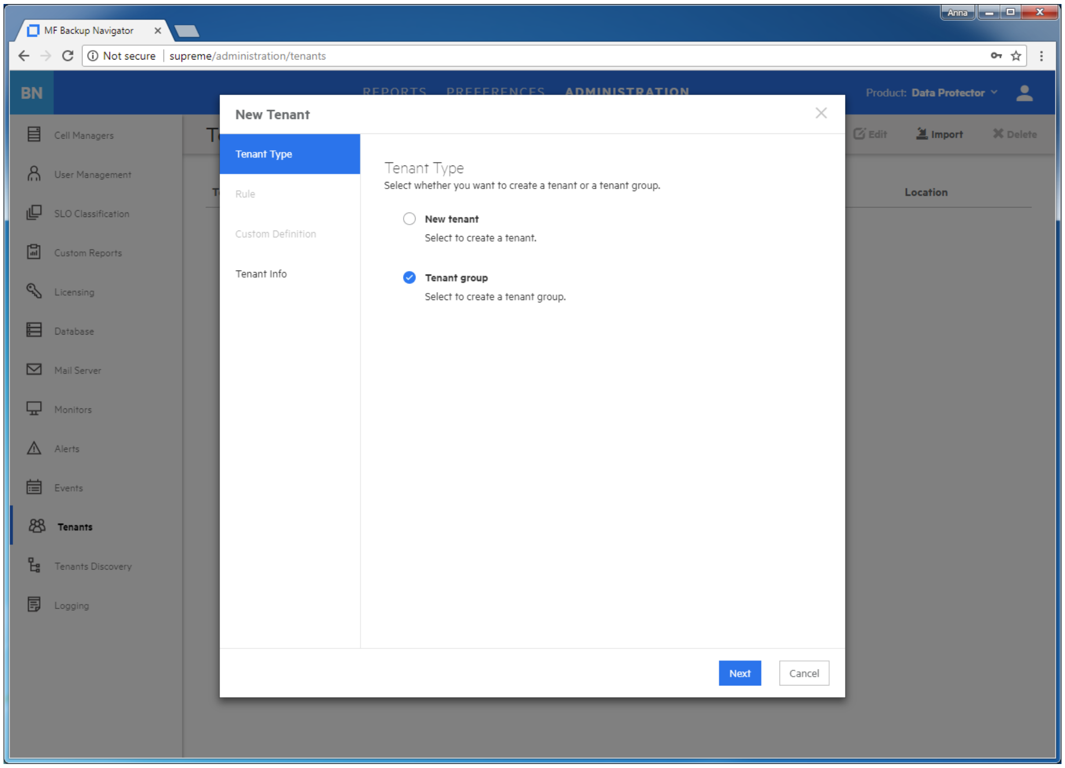
You can group multiple tenants that share some common characteristics (for example, location) by creating a tenant group.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Tenants**.

3. In the Tool bar of the Results Area, click **New**.
4. In the New tenant wizard, select **Tenant group**. Click **Next**.

Figure 23: Creating tenant group



New Tenant

Tenant Type

Select whether you want to create a tenant or a tenant group.

○ **New tenant**
Select to create a tenant.

● **Tenant group**
Select to create a tenant group.

5. In the Tenant Info page, provide the tenant group related information in the input text boxes. Select the tenants that will be the members of the group. Click **Finish**.

   The newly created tenant group is added to the tenants list. It is also added to the Scope settings and is visible in the Navigation Pane. You can later add it to a parent tenant group, add new tenants to it, edit its properties, or delete it.

Backup Navigator logging

Configure logging to analyze and troubleshoot the entire Backup Navigator operation and the reporting functionality.

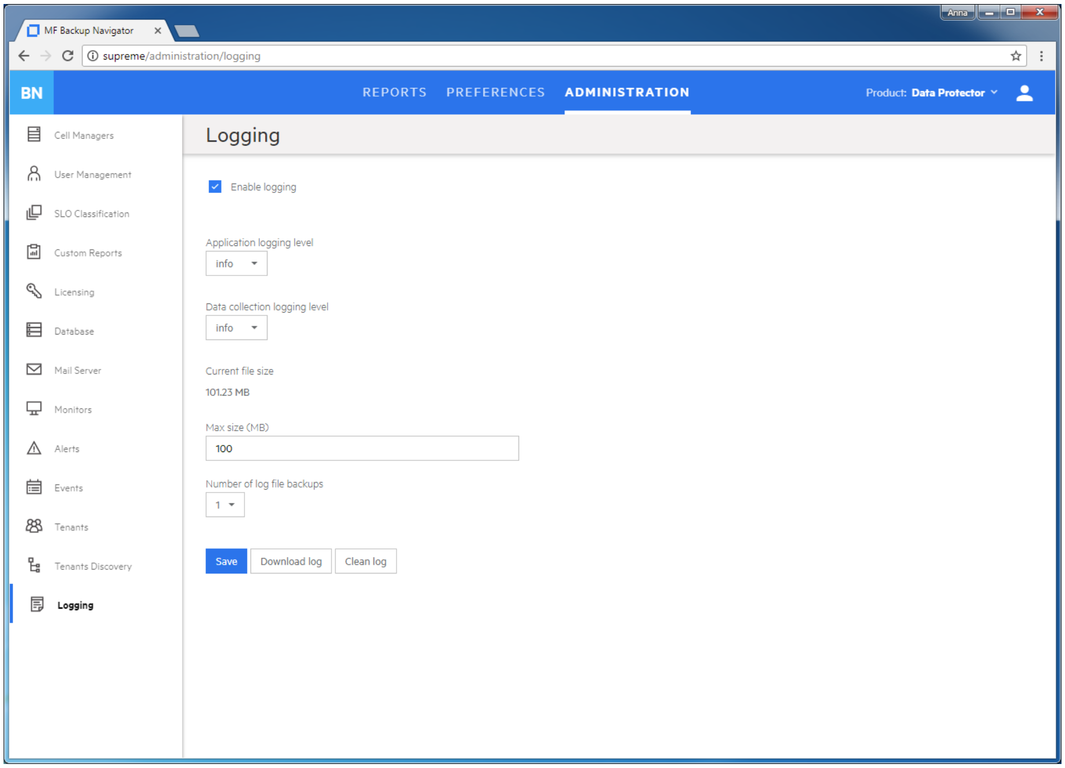
- To configure logging on the Backup Navigator system, see Configuring logging on Backup Navigator, on the next page.
- To configure logging on the Backup Navigator remote agent system, see Configuring logging on the remote agent, on the next page.

Configuring logging on Backup Navigator

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Logging**.
3. Select **Enable logging**.

   Figure 24: Logging settings

   Logging

   ☑ Enable logging

   Application logging level: info

   Data collection logging level: info

   Current file size: 101.23 MB

   Max size (MB): 100

   Number of log file backups: 1

4. Set logging levels for application related operations and data collection operations. Modify other fields according to your needs.
5. Click **Save**.
6. If you want to view the log file, click **Download log**. If you do not need data from the current log file, click **Clean log**.

You can always change these settings later.

Configuring logging on the remote agent

On the Backup Navigator remote agent, the logging is enabled automatically. By default, the logging level is set to `INFO`. The available logging levels are:

- `TRACE`
- `DEBUG`

- `INFO`
- `WARN`
- `ERROR`
- `FATAL`

You can change the default logging level.

Steps

1. Stop the Backup Navigator Remote Agent service.

   On Windows:

   In the Windows Task Manager->Services, locate and right-click **BNAgentService**, and then click **Stop**.

   On RedHat, CentOS, and SUSE 11.x: Run the following command:

   ```
   # service remote-agent stop
   ```

   On SUSE 12.x: Run the following command:

   ```
   # systemctl stop remote-agent
   ```

2. Change the `level` parameter in the `logger` tag to the desired level. The variables are located at:

   On Windows: *`<BN_installation_directory>`*\Backup Navigator `Remote Agent\logback.xml`

   On Linux: `/opt/remote-agent/logback.xml`

   > **Example of setting logging level to `ERROR`**
   >
   > For agent core: `<logger name="agent.core" additivity="true" level="ERROR">`
   > For agent util_cmd:`<logger name="agent.util_cmd" additivity="true" level="ERROR">`

3. Start the Backup Navigator Remote Agent service.

   On Windows:

   In the Windows Task Manager->Services, locate and right-click **BNAgentService**, and then click **Start**.

   On Linux: Run the following command:

   ```
   # service remote-agent start
   ```

Chapter 7: Administration Tasks for VM Explorer Environment

This chapter is intended for Backup Navigator administrators and refers to using Backup Navigator only with the VM Explorer environment. If you use Backup Navigator to collect data from the Data Protector environment, refer to the administration tasks described in Administration Tasks for Data Protector Environment, on page 38.

Before you can start using the Backup Navigator functionality, perform the following administration and configuration tasks in the web user interface:

- To start collecting input data from VM Explorer Servers, add these servers to the Backup Navigator list. For a detailed procedure, see Establishing data collection environment, below.
- After you select the VM Explorer Servers to collect data for your reports, you can update the cell settings and perform other related tasks. For more information, see Administering selected servers, on page 77.
- You can perform the following configuration tasks to better adjust Backup Navigator functionality to your environment's needs.
  - To create new users with different permissions as well as edit and delete the existing user accounts in Backup Navigator, see Managing users and user roles, on page 78.
  - See the recommendations on the database maintenance in Maintaining database, on page 80.
  - To be able to receive emails from the Backup Navigator, configure the mail server. See Configuring mail server, on page 82.
- You can monitor different aspects of the VM Explorer environment in the event log. To view the event log, see Viewing events, on page 83.
- To analyze and troubleshoot potential problems and provide an appropriate input to Micro Focus Support, see Backup Navigator logging, on page 84.

Establishing data collection environment

Select a new VM Explorer Server to collect the input data for your reports from it.

Prerequisites

- On VM Explorer, generate an API key (a string token). It is used to identify and authenticate Backup Navigator and to enable data collection data from VM Explorer environment. To do so, follow these steps:
  1. In the VM Explorer, navigate to the User Settings, select the **Reporting API** context, and then click **Request new API Key**.
  2. In the Request new API Key dialog, enter the description and then click **Generate new API Key**.
  3. Copy the generated API Key. Click **OK**.

  For the most recent instructions, see the *VM Explorer Reporting API* documentation.
- From each VM Explorer Server, export the security certificate and then import the exported certificates to the Backup Navigator. Perform the following steps:

1. On the VM Explorer system, open the VM Explorer-Starter (`VMXStarter.exe`), click **Web Settings**, and then click the **VP Explorer HTTPS Certificate** link.
   a. In the Certificate properties page, click the **Certification Path** tab to make sure, that the certificate status is OK.
   b. In the Certificate properties page, click the **Details** tab and then click **Copy to File...**
   c. Complete the Certificate Export wizard using the default settings to export the certificate to the `CER` file.
2. On the Backup Navigator system, import this security certificate to the Backup Navigator system by running the following command:

   ```
   # keytool -import -alias <alias_description> -keystore /opt/dpa-ext/conf/BNjavaKeyStore.jks -file <certificate_filename>
   ```

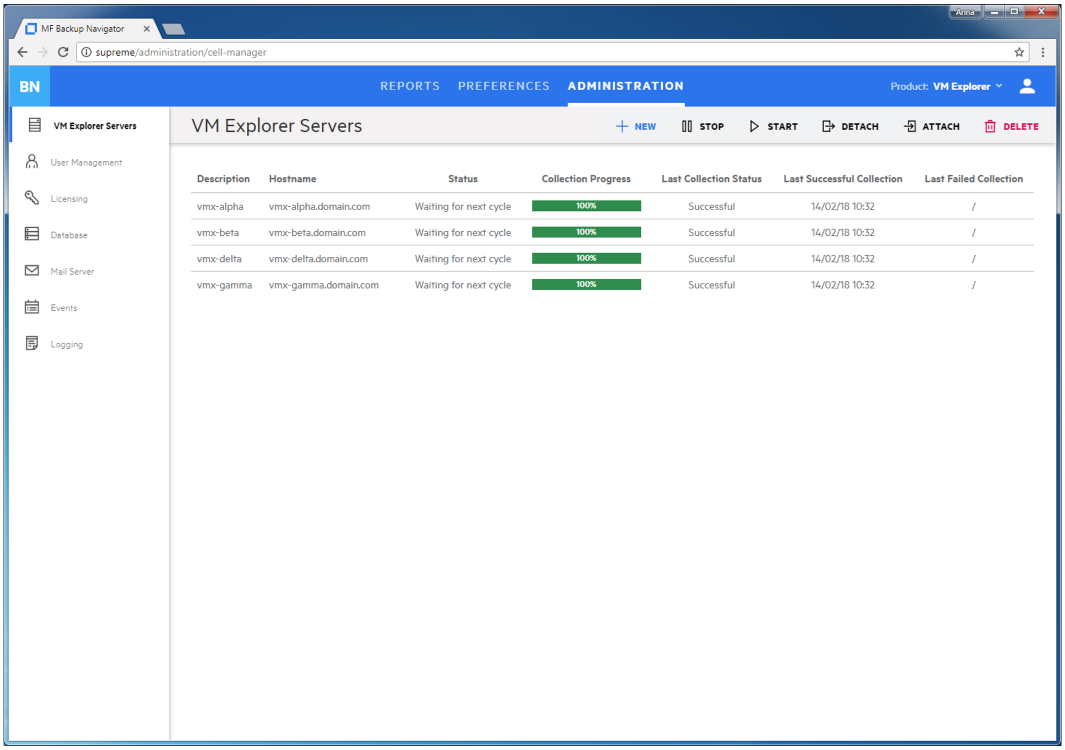
   When the `keytool` command requests a password, provide the one that is stored in `/opt/dpa-ext/conf/admin.properties`.

   ```
   # service tomcat restart
   ```

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **VM Explorer Servers**.

   Figure 25: Adding VM Explorer Servers

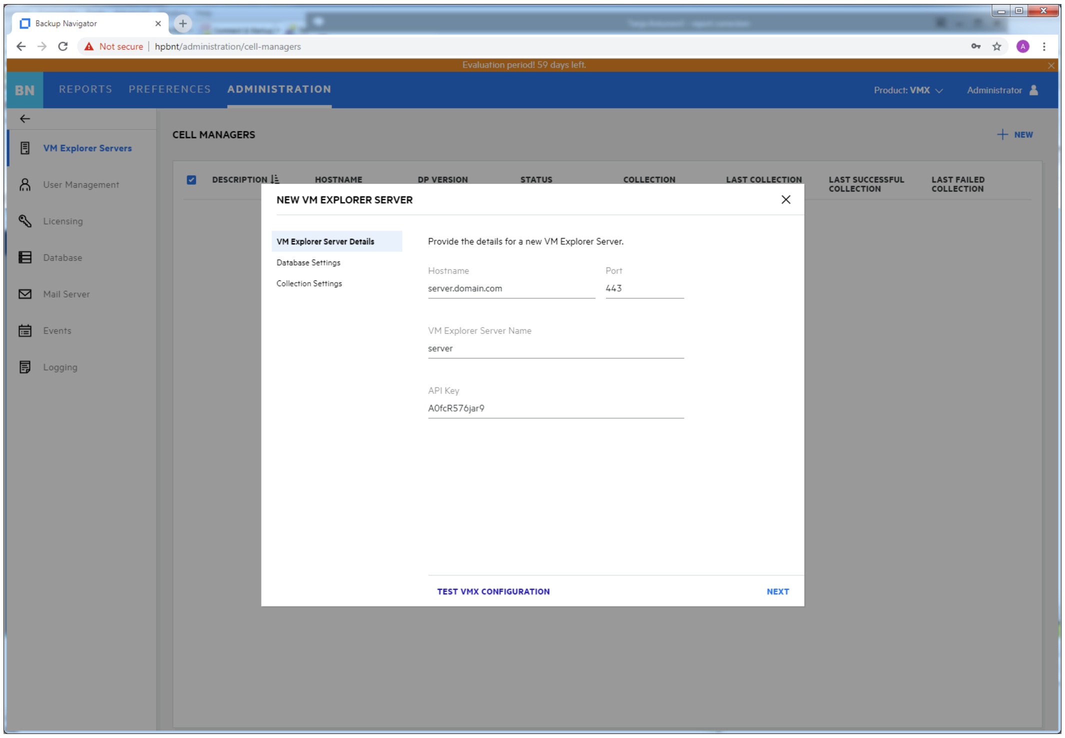


VM Explorer Servers

Description	Hostname	Status	Collection Progress	Last Collection Status	Last Successful Collection	Last Failed Collection
vmx-alpha	vmx-alpha.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-beta	vmx-beta.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-delta	vmx-delta.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-gamma	vmx-gamma.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/

3. In the Tool bar of the Results Area, click **New**. The New VM Explorer Server configuration window opens.

Figure 26: New VM Explorer Server Configuration window



Evaluation period! 59 days left.

Provide the details for a new VM Explorer Server.

Hostname: server.domain.com

Port: 443

VM Explorer Server Name: server

API Key: A0fcR576jar9

4. In the New VM Explorer Server window, enter the following data:
   - VM Explorer Server hostname or its IP address
   - INET port (by default, `443`)
   - VM Explorer Server name - the name of your choice, which will be used in Backup Navigator to identify the server
   - API key that you generated in the VM Explorer Server

   Configure the database of the new cell by specifying the following:
   - the hostname of the system where the database resides (by default, the system where you installed Backup Navigator)
   - the port of the system where the database resides (by default, `5432`)
   - the user name and the password of the PostgreSQL admin user with the `SUPERUSER` permissions.
   - the database name of your choice

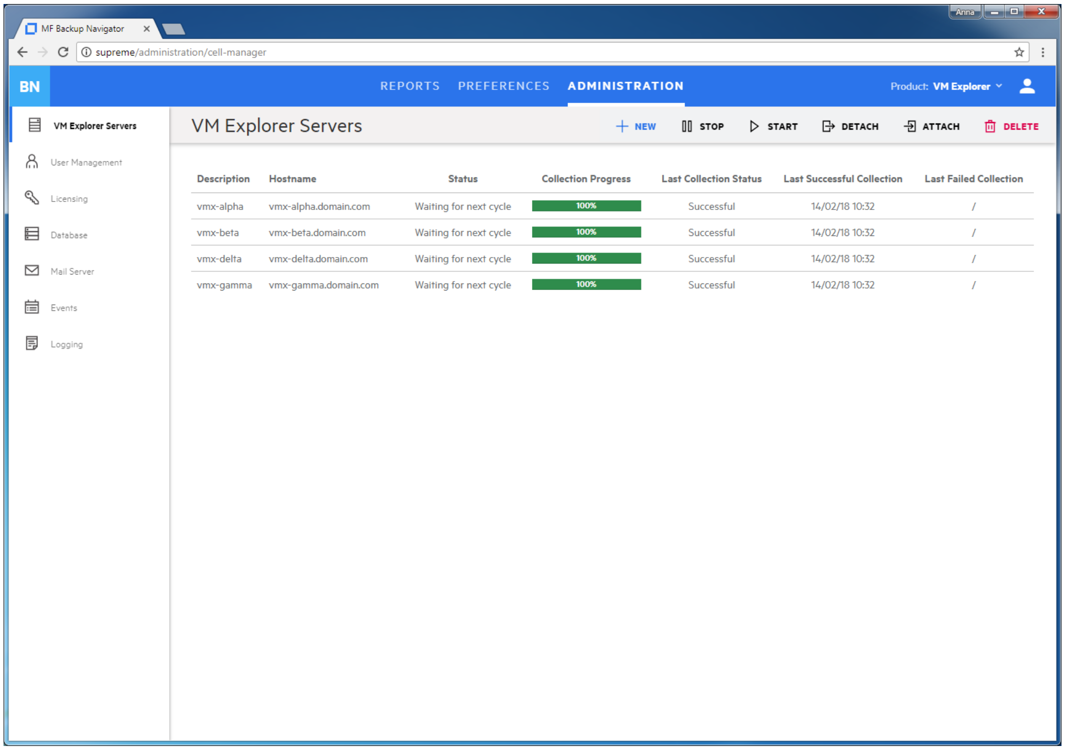
     The maximum number of characters for the database name is 25. The default name is `cell_`*`<description>`*, which you can change to another one.
   - the period for which you want to collect data for your reports (you can select the custom starting date or all existing data)
   - the time interval in which you want to collect the changed input data for your reports (for example, every 10 minutes)
5. Click **Test Configuration** to verify that the VM Explorer Server is configured appropriately.
6. Click **Save**. A new cell is added to Scope and is visible in the Navigation Pane.

You can always update your settings later.

Administering selected servers

After you selected the VM Explorer Servers to collect data for your reports, they are listed in the VM Explorer Server window of the Administration context.

Figure 27: Administering cells



VM Explorer Servers

Description	Hostname	Status	Collection Progress	Last Collection Status	Last Successful Collection	Last Failed Collection
vmx-alpha	vmx-alpha.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-beta	vmx-beta.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-delta	vmx-delta.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/
vmx-gamma	vmx-gamma.domain.com	Waiting for next cycle	100%	Successful	14/02/18 10:32	/

You can change the VM Explorer Server's settings or status by clicking on it and selecting one of the following actions:

- **Edit**: Change the VM Explorer Server and database settings.

  > **IMPORTANT:** If you moved the database to a new server or performed any other database configuration changes that affect the Backup Navigator functionality, make the necessary database setting updates on every related Cell Manager.

- **Stop/Start**: Pause data collection from the selected cell by stopping it, when you temporarily do not need to include its data to your reports. When stopped, the cell is still present in the scope and to the reports. Start data collection from the selected cell, when you need this data for your reports.
- **Download**: Download package for the Backup Navigator remote agent installation. Applicable for the remote Cell Managers.
- **Detach/Attach**: Pause data collection from the selected cell by detaching it, when you want to have access to the collected data in the database, but do not need to include this data in your reports. When detached, the cell is not visible in the scope and in the reports. Attach the selected cell and then start data collection from it, when you need its data for your reports.
- **Delete**: Delete the selected cell from the Backup Navigator list. The database of this cell with all

previously collected data is deleted. You can always add this cell to the list later. Note, that a filter that contains only this cell, will be also deleted.

Managing users and user roles

Depending on their role, users have different permissions. Backup Navigator supports the following user roles:

- **Built-in Administrator**

  This user role is created during installation. There is only one Built-in Administrator in the Backup Navigator environment and it cannot be deleted or changed. The Built-in Administrator has permissions to generate reports on all VM Explorer Servers and to perform administration tasks in Backup Navigator.

- **Administrator**

  The Administrator has permissions to generate reports on all VM Explorer Server and to perform administration tasks in Backup Navigator. Administrator accounts can be created, edited, and deleted by the Built-in Administrator or Administrator.

- **Standard User**

  An Administrator can create, edit, and delete the Standard User account and grant it permissions for all or selected VM Explorer Servers. The Standard User can change the profile, manage subscriptions and filters, and generate reports on the VM Explorer Servers, for which the permissions were granted by the Administrator.

If you configured LDAP authentication (see Configuring SSL for LDAP authentication, on page 22), you can specify users that can be authenticated with the LDAP server. Before you can add LDAP users, you need to specify an LDAP server that will be used by Backup Navigator. For detailed procedure, see Adding LDAP Server, below.

To create a new user, see Creating new users, on the next page.

Adding LDAP Server

Add LDAP server, if you want to create users with LDAP authentication.

Prerequisite

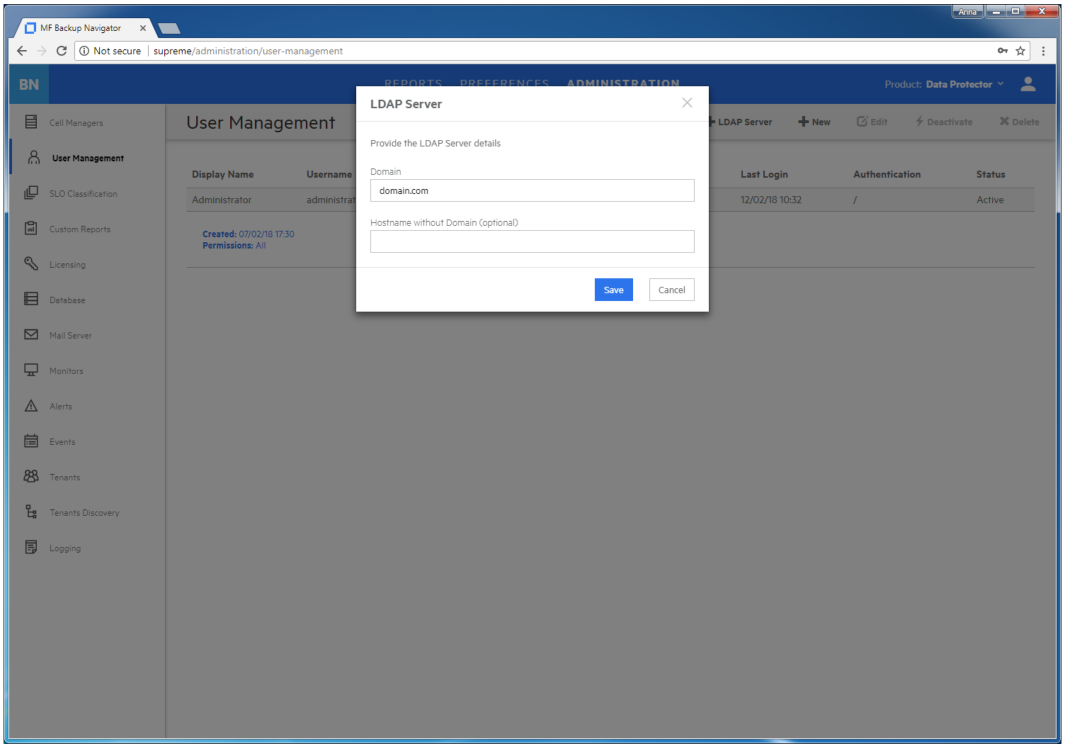
LDAP authentication is configured on the Backup Navigator server.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **User Management**.
3. In the Tool bar of the Results Area, click **LDAP Server**.
4. In the LDAP Server properties window, specify the domain name that should be recognized by the LDAP server.

   You can also specify the hostname, if you want that the LDAP server recognizes the specific host.

Figure 28: Specifying LDAP server



Display Name	Username	Last Login	Authentication	Status
Administrator	administrat	12/02/18 10:32	/	Active

Created: 07/02/18 17:30
Permissions: All

LDAP Server

Provide the LDAP Server details

Domain: domain.com

Hostname without Domain (optional):

Click **Save**.

The LDAP server is added successfully.

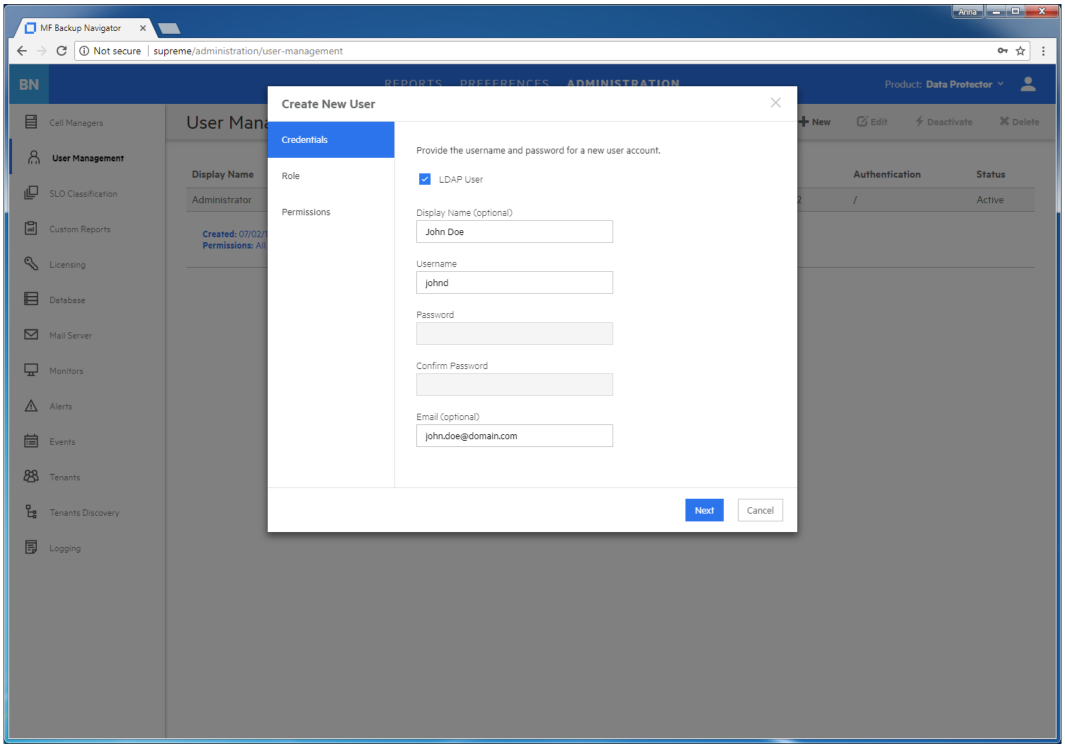
Creating new users

Create new users with the specific user roles.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **User Management**.
3. In the Tool bar of the Results Area, click **New**. The Create New User wizard displays.
4. If you added an LDAP server, select the **LDAP User** option. Enter the user display name, username, and password (for the LDAP user, the password from the LDAP server is used) of the user that you add to Backup Navigator and, optionally, the email. Click **Next**.

Figure 29: Creating a new user



Create New User

Provide the username and password for a new user account.

☑ LDAP User

Display Name (optional): John Doe

Username: johnd

Password:

Confirm Password:

Email (optional): john.doe@domain.com

5. Select **Administrator** or **Standard User** as a user role for this user account.

   If you selected `Administrator`, click **Finish**. If you selected `Standard User`, click **Next**.

6. For the Standard User, select the VM Explorer Servers the user can access to generate reports. Click **Finish**.

A new user account is added to the User Management table. You can later edit, deactivate or delete it.

> **IMPORTANT:** You cannot perform any actions on the account with which you are currently logged in to Backup Navigator.

Maintaining database

Ensure regular backups, archiving, and clean-up of the Backup Navigator database. Be prepared for a potential recovery. For the related procedures, see the PostgreSQL documentation.

You can use pgAdmin GUI to administer PostgreSQL. You can download this tool from: http://www.pgadmin.org/download/

To view the database settings in the web user interface, see Viewing database settings, on the next page.

You can perform the following database maintenance tasks in Backup Navigator:

- Purging the database. See Purging database, on the next page.
- Performance tuning. See Tuning database performance, on page 82.

Viewing database settings

You can view the database settings information.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Database**. The database settings information is displayed. To change these settings perform the procedure described in Maintaining database, on the previous page.

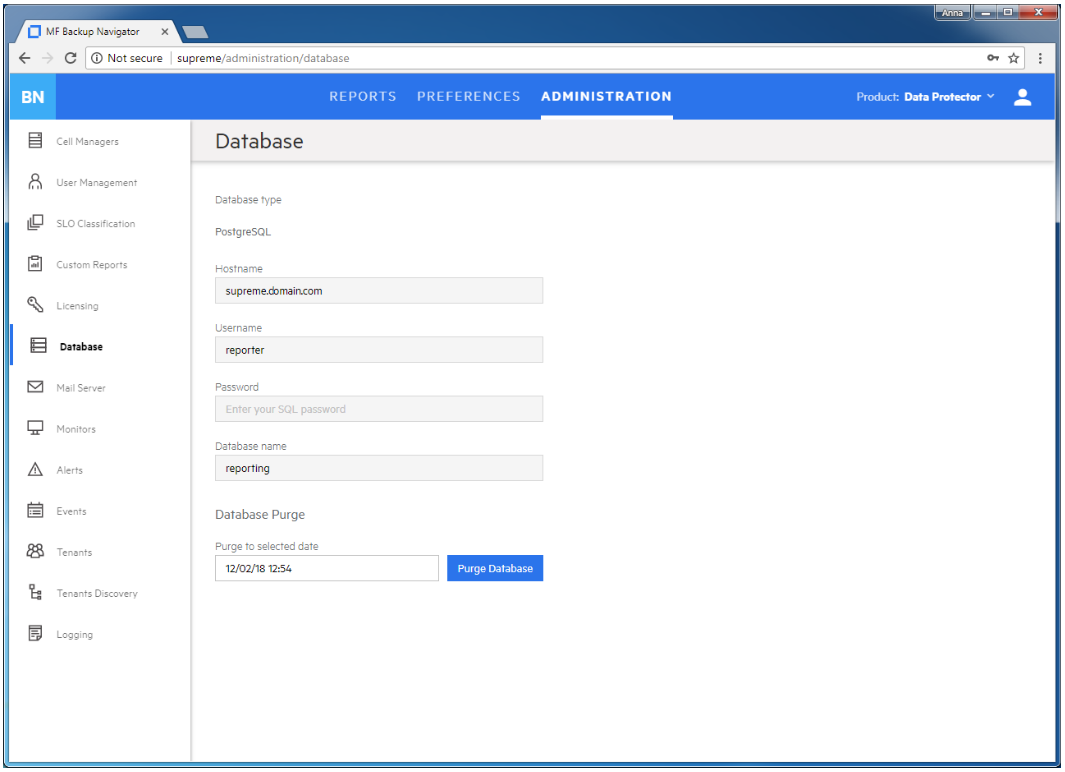
Purging database

You can use the Backup Navigator web user interface to clean up the database.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Database**. The database settings information is displayed. Under Database Purge, specify the date, up to which you want to purge the Backup Navigator database and then click **Purge Database**.

   Figure 30: Database settings



Database

Database type

PostgreSQL

Hostname

supreme.domain.com

Username

reporter

Password

Enter your SQL password

Database name

reporting

Database Purge

Purge to selected date

12/02/18 12:54

Purge Database

3. In the Purge Database window, select to purge all cells or specify the cells you want to purge.

Click **Purge** and then click **Confirm**.

During the database cleanup, the data older than the specified date is deleted.

Tuning database performance

When you install and configure Backup Navigator, PostgreSQL database server is also configured. The provided default settings related to the database performance correspond to the minimum system requirements and are as follows:

```
shared_buffers = 1000MB
effective_cache_size = 2000MB
work_mem = 64MB
maintenance_work_mem = 256MB
```

If the memory resources of your Backup Navigator allow, you can allocate more memory resources to improve performance. If you consider that the Backup Navigator performance is not sufficient, you can change the performance related settings to tune the performance to the needs of your specific environment. For the description of these settings and detailed procedures, see the PostgreSQL documentation.

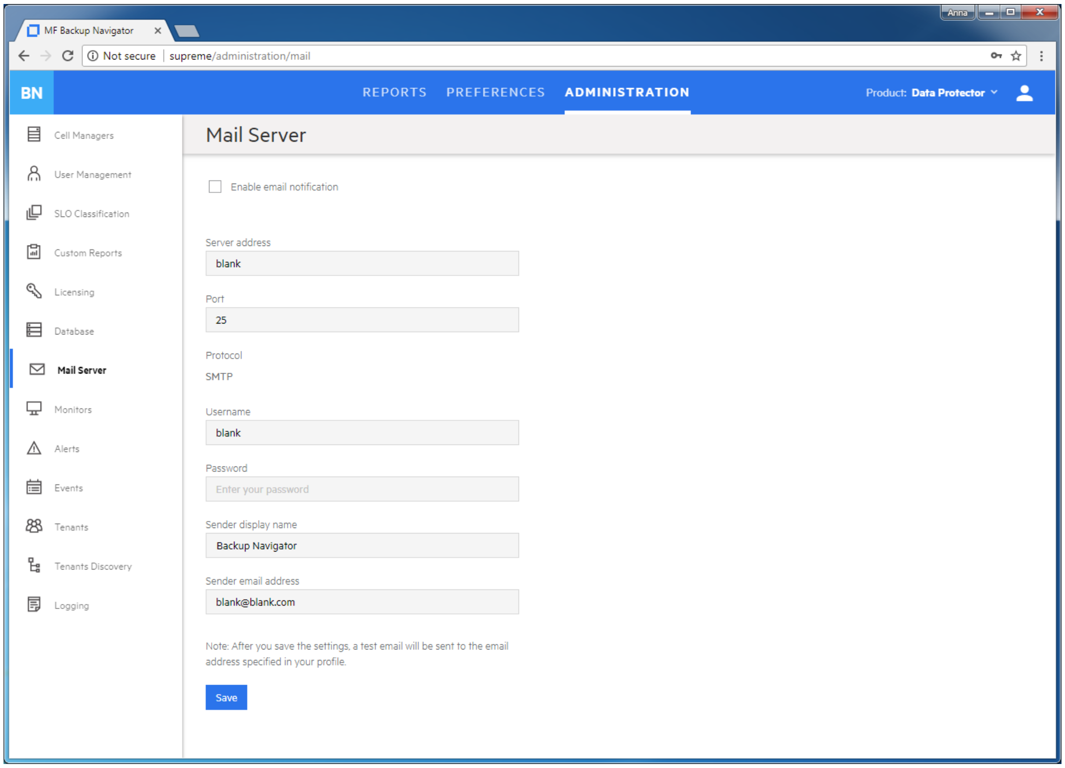
Configuring mail server

Configure your mail server to be able to receive emails.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Mail Server**.

Figure 31: Configuring Mail Server



Mail Server

□ Enable email notification

Server address: blank

Port: 25

Protocol: SMTP

Username: blank

Password: Enter your password

Sender display name: Backup Navigator

Sender email address: blank@blank.com

Note: After you save the settings, a test email will be sent to the email address specified in your profile.

3. In the Results Area, select **Enable email notification**.
4. Enter the web address of the server, which you want to use for sending emails.
5. Enter the server port, username, and password.
6. Enter the sender's display name and email address (mandatory).
7. Click **Save**. A test email is sent to the specified email address.

You can always change these settings later.

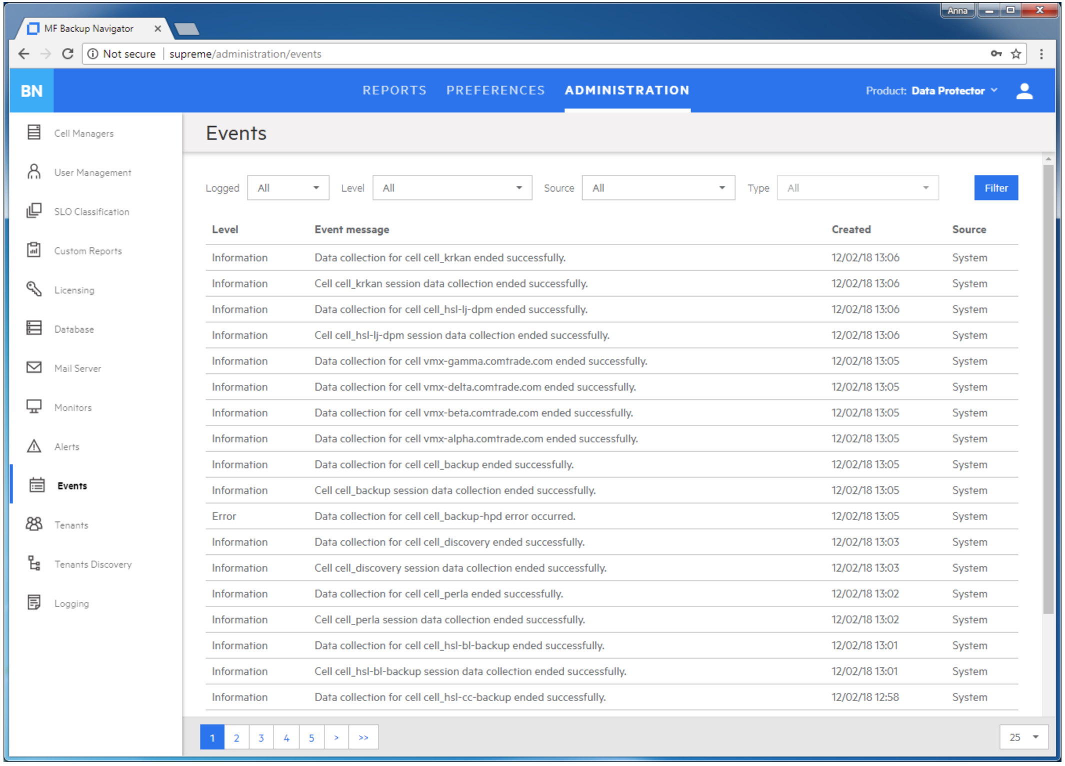
Viewing events

You can view the events occurred in Backup Navigator. An event is logged, when the conditions specified in the monitors are met.

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Events**. A table with the Backup Navigator events displays. You can filter and sort table by name, severity level, and timeframe. To apply the specified filter, click **Filter**.
3. To view the specific event details, double-click it.

Figure 32: Events list



Events

Logged: All Level: All Source: All Type: All

Level	Event message	Created	Source
Information	Data collection for cell cell_krkan ended successfully.	12/02/18 13:06	System
Information	Cell cell_krkan session data collection ended successfully.	12/02/18 13:06	System
Information	Data collection for cell cell_hsl-lj-dpm ended successfully.	12/02/18 13:06	System
Information	Cell cell_hsl-lj-dpm session data collection ended successfully.	12/02/18 13:06	System
Information	Data collection for cell vmx-gamma.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-delta.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-beta.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell vmx-alpha.comtrade.com ended successfully.	12/02/18 13:05	System
Information	Data collection for cell cell_backup ended successfully.	12/02/18 13:05	System
Information	Cell cell_backup session data collection ended successfully.	12/02/18 13:05	System
Error	Data collection for cell cell_backup-hpd error occurred.	12/02/18 13:05	System
Information	Data collection for cell cell_discovery ended successfully.	12/02/18 13:03	System
Information	Cell cell_discovery session data collection ended successfully.	12/02/18 13:03	System
Information	Data collection for cell cell_perla ended successfully.	12/02/18 13:02	System
Information	Cell cell_perla session data collection ended successfully.	12/02/18 13:02	System
Information	Data collection for cell cell_hsl-bl-backup ended successfully.	12/02/18 13:01	System
Information	Cell cell_hsl-bl-backup session data collection ended successfully.	12/02/18 13:01	System
Information	Data collection for cell cell_hsl-cc-backup ended successfully.	12/02/18 12:58	System

Backup Navigator logging

Configure logging to analyze and troubleshoot the entire Backup Navigator operation and the reporting functionality.

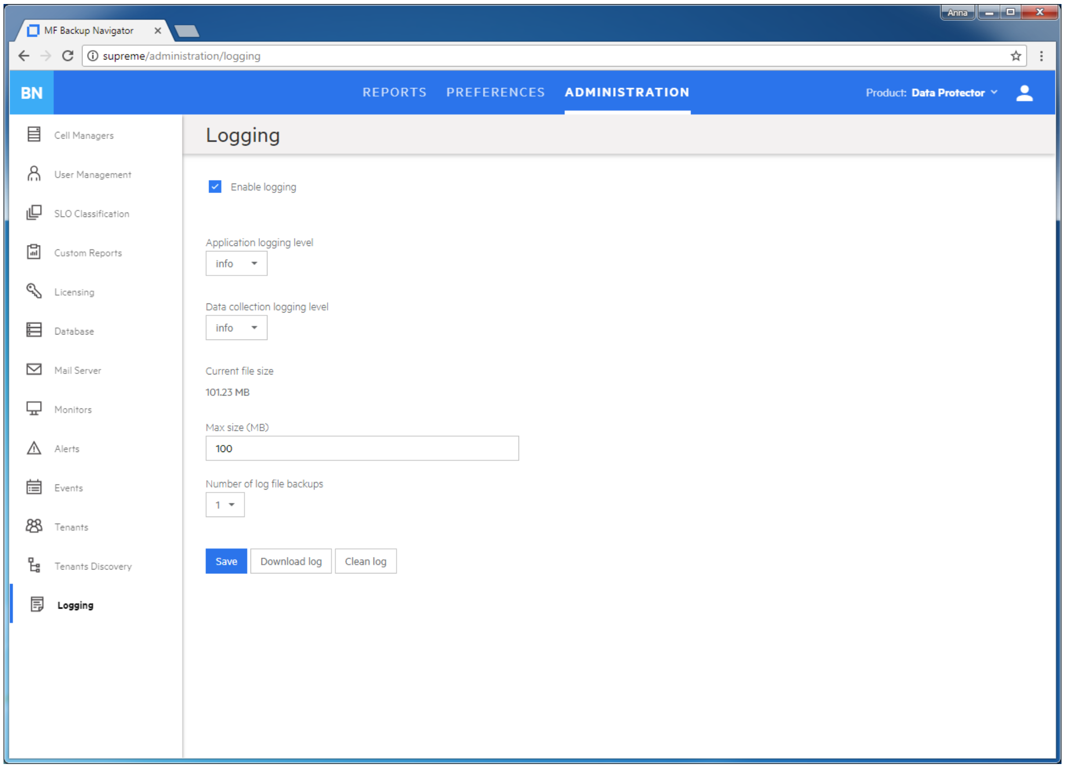
- To configure logging on the Backup Navigator system, see Configuring logging on Backup Navigator, below.
- To configure logging on the Backup Navigator remote agent system, see Administration Tasks for VM Explorer Environment, on page 74.

Configuring logging on Backup Navigator

Steps

1. Select the **Administration** context.
2. In the Navigation Pane, click **Logging**.
3. Select **Enable logging**.

Figure 33: Logging settings



Logging

☑ Enable logging

Application logging level: info

Data collection logging level: info

Current file size: 101.23 MB

Max size (MB): 100

Number of log file backups: 1

4. Set logging levels for application related operations and data collection operations. Modify other fields according to your needs.
5. Click **Save**.
6. If you want to view the log file, click **Download log**. If you do not need data from the current log file, click **Clean log**.

You can always change these settings later.

Chapter 8: About Reports

The key Backup Navigator feature is a visual presentation of complex data. To achieve a comprehensive and precise input data presentation and visualization, and to deliver the desired information clearly and effectively, Backup Navigator provides a set of predefined reports and tools that help to tailor the reports to meet your needs.

Report visualization and delivery

All reports can be viewed in a dashboard area of the Backup Navigator user interface. Reports can be presented as a table with access to all input data or as a chart to visualize this data. The following report chart types are used to visualize the selected reports: column chart, bar chart, pie chart, line chart, or area chart.

Besides viewing reports in the web browser, Backup Navigator enables you to subscribe to reports to receive them automatically by email at a specified time, as well as to export them to a wide variety of formats, including PDF, XLSX, CSV, DOCX, PPTX, and HTML. You can choose the format that provides you with the most convenient way of exploring reports.

Report exploration

To easily gain insight into the data used for a specific report, and to enhance reporting and analysis capabilities, the following is available:

Table view: You have an option to view all the data used for generating a report as a table. In the table, you can sort values in the columns according to the available parameters.

Related reports: A majority of the reports contain references to other reports with related content. A related report is a logical report in the sequence and is presented on the same scope as the original report.

Drill-down functionality: You can examine report data in more detail by using the drill-down functionality. Navigate from the report of your interest to the connected reports, each time with deeper insight into the data, and discover the data you need.

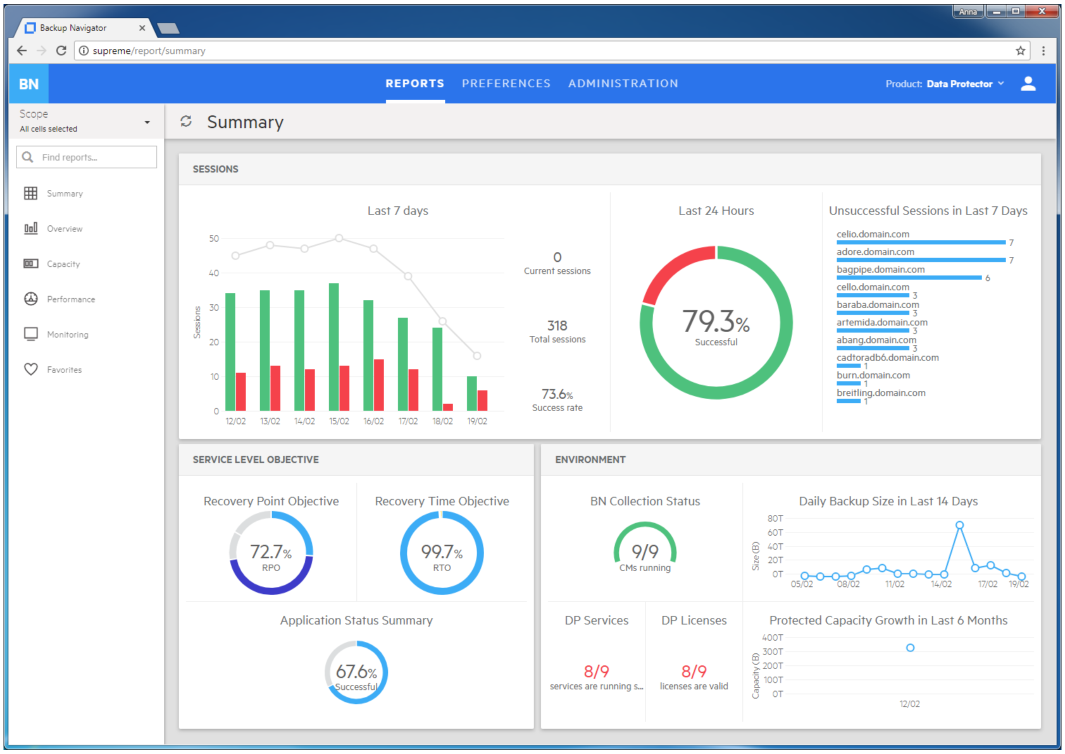
Scope: To ensure that your reports contain only the data that you currently require for your specific purposes, you can limit the scope of your reports only to certain VM Explorer Servers or to the Data Protector cells, tenants, or to certain groups of the IDB data (for example, devices, device pools, media, media pools, clients).

Summary dashboard

The Backup Navigator Summary dashboard provides you with an at-a-glance overview of your Data Protector backup environment. This intuitive dashboard enables you to monitor different activities and to quickly identify areas that need your attention.

You access the Summary dashboard the first time you log in to Backup Navigator and you can later view it from the **Reports** context by clicking **Summary** in the Navigation Pane.

Figure 34: Summary dashboard



You can view the following information in the Summary dashboard widgets:

Widget	Description
Sessions	Shows information on the successful (completed without errors) and unsuccessful sessions: • The session report for the last 7 days shows the total number of sessions and the success rate, and the number of successful and unsuccessful sessions per day. • The success rate report for the last 24 hours shows the percentage of successful and unsuccessful sessions. • The report on unsuccessful sessions in the last 7 days shows the top ten clients with the highest number of unsuccessful sessions.
Service Level Objective	Shows information related to the Service level objectives (SLO): • The Recovery point objective (RPO) report shows the percentage of backup applications that are compliant with the RPO specified in the respective SLO category. It also features the percentage of backup applications that breached the specified RPO, that are backed up too frequent for the specified RPO, and of those without an assigned SLO category. • The Recovery time objective (RTO) report shows the percentage of backup applications that are compliant with the RTO specified in the respective SLO category. It also features the percentage of backup

Widget	Description
	applications that breached the specified RTO and of those without an assigned SLO category. • The Application Status Summary report shows the percentage of the latest successful (completed) and unsuccessful sessions of the backup applications.
Environment	Shows information on different aspects of the Data Protector cells: • The Data Protector Cell Manager related reports show the data collection status, Cell Manager services status and license related information. • The backup size related report shows transfer size of the data that was backed up from or restored to a particular source (cell, tenant, client, or application) within the last 14 days. • The protected capacity related report shows changes in the amount of space on the media that are protected from being overwritten in the last 6 months.

You can use this dashboard as a starting point for your everyday tasks because it enables you to easily access the area of interest. By clicking the corresponding item on a widget, you generate a detailed drill-down report.

Reports and report categories

The predefined set of reports covers all aspects of the backup application functionality (Data Protector and VM Explorer Server). Reports are logically divided into four main categories, each containing subcategories.

> **NOTE:** The report categories and subcategories may differ for different backup applications.

Depending on the information about your backup environment that you want to retrieve, you can choose a report from the following report categories:

- Overview, on the next page.
- Monitoring, on page 96.
- Capacity, on page 96.
- Performance, on page 100.

Each report can be adjusted to your needs by specifying additional parameters, which are specific for each report, such as a time interval, sorting order, units, and similar. You can set a report as your favorite to access it quicker later on and to be able to subscribe to it. Administrators can create custom reports that are based on the collected data. If you set filters for the input data, only the data from the selected cells and specified data groups is considered.

Some reports cannot be accessed from the Navigation Pane, they are dependent on other reports and can be accessed only when using the drill-down functionality:

Drill-down reports, on page 101.

Overview

Overview reports summarize data on your backup environment.

Infrastructure Summary	
Data Protector environment	
Cell Manager Status	Shows health statuses that can be retrieved from a Cell Manager for the following objects: Cell Manager services, IDB health status, licenses (whether Data Protector licenses are available on the Cell Manager), agent status (whether data can be collected from the Cell Manager), Cell Manager mode (mode `GREEN`, when data collection from the Cell Manager is active; mode `GREY`, when data collection from the Cell Manager stopped.)
Agent Status	Shows health status for collecting data from the Cell Manager (agent status). If the agent is running, the status is marked `GREEN`, in case of failure it is marked `RED`. The report also shows Last Collection Status (Successful or Failed), Last Successful Status (Time of the last successful Collection), Last Failed Collection (Time of the last failed Collection), Cell Manager Fetch Date (Initial Collection Date) and the Cell Manager Data Protector properties, such as hostname, virtual name, version, capacity, and other.
Operating Systems Overview	Shows which operating systems exist and the number of clients running on these operating systems.
DP Components	Shows a list and a number of the installed Data Protector components.
List of Backup Specs	Shows all backup specifications and their properties, such as application type, session type, time of the last modification and execution, last finished session status, as well as client , instance and retention information. For the Data Protector 10.xx cells with the enabled `Data Protector version is 10.xx` option and specified Web User credentials, the `Resume` action is available for all failed sessions, while the `Restart` action is available for all failed filesystem and Oracle Server integration sessions. For instructions on how to enable the `Data Protector version is 10.xx` option, see Establishing data collection environment, on page 39.
Backup Spec Overview	Shows a number of the backup specifications of a particular application type (Filesystem, IDB, client backup, and so on).

Clients Without Backup Spec	Shows a number of clients for which no backup specification is created and consequently they are not being backed up.
VM Explorer environment	
VM Explorer Server Status	Shows health statuses that can be retrieved from a VM Explorer Server for the following objects: licenses (whether VM Explorer licenses are available on the VM Explorer Server), agent status (whether data can be collected from the VM Explorer Server).
Agent Status	Shows VM Explorer version and status as well as health status for collecting data from the VM Explorer Server.

Sessions/Tasks Summary	
Data Protector environment	
List of Sessions	Shows all finished sessions, their status and properties, such as application type, session type, backup type, backup method, session start and duration, client and instance related information. The report also provides detailed error descriptions and troubleshooting information on unsuccessfully completed sessions.
List of Objects	Shows all backed up objects and their properties including deduplication ratio, list of their copies, and object's retention.
Sessions per Session Status	Shows a number of the performed sessions and their statuses.
Sessions per Time and Status	Shows a number of sessions performed on a particular day and their statuses.
Sessions per Session Type	Shows a number of the performed sessions and the session type, such as, backup, consolidation, copy, media management, replication, and restore.
Sessions per Backup Object	Shows a number of sessions and their statuses for all backup application types (for example, Filesystem, IDB, Oracle, MS SQL, and so on).
Sessions per Client	Shows a number of sessions performed on a particular client and their statuses.
Session Flow per Client	Shows the backup sessions duration for all clients and their status.
Session Flow per Backup Spec	Shows the backup sessions duration and statuses for all backup specifications.
Sessions per Data Location	Shows the backup sessions for the selected data source

Sessions/Tasks Summary	
	(Backup specification, Hostname, Session ID) and the selected data location (Device, Media, Media Location, Media Pool).
VM Explorer environment	
List of Tasks	Shows all tasks, their status and properties, such as name, ID, start, duration, and related errors or warnings.
List of Task Elements	Shows task elements and their properties, such as type, size, status, virtual environment specifics.
Tasks per Task Status	Shows a number of the performed tasks and their statuses.
Tasks per Time and Status	Shows a number of sessions performed on a particular day and their statuses.
Tasks per Backup Type	Shows a number of tasks and their statuses for all backup types (for example, normal full, full incremental; delta incremental).
Tasks per Datacenter	Shows a number of tasks performed on a particular datacenter and their statuses.

Service Level Objective	
Data Protector environment	
Application Overview	Shows applications running on a particular instance and client. For each application, the compliance with the identified SLO category[1] is checked and is reflected in the status of the corresponding recovery point (RP)[2] and recovery time (RT)[3] status: • `GREEN`: RP and RT are compliant with the corresponding SLO category • `BLUE`: RP and RT are compliant with the corresponding SLO category, but the backups are too frequent • `RED`: RP and RT are breached

[1] Service level objective (SLO) category refers to a combination of the RTO (a time period needed before an application is brought back online) and the RPO (a time period when data can be lost after an event that causes an application to go offline occurs), which are specific for your backup environment goals.

[2] Recovery point (RP) refers to the amount of time between the last and the previous successful backups of the same application.

[3] Recovery time (RT) refers to the estimated time needed for the application recovery of the last successful backup chain.

Service Level Objective	
	The report includes application type (Filesystem, Oracle, Exchange, VEAgent, and so on), RP, maximum RP[1], RT, maximum RT[2], and the SLO category. Application type Unknown refers to the clients that are not protected with Data Protector backup. As Administrator, you can assign and change the SLO categories within this report, see Administration Tasks for Data Protector Environment, on page 38.
Application Status	Shows the last backup session status of the applications running on a particular instance and client including information on the last successful and last failed session, and protection related information.
Application Status Summary	Shows the percentage of the last successful (completed) and unsuccessful (failed or aborted) backup sessions of the applications running on a particular instance and client.
VM Explorer environment	
VM Status	Shows session status of virtual machines.
VM Status Summary	Shows the percentage of virtual machines tasks divided by status: `Success` (completed), `Running` (running and in a queue), `Failed` (failed and aborted), and `Warning` (with warning s and errors).

Data Protection Summary (Data Protector specific)	
Session Success	Shows the percentage of successful (completed without errors) and unsuccessful backup sessions.
Number of Backup Versions	Shows a number of performed backups of a particular backup type (Full, Incremental, Differential, and Transaction Log backup) for all backup specifications.
Time Since Last Successful Backup	Shows the time passed since the last successful backup for all backup specifications.

[1] MAX RP refers to the maximum amount of time between two successful backups of the same application that is still protected.
[2] MAX RT refers to the maximum estimated time needed for recovery of the same application that is still protected.

Devices Summary (Data Protector specific)	
List of Devices	Shows all libraries and devices that are configured for use with Data Protector. For each library, the report shows location, list of drives, device type, system the drive is connected to, and its media pool. For StoreOnce devices it also shows the Store name. The report includes information on libraries that are configured to be used with Data Protector, but are not used so far (Library Utilization - Not Utilized). The report can be generated for libraries and identified device types.
Device Utilization	Shows the percentage of the device utilization for all devices and average utilization for all devices per device library. You can filter the top most utilized or least utilized devices.
Session Flow per Device	Shows the backup sessions duration for all devices (libraries and drives).

Target Locations Summary (VM Explorer specific)	
List of Target Locations	Shows a list target locations with their properties in a tabular view.

Media Summary (Data Protector specific)	
Media Summary per Pool	Shows a number of media and their quality (Good, Fair, and Poor) in all media pools.
Media Quality Summary	Shows a number of errors and overwrites on all media.

Backup Time Summary (Data Protector specific)	
Backup Schedule Drive Detail	Shows the backup schedule for drives specified for the scheduled backup sessions and the related backup specifications. If a conflict in the drive usage is recognized (the same drive is specified for the simultaneous backup sessions), an additional bar shows such conflict.
Backup Schedule Overview	Shows the backup schedule for the configured backup specifications and the eventual conflicting backup sessions.
Average Backup Time per Backup Spec	Shows an average duration of the backup session for a particular backup specification.
Average Backup Time per Client	Shows an average duration of the backup session on a

Backup Time Summary (Data Protector specific)	
	particular client.
Top Time Difference per Backup Spec	Shows the biggest time difference that occurs when running backups using the same backup specification.
Average Backup Time per VM	Shows an average duration of the backup session on a particular virtual machine. It can help you to figure out, on which virtual machines a backup takes more time.

Errors Summary	
Data Protector environment	
Most Frequent Errors	Shows a number of occurrences of the specific minor, major and critical error messages during the backup sessions.
Most Unreliable Clients	Shows a number of errors and warnings that occurred on a particular client. Most unreliable clients are those with the highest number of errors.
Most Unreliable Devices	Shows a number of errors and warnings that occurred on a particular device. Most unreliable devices are those with the highest number of errors.
Most Unreliable Backup Specs	Shows a number of errors and warnings that occurred for a particular backup specification. Most unreliable backup specifications are those with the highest number of errors.
Most Unreliable Media	Shows a number of errors that occurred on a particular medium. Most unreliable media are those with the highest number of errors.
Backup Spec Errors Timeline	Shows a number of errors and warnings that occurred using a particular backup specification in a timeline.
Device Errors Timeline	Shows a number of errors and warnings that occurred on a particular device in a timeline.
Client Errors Timeline	Shows a number of errors and warnings that occurred on a particular client in a timeline.
Media Errors Timeline	Shows a number of errors and warnings that occurred on a particular medium in a timeline.
Most Unreliable VMs	Shows a number of unsuccessful sessions that occurred on a particular virtual machine. Most unreliable virtual machines are those with the highest number of the failed sessions.
VM Explorer environment	
Most Unreliable Datacenters	Shows a number of errors and warnings that occurred on a

Errors Summary	
	particular datacenter. Most unreliable datacenters are those with the highest number of errors.
Target Location Errors Timeline	Shows a number of errors and warnings that occurred on a particular target location in a timeline.
Most Unreliable VMs	Shows a number of unsuccessful sessions that occurred on a particular virtual machine. Most unreliable virtual machines are those with the highest number of errors.

VM Infrastructure	
Data Protector environment	
VMs Vs Physical Clients	Shows the percentage of the physical clients and virtual machines in your backup environment, both protected and not protected.
Virtual Vs Physical Environment	Shows how the number of physical clients and virtual machines changes in your backup environment.
VMs per Hypervisor Type	Shows the percentage of virtual machines distribution between the hypervisor types (VMware and Hyper-V).
VMs in Time Period	Shows how the number of virtual machines of different hypervisor types (VMware and Hyper-V) changes in your backup environment.
VMs per Datacenter	Shows the distribution of the VMware virtual machines between datacenters.
VMs per Hypervisor Host	Shows the distribution of virtual machines between hypervisor host machines.
VM Explorer environment	
VMs per Server Type	Shows the distribution of virtual machines between hypervisors of different types (VMware and Hyper-V).
VMs per Datacenter	Shows the distribution of the VMware virtual machines between datacenters.

VM Session/Tasks Summary	
Data Protector environment	
VM Backup Status Overview	Shows a number of sessions performed on virtual machines and their statuses.

VM Session/Tasks Summary	
VM Backup Session Success	Shows the percentage of successful (completed without errors) and unsuccessful backup sessions for the virtual environment.
VMs Without Backup	Shows a list of virtual machines without a protected backup and those virtual machines that are not being backed up.
VM Explorer environment	
VM Backup Status Overview	Shows a number of tasks performed on virtual machines and their statuses.
VM Backup Task Success	Shows the percentage of successful (completed without errors) and unsuccessful backup tasks for the virtual environment.

Monitoring

Monitoring reports display data on currently running sessions and active devices.

> **NOTE:** Monitoring reports are available only for Data Protector environment.

Monitoring Reports	
Sessions in Progress	Shows the currently running sessions, the sessions start time, estimated finish time, and statuses.
Active Devices	Shows the backup devices that are currently used for the running sessions, the sessions start time, estimated finish time, and statuses.
Devices Overview	Shows a list of backup devices that are used for the running sessions.

Capacity

Capacity reports provide information on the amount of the backed up data, available space on media and in the IDB, and compression rates when using the deduplication technology. This helps you to diagnose capacity trends and improve future planning.

Backup Capacity	
Data Protector environment	
Transfer Size per Backup Spec	Shows an amount of the transferred data for a particular backup specification.

Backup Capacity	
Transfer Size	Shows a total, deduplicated, average, and maximum size of the data that was backed up from or restored to a particular cell, tenant, client, instance or application.
Transfer Size per Device	Shows a size of the transferred data for a particular device.
Transfer Size per Media Pool	Shows an amount of the data transferred to a particular media pool.
Transfer Size per Application Type	Shows an amount of the transferred data depending on the application type (for example, Filesystem, IDB, Oracle, SQL, Virtual Environment, and so on).
Top Backup Transfer Size Changes	Shows the biggest growth of transfer size for the same backup specification for full and incremental backups.
Transfer Size Prediction	Shows a transfer size of the data that was backed up from or restored to a particular source (cell, tenant, client, or instance) within a specified timeframe. Based on the current size, the trend is estimated, and the prediction of the transferred data change for the future is calculated.
VM Explorer environment	
Transfer Size per Target Location	Shows a size of the transferred data for a particular target location.

Media Capacity (Data Protector specific)	
Media Pool Capacity	Shows the amount of space available for storing the backed up data in all media pools. The amount of used and free space is indicated.
Target Capacity	Shows the amount of space available for storing the backed up data on all targets. The amount of used and free space is indicated.
Protected Capacity	Shows the amount of space on the media that are protected from being overwritten on the specified date for each Cell Manager, client, or instance.
Data Protection Expiration	Shows the amount of space on the media that are protected from being overwritten. It also provides information, whether the data protection is permanent or will expire after a period of time.
Target Size Prediction	Shows the amount of space used by the backed up data on a particular target as well as an estimated trend of how the amount of used and free space will be changed on this target in

Media Capacity (Data Protector specific)	
	the future.

Dedupe Capacity (Data Protector specific)	
Dedupe Rate per Backup Spec	Shows the amount of data that is backed up and compressed using a deduplication technology and the original size of this data for all backup specifications.
Dedupe Savings per Backup Spec	Shows the amount of space on media that was saved by using a deduplication technology during backup for all backup specifications.
Dedupe Rate Timeline per Backup Spec	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data for all backup specifications in a timeline.
Dedupe Rate per Client	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data on all clients.
Dedupe Savings per Client	Shows the amount of space on media that was saved by using a deduplication technology during backup on all clients.
Dedupe Rate Timeline per Client	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data on all clients in a timeline.
Dedupe Rate per Device	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data on all backup devices.
Dedupe Savings per Device	Shows the amount of space on media that was saved by using a deduplication technology during backup for all backup devices.
Dedupe Rate Timeline per Device	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data on all backup devices in a timeline.
Dedupe Rate Prediction	Shows the amount of the data that is backed up and compressed using a deduplication technology and the original size of this data for all backup specifications. Based on the amount of data that has been backed up so far, the trend of data change is figured out, and a prediction for the amount of the backed up data within the future timeframe is estimated. It

Dedupe Capacity (Data Protector specific)	
	also provides information on the device capacity[1] and shows the available space and estimation when this limit will be reached.
Dedupe Store Capacity	Shows the amount of the data that is backed up and compressed using a deduplication technology. It also shows free space on the deduplication device stores and details on the deduplication and actual size.

IDB Capacity (Data Protector specific)	
IDB Capacity Summary	Shows the current size of the Data Protector IDB and the size of each of the IDB parts, such as Media Management Database (MMDB), Catalog Database (CDB), Detail Catalog Binary Files (DCBF), Serverless Integrations Binary Files (SIBF), and Session Messages Binary Files (SMBF).
CDB Capacity Summary	Shows the current size of the Data Protector CDB and of the records it contains, such as sessions (backup, restore, object copy, object consolidation, object verification, and media management), backed up objects, their versions and object copies, positions of backed up objects on media, and filenames of the backed up files.
MMDB Capacity Summary	Shows the current size of the Data Protector MMDB and of the records it contains, such as, devices, stores, cartridges, compounds, pools, and media.
IDB Capacity Growth	Shows the size changes of the Data Protector IDB and each of its parts, such as MMDB, CDB, DCDB, SIBF, and SMBF.
CDB Capacity Growth	Shows the size changes of the Data Protector CDB and of the records it contains.
MMDB Capacity Growth	Shows the size changes of the Data Protector MMDB and of the records it contains.

VM Capacity	
Data Protector environment	
Transfer Size of VMs Vs Physical Clients	Shows the percentage of the transfer size in the virtual environment and in the physical environment.
Transfer Size per Hypervisor Type	Shows the percentage of hypervisor types (VMware and Hyper-V) in the virtual environment transfer size.

[1] Information on the StoreOnce device capacity is available with Data Protector 9.02 and newer versions.

VM Capacity	
Transfer Size per Datacenter	Shows the distribution of the VMware virtual clients transfer size between datacenters.
Transfer Size per Hypervisor Host	Shows the distribution of virtual clients transfer size between the host machines featuring the host machine hypervisor type and location.
Transfer Size per VM	Shows an amount of the transferred data on a particular virtual machine.
VM Backup Capacity	Shows an amount of the data backed up in the virtual environment.
VM Backup Capacity per Hypervisor Type	Shows volume changes of the data backed up in the virtual environment for each hypervisor type (VMware and Hyper-V).
VM Backup Capacity per Datacenter	Shows volume changes of the data backed up in the VMware virtual environment for each datacenter.
VM Explorer environment	
Transfer Size per Server Type	Shows the percentage of hypervisor types (VMware and Hyper-V) in the virtual environment transfer size.
Transfer Size per Datacenter	Shows the distribution of the VMware virtual clients transfer size between datacenters.
Transfer Size per VM	Shows an amount of the transferred data on a particular virtual machine.
VM Backup Capacity	Shows an amount of the data backed up in the virtual environment.
VM Backup Capacity per Server Type	Shows volume changes of the data backed up in the virtual environment for each hypervisor type (VMware and Hyper-V).
VM Backup Capacity per Datacenter	Shows volume changes of the data backed up in the VMware virtual environment for each datacenter.

Performance

Performance reports provide information on device and media performance as well as on different aspects of the data transfer rate during the sessions.

> **NOTE:** Performance reports are available only for Data Protector environment.

Client Performance	
Backup Transfer Rate per Backup Spec	Shows a data transfer rate during the backup sessions for all backup specifications.

Client Performance	
Backup Transfer Rate per Client	Shows a data transfer rate during the backup sessions on all clients.
Copy Transfer Rate	Shows a data transfer rate during the copy sessions on all clients.

Device Performance	
Device Transfer Rate	Shows a minimum, maximum, and average data transfer rate of read and write operations on all devices.
Media Transfer Rate	Shows a data transfer rate during the backup sessions on all media.

Drill-down reports

These reports can be accessed only when you use the drill-down functionality. Therefore, they provide only information related to the selection in the parent report. The reports are available only in a tabular view.

Lists	
Data Protector environment	
Cell Manager Services	Shows a list of the Data Protector services running on the Cell Manager and their health statuses.
Agent Status	Shows health status for collecting data from the Cell Manager (agent status) and the following information on this Cell Manager: Data Protector version, Cell Manager mode, capacity, and other properties.
IDB Health	Shows health status for the Data Protector IBD.
Licenses	Shows health status for the Data Protector licenses availability on the Cell Manager.
List of Backup Spec Objects	Shows all backup objects specified in a particular backup specification and their properties.
Backup Spec Changes	Shows a list of all versions of the selected backup specification.
Backup Spec Content	Shows in detail the content of the selected backup specification.
Session Output	Shows a report on a particular session. It contains messages on session flow, statistics, status, and results. In case of errors, it also provides error messages.

Lists	
Single Session Report	Shows statistics and properties on a particular session.
List of Clients	Shows all clients and their properties.
List of Media Pools	Shows all media pools and their properties.
List of Media	Shows all media and their properties.
List of VMs	Shows all virtual machines and their properties.
Application RPO	Shows a list of backup sessions with the protected backup data and their RPO[1] status. The RPO breach and warning issue values are specified in the RPO monitor.
Application RTO	Shows a list of backup sessions with the protected backup data and their RTO[2] status. The RTO breach and warning issue values are specified in the RTO monitor.
Session Flow per Backup Specification	Shows the backup sessions duration and statuses for all backup specifications.
Drive Properties	Shows the drive an library properties.
Library Properties	Shows the device properties.
VM Explorer environment	
Task Messages	Shows output messages on a particular task.
List of VMs	Shows all virtual machines and their properties.

How to manage reports

This chapter provides short instructions on how to use the predefined reports and how to adjust their presentation.

You can log in to the Backup Navigator system with your Windows session credentials. You can use the Backup Navigator functionality if your account is recognized as a Data Protector administrator. The available reports contain data collected from the Cell Managers, where your user account is added to the Admin user group. You can perform the following tasks:

- Configuring dashboard layout, on the next page.
- Creating and editing filters, on page 104.

[1] Recovery point objective (RPO) refers to he amount of time that is acceptable between two successful backup of the same application. Define RPO in a monitor to get the value in the report.

[2] Recovery time objective (RTO) refers to the amount of time that is acceptable to restore the backed up data. Define RTO in a monitor to get the value in the report.

- Generating reports, on page 105.
- Adding reports to favorites, on page 106.
- Subscribing to reports, on page 107.
- Exporting reports, on page 108.
- Sending reports by email, on page 108.
- Using drill-down functionality, on page 108.

You can update your Backup Navigator profile, as described in Configuring user profiles, on page 110. If you want to set your region or specify the date format, see Configuring region settings, on page 110.

Configuring dashboard layout

Adjust the dashboard layout for each report category to your needs.

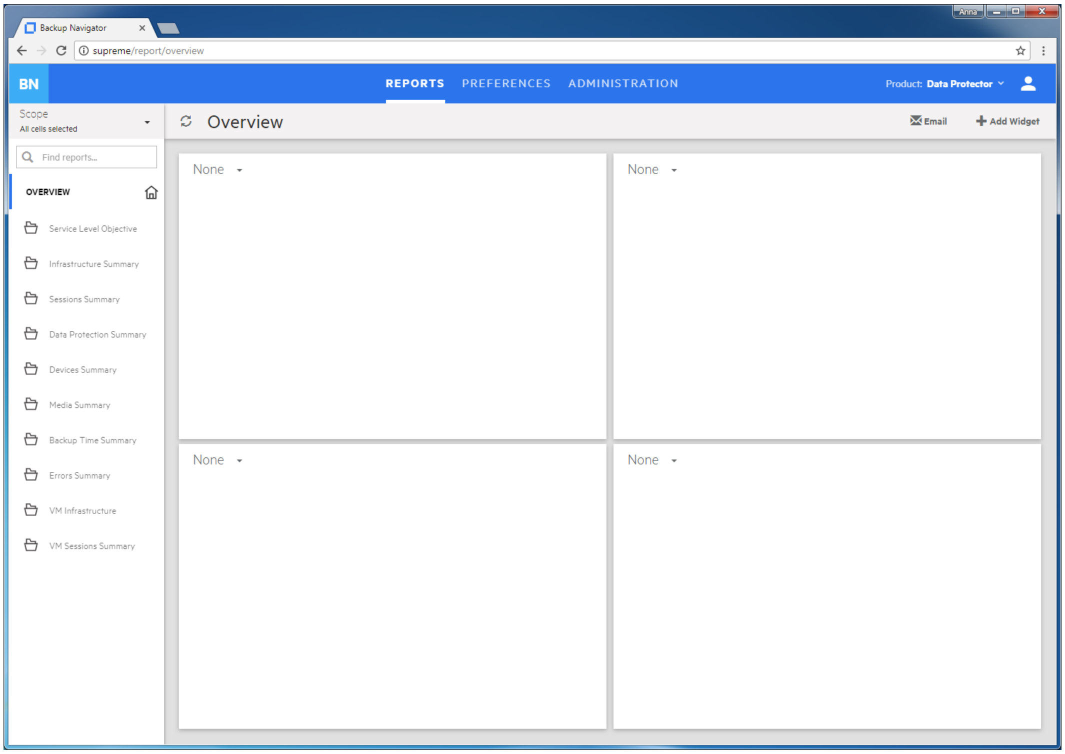
Prerequisite

The report you want to add to dashboard, is added to your favorites. This report has the same scope and parameters as the favorite report.

Steps

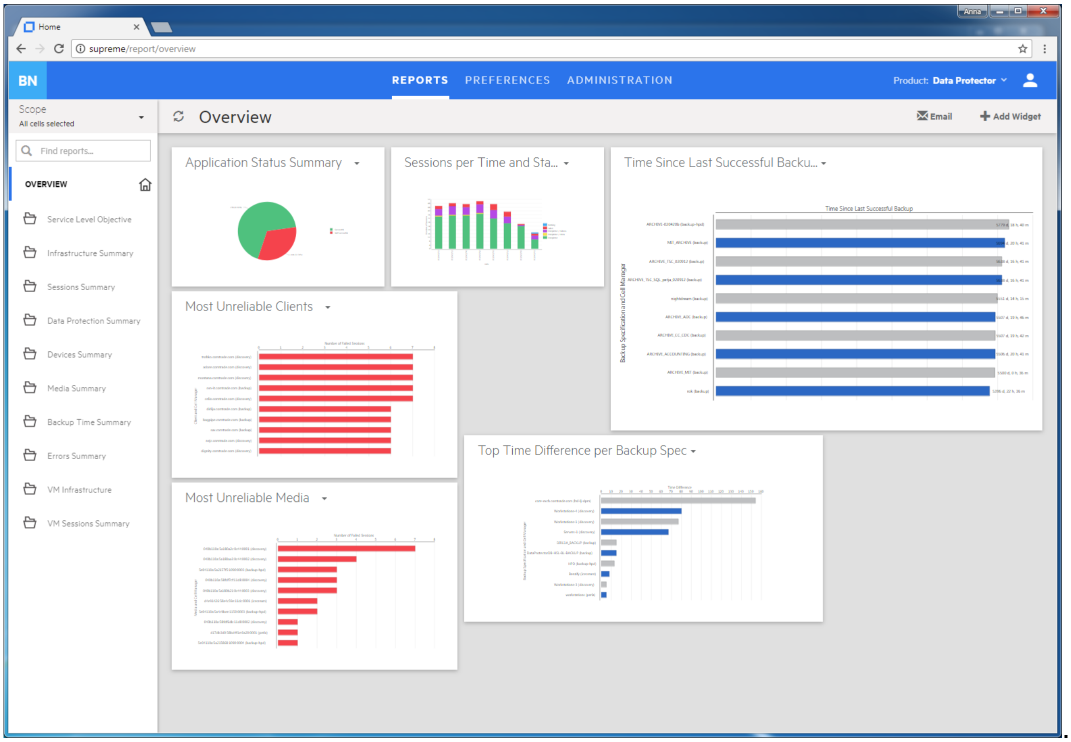
1. Select the **Reports** context.
2. In the Navigation Pane, select the report category (**Overview, Monitoring, Capacity, Performance**), for which you want to configure the dashboard layout.
3. In the Results Area, the default dashboard layout is displayed.

Figure 35: Default dashboard layout



4. In the empty widget, click the arrow and select the available report, which you want to be displayed in this widget. You can later change this report or delete it.
5. To add new more widgets to your dashboard (up to 16), click **Add Widget** in the Tool bar. You can change the size and position of the widget, and delete it from the dashboard.

Figure 36: Configuring dashboard layout



The dashboard layout is save automatically.

Creating and editing filters

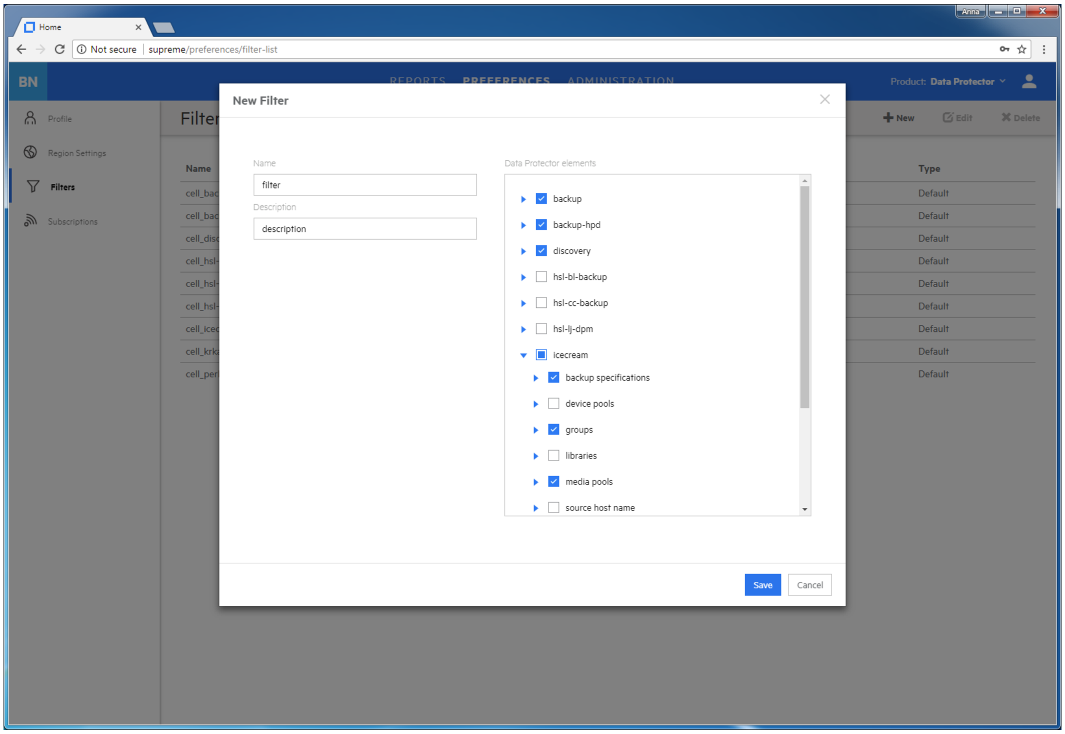
Create a filter to limit the input data for your reports. The input data is information on your Data Protector backup environment received from the Data Protector IDB and stored in the Backup Navigator database in a similar way.

Steps

1. Select the **Preferences** context.
2. In the Navigation Pane, click **Filters**.
3. In the Tool bar of the Results Area, click **New**.
4. In the New filter dialog box, name your filter and enter its description.

   From the available Data Protector cells, select the input data for your reports. You can select the entire cell to collect all data stored in the IDB or only a specific group of the IDB data (for example, devices, device pools, media, and so on). Any number of cells and groups of the IDB data can be selected. The selection represents your new filter.

Figure 37: Configuring filters



New Filter

Name: filter

Description: description

Data Protector elements

- ☑ backup
- ☑ backup-hpd
- ☑ discovery
- □ hsl-bl-backup
- □ hsl-cc-backup
- □ hsl-lj-dpm
- ■ icecream
  - ☑ backup specifications
  - □ device pools
  - ☑ groups
  - □ libraries
  - ☑ media pools
  - □ source host name

5. Click **Create filter**. The new filter is visible in the Navigation Pane.

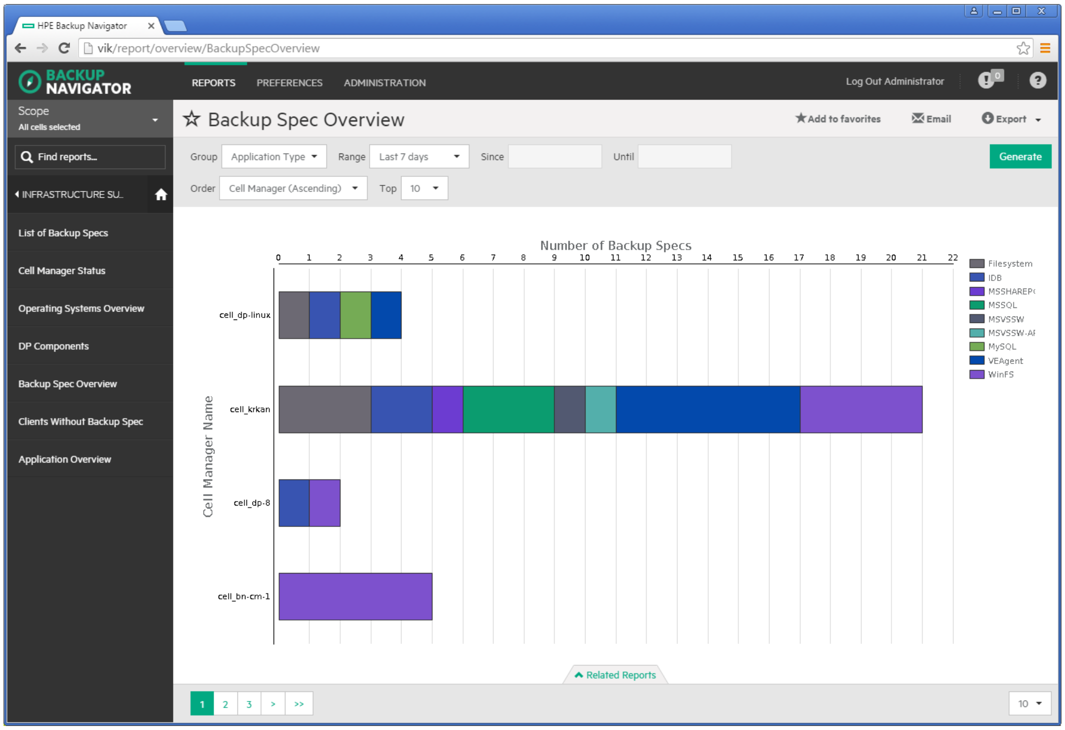
To edit a filter, click the desired filter, change the filter selection and apply your changes.

Generating reports

Update a report with the current data from the Backup Navigator database.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, click **Scope**, and the select **Cells**, **Filters**, or **Tenants**.
3. Select cells or filters to limit your input data, and then click **Apply**.
4. In the Navigation Pane, select the report category and then navigate to the report that you want to generate. You can also search for it by using **Find reports**. The selected report is displayed in the Results Area.
5. In the Tool Bar of the Results Area, specify available parameters according to your needs and then click **Generate**.



Group: Application Type
Range: Last 7 days
Since:
Until:
Order: Cell Manager (Ascending)
Top: 10

You can view the report in a chart or in a table format:

- Use the **Related Reports** tab to see references to the reports that are related to the current one.
- Use numbers and arrows in the bottom left corner of the report to switch between the report related pages. For example, between a graphical and tabular report presentation or between pages of a table.
- Use the drop-down list in the bottom right corner of the report to specify the number of table rows you want to display on one page.

Adding reports to favorites

Add a report to your favorites to access it quicker next time when you need it, to be able to subscribe to it, and to view it within the specified scope and parameters set.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select the report category and then the report that you want to add as your favorite. The selected report is displayed in the Results Area.
3. Change the report parameters according to your interest and click **Generate**.
4. In the Tool Bar, click **Add to favorites**.
5. In the Favorites dialog box, you can enter a name for your favorite report or leave its predefined name.
6. Click **Save favorite**. The report is added to Favorites in the Navigation Pane.

A report is saved with the parameters that were defined when you saved it to favorites. You can edit or remove your favorite report later.

Subscribing to reports

Subscribe to a report to receive it regularly by email.

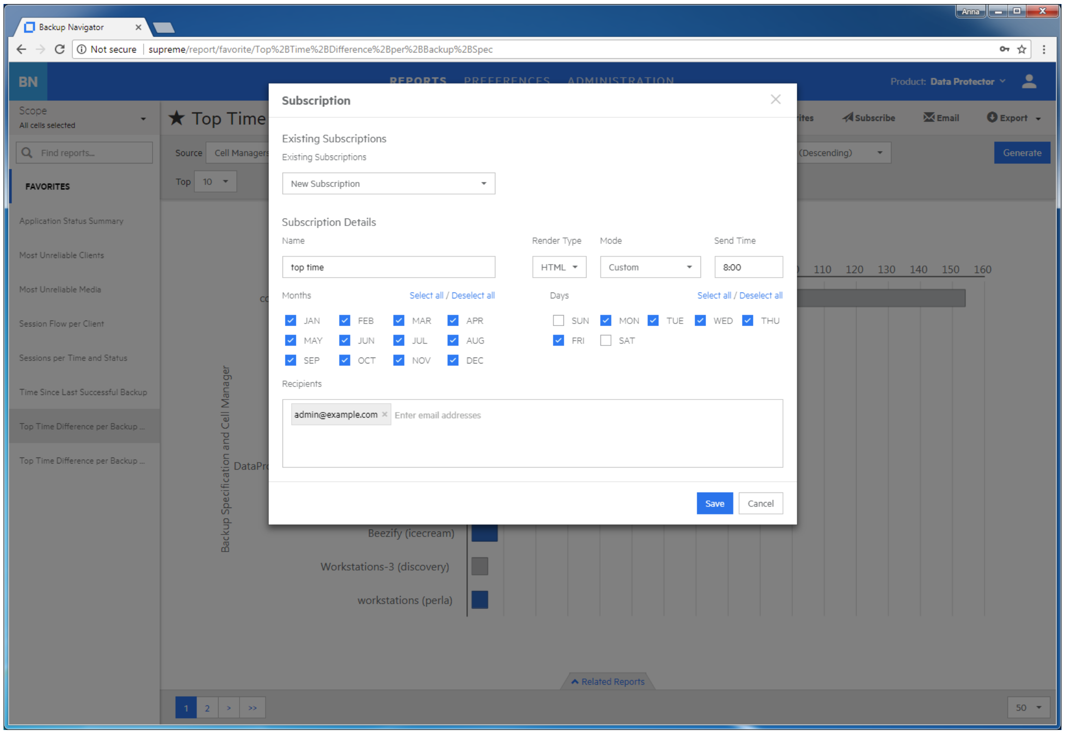
Prerequisite

The report you want to subscribe to, is added to your favorites. This report has the same scope and parameters as the favorite report.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, under Favorites, select the report, to which you want to subscribe. The selected report is displayed in the Results Area.
3. In the Tool Bar, click **Subscribe**.

   Figure 38: Subscribing to reports

   Subscription

   Existing Subscriptions

   Existing Subscriptions: New Subscription

   Subscription Details

   Name: top time | Render Type: HTML | Mode: Custom | Send Time: 8:00

   Months — Select all / Deselect all

   ☑ JAN ☑ FEB ☑ MAR ☑ APR
   ☑ MAY ☑ JUN ☑ JUL ☑ AUG
   ☑ SEP ☑ OCT ☑ NOV ☑ DEC

   Days — Select all / Deselect all

   □ SUN ☑ MON ☑ TUE ☑ WED ☑ THU
   ☑ FRI □ SAT

   Recipients: admin@example.com × Enter email addresses

   Save Cancel

   - Enter a subscription name.
   - Specify time, select months of a year, and days of a week.
   - Enter one or more email addresses, or a mailing list.
4. Click **Save**.Your subscription is added. To review it, select the **Preferences** context and then click **Subscriptions** in the Navigation Pane.

You can always update your subscriptions later.

Exporting reports

Export a report to various formats.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select the report that you want to export to one of the available formats. The selected report is displayed in the Results Area.
3. In the Tool Bar, click **Export**.
4. Select the desired format (**PDF, XLSX, CSV, DOCX, PPTX, HTML**) to download and view the report.

Sending reports by email

Send a report by email to one or more recipients.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select the report that you want to send by email. The selected report is displayed in the Results Area.
3. In the Tool Bar, click **Email**.
4. Enter a subject and recipients email addresses.
5. Click **Send**.

You can also send all reports displayed in the dashboard.

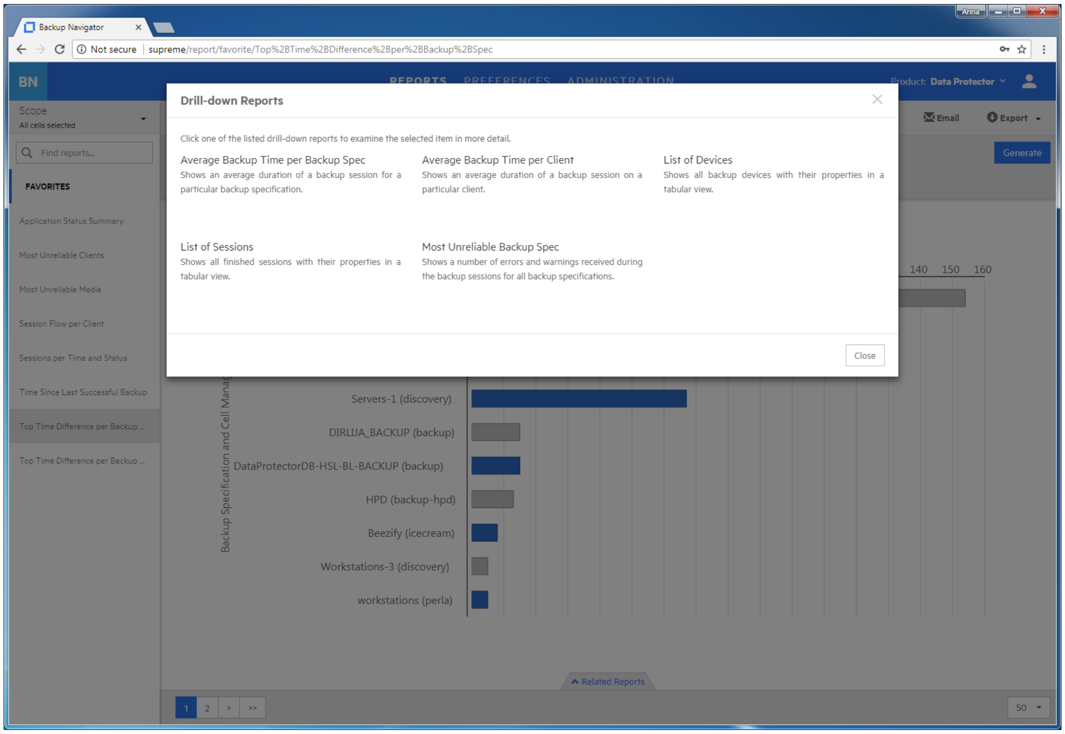
Using drill-down functionality

Examine your report data in a more detail by using the drill-down functionality. You can find out the reason for deviated or error behavior in your environment.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select the report category and then the report that you want to examine. The selected report is displayed in the Results Area.
3. Click an item of your interest inside the graphical report view.

Figure 39: Drill-down reports



Drill-down Reports

Click one of the listed drill-down reports to examine the selected item in more detail.

Average Backup Time per Backup Spec
Shows an average duration of a backup session for a particular backup specification.

Average Backup Time per Client
Shows an average duration of a backup session on a particular client.

List of Devices
Shows all backup devices with their properties in a tabular view.

List of Sessions
Shows all finished sessions with their properties in a tabular view.

Most Unreliable Backup Spec
Shows a number of errors and warnings received during the backup sessions for all backup specifications.

Close

4. In the pop-up window, click one of the available drill-down reports to examine your report data in more detail.
5. Continue to drill down the subsequent reports.

Example of using drill down 1

This example describes how to find the reasons for the failed sessions.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select **Overview > Sessions Summary > Sessions by Session Status**.
3. In the Results Area, click on the pie chart sector, which represents failed session. A window with links to the available drill-down reports pops up.
4. In the pop-up window, click **Most Unreliable Backup Spec**.
5. Select a backup specification with the highest number of errors and click on the bar area of this backup specification, which represent errors.
6. In the pop-up window, click **List of Sessions**.
7. Select the backup session that you want to examine and click on it.
8. In the pop-up window, click **Session Output**. A session report opens.
9. Examine the messages in the session report to find out the reason of the session failure.

Example of using drill down 2

This example describes how to identify the location of the most unreliable medium that will soon be released from protection and available for writing data again.

Steps

1. Select the **Reports** context.
2. In the Navigation Pane, select **Capacity > Media Capacity > Data Protection Expiration**.
3. In the Results Area, click on the bar, which represents the media where data protection will expire soon. A window with links to the available drill-down reports pops up.
4. In the pop-up window, click **Media Summary per Pool**.
5. Select the media pool that contains media of poor quality and click on the part of the bar that represents media pools of the poorest quality.
6. In the pop-up window, click **Media Quality Summary**.
7. Select the medium with the highest number of errors, overwrites, or both and click on the corresponding bar.
8. In the pop-up window, click **Most Unreliable Media**.
9. Select the medium with the highest number of errors and click on the corresponding bar.
10. In the pop-up window, click **List of Media**.
11. Examine the media properties to identify the location.

Configuring user profiles

Configure your profile as an Backup Navigator user.

Steps

1. Select the **Preferences** context.
2. In the Navigation Pane, click **Profile**.
3. Modify the desired fields.
4. Click **Save**.

You can always change these settings later.

Configuring region settings

You can specify your region settings and or change the date format.

Steps

1. Select the **Preferences** context.
2. In the Navigation Pane, click **Region settings**.
3. Select your region and date format.
4. Click **Save**.

You can always change these settings later.

Chapter 9: Troubleshooting

If you encounter problems when using Backup Navigator, you can often solve them yourself. This chapter is intended to help you.

Before you report the problem to the Micro Focus Customer Support Service, ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Backup Navigator limitations and recommendations, as well as known problems, see the *Backup Navigator Release Notes*.
- Your problem is not related to third-party hardware or software. In this case, contact the respective vendor for support.
- You have appropriate prerequisite software installed and configured according to the instructions provided in this guide.
- The system is not running low in space.

How to troubleshoot

When a problem occurs, you can try to solve it by yourself. If you do not succeed in eliminating a problem, prepare all the relevant information for Micro Focus Customer Support Service, and send this data to them.

- On how to recognize a problem, see How to recognize a problem, below.
- On how to perform general checks to determine the cause of a problem and try to resolve it, see General checks, on the next page and Log files, on page 113.
- On how to collect necessary data to send to Micro Focus Customer Support Service, see Collecting data for Micro Focus Customer Support, on page 114.

How to recognize a problem

You usually recognize a problem in Backup Navigator, when you cannot perform some tasks or encounter errors. You can also get information on possible errors from the following sources:

- Backup Navigator event log

  Errors on Backup Navigator related operations are reported to the event log. To view the event log, see Viewing events, on page 62.
- Application server properties

  For some problems, the error messages are issued and can be seen in the application server (Data Protector Cell Manager or VM Explorer Server) property page as Agent messages. The following error messages are available:

  - `License is not valid`: The error occurred, because license is not valid. For information on possible license issues, see Licensing, on page 34
  - `General exception`: The error occurred at an unexpected time. Check the `agent_core.log` file

and search logs marked `FATAL` and then find this problem details in `agent_util_cmd.log`. For information on log files, see Log files, on the next page.

General checks

Perform the following checks to determine and resolve the problem:

1. Verify installation

   If you installed Backup Navigator using the automatic installation script, check, if any errors were reported in the `/var/log/backup-navigator/mf-backup-navigator-install.log` file. If you used manual installation, you should manually verify if all Backup Navigator prerequisites were installed and configured correctly.
2. Verify configuration

   Check, if any errors occurred during the database or user configuration were reported to the Backup Navigator log files. Depending on whether you installed or upgraded Backup Navigator, the errors are reported to the `install.log` or `upgrade.log` file located in the `/opt/dpa-ext/logs` directory.
3. Verify Backup Navigator functionality

   If you have problems with using Backup Navigator, check the following:

   - The database server is up and running and the connection to the database server is established properly.
   - The scope of the cells selected for reports is not empty. Check this by clicking **Reports -> Scope**. If there is no cell selected for reports or the scope is empty, select the cells you want to get reports for or add the cells to the scope respectively. See Establishing data collection environment, on page 39.
   - The initial data collection is finished. Check this by clicking **Administration -> Cell Managers/ VM Explorer Servers**. In the server settings table, check, if the Agent messages column contains the `Initial data collection` message. Wait until the initial data collection is finished.
4. If you use Backup Navigator with Data Protector, verify network configuration and communication with the Data Protector Cell Manager:

   - Hostname resolution

     For successful communication, Backup Navigatorand Data Protector Cell Managers must resolve each others hosts by the fully qualified domain names (FQDN). Resolving a host means that one host can interpret the FQDN of another host and determine its IP address. Use the `ping` command with the FQDN to verify the hostname resolution on the Cell Manager (to this Cell Manager and to the Backup Navigator system) and on the Backup Navigator system (to the Cell Manager and to this Backup Navigator system).

     To check, whether Backup Navigator resolves the Data Protector Cell Manager hostname, run the following command on the Backup Navigator host:

     ```
     # wget hostname:port
     ```

     Where *`hostname`* is the Cell Manager name, as it is specified in Backup Navigator; *`port`* is the Cell Manager port (by default, `5555` and on the Data Protector 10.xx, `5565`).
   - Firewall

To verify, whether the firewall causes problems, turn it off and wait for the next data collection. If the problem persists, turn on the firewall and continue with your investigation. If the problem is eliminated, ensure, that the firewall port range is the same as in the `omnirc` file on the Cell Manager. For example:

a. On the Backup Navigator system, run:

```
# iptables -L INPUT -n -v
```

b. Ensure that the entry with a specified port range is as follows:

```
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpts:XXXX:YYYY
```

where *XXXX*:*YYYY* is a port range.

- Port range

  On the Backup Navigator system, verify that the `OB2PORTRANGE` environment variable value is the same as in the `omnirc` file on the Cell Manager:

  ```
  # echo $OB2PORTRANGE
  ```

  If the value is different, update it:

  ```
  # echo “export OB2PORTRANGE=\”XXXXX-YYYYY\”” >>
  /etc/profile.d/ob2portrange.sh
  # source /etc/profile.d/ob2portrange.sh
  ```

- Connection between Backup Navigatorand Data Protector Cell Manager

  On Backup Navigator, run:

  ```
  # ping CellManager_hostname
  ```

- Connection from the Cell Manager to Backup Navigator

  On the Cell Manager, run:

  ```
  # ping BN_hostname
  ```

- Cell Manager services

  On the Cell Manager, run:

  ```
  # omnisv –status
  ```

  If any of the services is not active, restart the Data Protector services:

  ```
  # omnisv –stop
  ```

  ```
  # omnisv –start
  ```

- If `allow_hosts` and `deny_hosts` lists are enabled on the Cell Manager, add Backup Navigator to the `allow_hosts` list. For detailed instructions, see the Data Protector documentation.
- If the Cell Manager is running in an encrypted mode, add the Backup Navigator system to the Security Exceptions list on the respective Cell Manager to allow non-encrypted communication. For instructions, see the Data Protector documentation.

Log files

Inspecting Backup Navigator log files can help you determine the problem.

Most of the Backup Navigator log files are located at `/opt/dpa-ext/logs`, the log file created during the automatic installation is located at `/var/log/`.

The table below describes the Data Protector log files:

Log file	Description
`agent_core.log`	Contains high-level overview of the data collection operations.
`agent_util_cmd.log`	Contains detailed information on the data collection operations.
`cron_logs.log`	Contains information on data calculation, subscription, and dashboard refresh related operations.
`event.log`	Contains information on the events in Backup Navigator.
`full_app.log`	Contains all operations performed in Backup Navigator besides those written to `event.log`, `cron_logs.log`, and the agent related logs.
`report.log`	Contains information on the generated Backup Navigator reports.
`sts.log`	Contains operating system related information collected during initial installation. This information is mainly intended for the support organization.
`install.log`	Contains information on the initial configuration of the database and user accounts after the Backup Navigator installation.
`upgrade.log`	Contains information on the initial configuration of the database and user accounts after the Backup Navigator upgrade.
`mf-backup-navigator-install.log`	Contains information on the Backup Navigator installation and upgrade, when using the installation script.
`mf-backup-navigator-download.log`	Contains information on the prerequisite software packages download during the Backup Navigator installation and upgrade, when using the installation script.

Collecting data for Micro Focus Customer Support

Collect the relevant data about the problem and send it to Micro Focus Customer Support Service:

- Description of your problem and environment.
- Collected log files. See Backup Navigator logging, on page 71.
- Information about the Cell Managers you collect data from: operating system and Data Protector version.
- Debug logs from the Cell Manager. For instructions on collecting the debug logs, see the Data Protector documentation.

Appendix A: Command Line Reference

Backup Navigator provides commands and scripts to perform some installation and configuration tasks.

mf-backup-navigator-install.sh

Installation script runs installation and upgrade of Backup Navigator. It also downloads prerequisites packages , compresses installation logs, and checks signature of the Backup Navigator installation packages.

Synopsis

```
mf-backup-navigator-install.sh

mf-backup-navigator-install.sh --version | -v

mf-backup-navigator-install.sh --help | -h

mf-backup-navigator-install.sh --download | -d

mf-backup-navigator-install.sh --compress-logs | -cl

mf-backup-navigator-install.sh --signature-check | -sc
```

Description

The `mf-backup-navigator-install.sh` is the Backup Navigator installation script. When used without options, installs or upgrades Backup Navigator.

Options

`--version`

Displays the version of the installation script.

`--help`

Displays the usage synopsis of the installation script.

`--download`

Downloads all prerequisite packages and compresses them to the *`filename`*`.tar.gz` file.

`--compress-logs`

Compresses all installation logs to the *`filename`*`.tar.gz` file.

`--signature-check`

Checks signature of the Backup Navigator `.rpm` packages located in the current directory.

service remote-agent

The `service remote-agent` command starts, stops and checks status of the remote agent processes. Start of the remote agent processes also starts data collection on the Backup Navigator remote agent. When you stop the remote agent processes, data collection also stops.

Synopsis

On RedHat 6.x, CentOS 6.x, SUSE 11.x, the synopsis is as follows:

```
service remote-agent start
```

```
service remote-agent stop
```

```
service remote-agent status
```

On SUSE 12.x, the synopsis is as follows:

```
systemctl start remote-agent
```

```
systemctl stop remote-agent
```

```
systemctl status remote-agent
```

Options

`start`

Starts the remote agent processes and subsequently data collection on the remote agent.

`stop`

Stops the remote agent processes and consequently data collection on the remote agent.

`status`

Checks status of the remote agents.

service tomcat

The `service tomcat` command starts, stops, restarts, and checks status of the `tomcat` service.

Synopsis

On RedHat 6.x, CentOS 6.x, SUSE 11.x, the synopsis is as follows:

```
service tomcat restart
```

```
service tomcat start
service tomcat stop
```

```
 service tomcat status
```

On SUSE 12.x, the synopsis is as follows:

```
systemctl start tomcat
```

```
systemctl stop tomcat
```

```
systemctl status tomcat
```

Options

`restart`

Restarts the `tomcat` service

`start`

Starts the `tomcat` service.

`stop`

Stops the `tomcat` service.

`status`

Checks status of the `tomcat` service.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Micro Focus Backup Navigator 10.20)

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docs.feedback@microfocus.com.

We appreciate your feedback!