

HP BSA Essentials

For the Red Hat Enterprise Linux operating system

Software Version: 9.20

Administrator Guide

Document Release Date: September 2012

Software Release Date: September 2012



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2000 - 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at:

<http://www.hp.com/go/hpsoftwaresupport>

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

HP Software 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
- Download software patches
- Manage support contracts
- Look up HP 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 that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Administrator Guide.....	1
Contents.....	6
Welcome to BSA Essentials.....	9
BSA Essentials Clients.....	9
The BSA Essentials Web Client.....	9
Logging In to the BSA Essentials Web Client.....	9
Supported Browsers.....	10
JRE Versions and Report Authoring.....	10
The BSA Essentials Java Client.....	11
Installing the BSA Essentials Java Client.....	11
Logging In to the BSA Essentials Java Client.....	13
Setting Advanced Options for the BSA Essentials Java Client.....	14
Managing Users and User Groups.....	16
First Time User and Group Setup.....	16
Enabling LDAP Authentication.....	16
Importing Users From Server Automation.....	17
The Admin User.....	19
Permission Types.....	19
Folder Permissions.....	20
Working with User Accounts.....	21
Creating User Groups.....	23
Adding Users To Groups.....	23
Default Users and Groups.....	24
Activating or Suspending User Accounts.....	26
Assigning Permissions to Groups.....	26
Setting Data Access Security Boundaries.....	27
Creating Security Boundaries.....	28
Configuring Cross Device, Policy, and Job Groups.....	30

Creating Cross Device Groups.....	30
Creating Cross Policy Groups.....	31
Creating Cross Job Groups.....	32
Setting Cross Job Groups ROI Unit.....	33
Core Server Administration.....	34
Running Scripts in a Dual Server Configuration.....	34
Starting and Stopping the Core Services.....	35
Enabling BSA Essentials Java Client Access on SA Server.....	36
Configuring Additional Memory.....	36
Configuring BSA Essentials Ports.....	37
Setting Up Live Content Downloads.....	40
Changing the Keystore Passphrase.....	40
Changing BSA Essentials Passwords.....	42
Changing the BSA Essentials Application Level Administrator Password.....	43
Changing the Oracle User Passwords.....	43
Changing the BusinessObjects Administrator Password.....	44
Resetting the BSA Essentials Application Level Administrator Password.....	45
Encrypting Passwords.....	46
Importing a Third Party SSL Certificate.....	48
Third Party Certificate Criteria.....	49
How to Import the Third Party Certificate.....	49
Viewing OMDB Versioning Information.....	52
Running and Configuring SA Compliance Universe Nightly Jobs.....	52
Viewing Oracle User Connectivity Diagnostics.....	53
Unlocking Oracle User Accounts.....	54
Purging the BSA Essentials Database.....	54
Central Management Console Admin Tasks.....	57
Starting and Stopping the Tomcat Server.....	57
Configuring the Reporting Mail Server.....	58
Setting the Default Path for Saved Files on the Core Server.....	59
Updating the Shared Secret.....	60
Monitoring BSA Essentials.....	62

Monitoring with BSA Essentials Tool.....	62
Installing the Monitoring Tool.....	62
Configuring the Monitoring Scripts.....	63
Running the Monitoring Scripts.....	65
Core Server Monitoring Scripts.....	65
Database Monitoring Scripts.....	67
Data Miner Monitoring Scripts.....	68
Integrating with Internal Tools.....	69
Backing Up BSA Essentials on Linux.....	73
Backing Up the BSA Essentials Core Server.....	73
Backing Up the BSA Essentials Database Instance.....	74
Restoring BSA Essentials on Linux.....	76
Preparing the Server or Servers for Restore.....	76
Restoring the BSA Essentials Database Instance.....	77
Restoring the BSA Essentials Core Server.....	78
Verifying BSA Essentials Functionality After Restore.....	78
Recovering New Data Collected Since the Last Backup.....	79

Chapter 1

Welcome to BSA Essentials

Welcome to BSA Essentials 9.20. This product provides both high level and detailed historical reporting on your data center's automation processes for Business Service Automation (BSA) Server and Network Automation products. BSA Essentials gives you insight into your environment through its rich reporting features. These reports provide information about the cost effectiveness and return on investments for the various automated processes in your data center and allow you to see the compliance state of your servers, devices, and business applications.

BSA Essentials Clients

BSA Essentials supports two types of clients that allow you to communicate with the BSA Essentials Core Server. One is considered a thin client and is accessed by using a Web browser. The other client is a Java application that must be downloaded to your personal computer.

To avoid confusion, in this documentation, the client accessed through a browser is referred to as the BSA Essentials Web Client. The client that is a Java application, which is installed on your system is referred to as the BSA Essentials Java Client.

For more information about the BSA Essentials clients, see the following topics.

- ["The BSA Essentials Web Client" \(on page 9\)](#)
- ["The BSA Essentials Java Client" \(on page 11\)](#)

The BSA Essentials Web Client

The BSA Essentials Web Client allows you to create and run BusinessObjects Web Intelligence reports and to perform some basic administrative tasks.

In order to use the BSA Essentials Web Client, you need to log in to the client using a supported Web browser. To view the list of supported Web browsers, see ["Supported Browsers" \(on page 10\)](#).

Before logging in, make sure you have the proper user name and password for the authentication system configured to work with BSA Essentials:

- If authenticating with Active Directory (AD) or LDAP, you need to enter your BSA Essentials username and AD or LDAP password.
- If authenticating with SA, you need to enter your SA username and SA password.
- If there is no external directory source, you must have a BSA Essentials account.

For instructions on how to log in to the BSA Essentials Web Client, see ["Logging In to the BSA Essentials Web Client" \(on page 9\)](#).

Logging In to the BSA Essentials Web Client

To log in to the BSA Essentials Web Client, perform the following steps:

1. Enter the URL of the BSA Essentials Core Server in a browser. For example:

```
https://<bsae-core-hostname>:8443
```

where 8443 is the default port value. It can be configured during the installation process.

2. In the boxes presented, enter your username and password. For example:
 - **Authentication Source:** Select an external authentication source, if configured.
 - **Login Name:** Enter your BSA Essentials (or AD or LDAP or SA) user name.
 - **Password:** Enter your BSA Essentials (or AD or LDAP or SA) password.
3. Click **Log In**.

Note: Users can log in with user name "guest" (no quotes, all lower case) and no password if the Guest user account has been enabled.

For more information on the Guest user and its permissions, see "[Default Users and Groups](#)" (on page 24). For information on how to enable a user account, see "[Activating or Suspending User Accounts](#)" (on page 26).

Supported Browsers

For the list of supported browsers for the BSA Essentials Web Client, see the *Platform Support* document included on the distribution media and available for download on the Self-Solve site at <http://h20230.www2.hp.com/selfsolve/manuals>.

JRE Versions and Report Authoring

For users who need to create reports in BSA Essentials using the Web Client, it is possible that the version of the JRE that is installed on your system may conflict with the JRE version required for the Web Intelligence Java-based report authoring feature.

Internet Explorer Users

If you are using Internet Explorer while trying to author or modify a report, and the reporting panel displays an error message regarding JRE versions or in general fails to successfully load the Web Intelligence reporting panel, perform the following steps:

1. Close the report window without saving, close the Web browser and uninstall the incompatible version of JRE on your system.
2. After you uninstall JRE, launch the BSA Essentials Web Client, log in, return to the reporting features and try to edit the report as before.

Web Intelligence will prompt you to install the required version. Accept the installation. You should now be able to author reports without this error once the required JRE is installed.

Firefox Users

If you are using Firefox and experiencing this problem, go to <http://java.sun.com/products/archive/j2se/6u3/index.html>, select your platform, then download and install the correct version of JRE.

For more information, follow the instructions found at the web sites listed below depending on your operating system platform:

Windows

http://www.java.com/en/download/help/firefox_online_install.xml

Linux

http://www.java.com/en/download/help/linux_install.xml

The BSA Essentials Java Client

You must use the BSA Essentials Java Client to set data access security boundaries on reporting objects; these boundaries once created, can be managed through the BSA Essentials Web Client. For information on how to create data access permission security boundaries, see "[Setting Data Access Security Boundaries](#)" (on page 27).

The BSA Essentials Java Client also allows you to create and run BIRT reports. For more information on BIRT reporting, see "About BIRT Reporting" in the BSA Essentials *User Guide*.

Before you can log in to the BSA Essentials Java Client, you need to download the installer from the BSA Essentials Core Server. Procedures to install, log in to, and configure settings for the BSA Essentials Java Client are described in the following sections:

- "[Installing the BSA Essentials Java Client](#)" (on page 11)
- "[Logging In to the BSA Essentials Java Client](#)" (on page 13)
- "[Setting Advanced Options for the BSA Essentials Java Client](#)" (on page 14)

Note: The BSA Essentials Java Client Launcher only allows you to log in to a BSA Essentials Core Server. If you attempt to log into a pre-BSA Essentials SAR Core Server, you will get a 404 page not found Java Web Start error message and not be able to log in to the Core.

Note: If you are running the BSA Essentials Java Client Launcher on Windows 2000, you may see a missing DLL error message when you log in. This error will not affect the log in procedure. To prevent this error from appearing, install the [Microsoft update](#).

Installing the BSA Essentials Java Client

In order to access the BSA Essentials Java Client you need to download and install the client launcher. You can find the link to download the client launcher on the BSA Essentials Web Client home page, just beneath the login fields. The BSA Essentials Java Client Launcher allows you to log in to a BSA Essentials Core Server. You must use the BSA Essentials Java Client to set data access security boundaries on reporting objects; these boundaries once created, can be managed through the BSA Essentials Web Client.

Installing the client requires that you perform the following tasks:

Task 1: Learn About the BSA Essentials Java Client and Client Launcher

The client launcher is a self-contained Java application that allows you to access the BSA Essentials Java Client from any BSA Essentials Core Server. You can use the launcher to log in to and download the latest version of the client. If the client has been upgraded on a specific BSA Essentials Server, you can choose the server you want to use for downloading the client.

The client launcher also allows you to configure advanced settings, such as debug settings, locale settings, and access to the Java Web Start that runs the launcher and the BSA Essentials Java Client.

The BSA Essentials Java Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). The client will not interfere with any other versions of JRE you may have installed on your system. The JRE will not be used (and is not usable) by any other Java

application on the target computer, and it will not set itself as the default JRE on the target computer.

Task 2: Understand BSA Essentials Java Client System Requirements

For the list of supported operating systems for the BSA Essentials Java Client, see the *Platform Support* document included on the distribution media and available for download on the Self-Solve site at <http://h20230.www2.hp.com/selfsolve/manuals>.

The minimum systems requirements to run the client are the following:

- Minimum 1 GB of DRAM
- Minimum 100 MB of disk space

If you are using the BSA Essentials Java Client to connect to a Core Server over a residential DSL connection, a minimum 384 Kbps DSL connection is recommended.

You need to be logged in as a user that has sufficient permissions to install software on the computer. (You do not need to be an administrator user to install the launcher.)

To run the client, you must download and install the BSA Essentials Java Client Launcher as explained in the next task.

Task 3: Install the BSA Client Launcher

In order to run the BSA Essentials Java Client, you need to download and install the client launcher, which is a Java application that allows you to access the client from any BSA Essentials Server. In order to install the client launcher, you must be a Windows user that is able to install applications on your system. When you install the client launcher, it installs all the necessary Java applications (Java Web Start and JRE) you need to run the client.

If you plan to have multiple users install the client launcher on the same computer, we recommend that each user choose a unique path to install the application. For example, if one user has already installed the client launcher in the default location, C:\Program Files\HP BSA\Launcher, then if another user logs in to the same computer and attempts to install to that same default location, the second user will see an error and not be able to install. If this occurs, choose a new location.

To install the client launcher, perform the following steps:

1. Open a Web browser, and enter the URL to the BSA Essentials Web Client server. For example:

```
https://<bsae-servername>:8443
```

where 8443 is the default port value. It can be configured during the installation process.
2. On the BSA Essentials Web Client home page, under the log in fields, click the **Download BSA Launcher** link.
3. Download the HP BSA Essentials Client Launcher installation file and double-click to start the launcher installation.
4. In the Welcome window, click **Next**.
5. In the License Agreement window, select the "I accept the agreement" option, and then click **Next** to proceed with the installation.

6. In the Select Destination Directory window, accept the default installation directory, or click **Browse** to select a custom location. Click **Next**.
7. In the Select clients to install window, select HP BSA Essentials Client.
8. In the Select Start Menu Folder window, accept the default name and click **Next**.
9. In the Select Additional Tasks window, accept the default options or choose your own, and then click **Next** to install the client launcher.
10. When the installation has completed, click **Finish** to exit.

Task 4: Uninstall the Client Launcher - Optional

You can uninstall the client launcher using the Windows Add or Remove Programs utility located in the control panel on your system.

To uninstall the client launcher, perform the following steps:

1. From the Start menu, select Control Panel.
2. Double-click the Add or Remove Programs application.
3. In the Currently Installed Programs table, select the HP BSA Launcher application.
4. Click **Remove**.
5. Close the Add or Remove Programs application.

Logging In to the BSA Essentials Java Client

To launch the BSA Essentials Java Client, perform the following steps:

1. Start the Java Client Launcher by selecting **Start** → **All Programs** → **HP Business Service Automation** → **HP BSA Essentials Client**.
2. In the Log In to HP BSA Essentials Client window, enter your BSA Essentials user name, password, and the BSA Essentials Server you want to log in to.

Note: If you are using an external authentication system with BSA Essentials, such as AD, LDAP or Server Automation (SA), you need to append your username with that authentication system when you log in, using the following syntax:

```
username@$authsource_name
```

For example, if a user named `joe_user` wanted to log in and was using SA as an external authentication source, the username log in would look like this:

```
joe_user@sa
```

3. Enter the BSA Essentials Server's IP address or host name in the core server field, such as:
`<bsae-2-0-servername>:<port>`.

where `<port>` is the port value for the BSA Essentials Core Server. If the server is listening at the default port value of 8443, it does not need to be specified.

If this is the first time you are logging into a specific BSA Essentials Server, the launcher will download the latest version of BSA Essentials when you log in. If you would like to differentiate between the BSA Essentials Core Server you log in to and the core from which you download

the latest version of the BSA Essentials Java Client, you can change those options by clicking **More >>** in the log in window. See "[Setting Advanced Options for the BSA Essentials Java Client](#)" (on page 14).

4. Click **Log In**.
5. If you are asked to accept the certificate from the core server, click **Yes**. The BSA Essentials Client now appears.

Setting Advanced Options for the BSA Essentials Java Client

You can configure the following advanced options for the BSA Essentials Java Client:

- **Debug Settings:** Gives you control over the level of detail, as well as the type of information included in BSA Essentials Client log file.
- **Client Download Server:** Allows you to change the host server from which you want to download the BSA Essentials Client.
- **Proxies:** Allows you to configure the BSA Essentials Client proxy server settings.
- **HP BSA Essentials Home:** Allows you to change the default location from which the BSA Essentials Client is downloaded and saved on your local computer, and to delete the BSA Essentials Client's cache, and to change the location of BSA Essentials Client log files.

To configure the BSA Essentials Java Client's advanced options, perform the following steps:

1. Start the Java Client Launcher by selecting **Start** → **All Programs** → **HP Business Service Automation** → **HP BSA Essentials Client**
2. Click **More >>**. In the expanded window, you can configure the following settings:
 - **Locale:** Select the version of the BSA Essentials client to match your system's locale. English (en) is the default, but you can also select either Japanese (ja) or Korean (ko).
 - **Debug Settings:** Set the debugging options for the log file located at `<user_home>\Application Data\HP BSA\deployment\log\javaws*.log`.
 - **Enable Debug Logging (Fine):** Enables debugging and sends BSA Essentials Client operations and errors to the log file.
 - **Enable Server Method Call Logging:** Adds server method calls to the log file.
 - **Show Console:** Displays the Java Console window while the BSA Essentials Client runs.
3. Click **Advanced Settings**. In the Advanced Settings Window, you can configure the following settings:
 - **Client Download Server:** You can configure the BSA Essentials Client Launcher so the default core you log in to is different from the core you use to access the latest version of the BSA Essentials Client. This can be useful if you do not want to download a new version of the BSA Essentials Client each time you log in to a different core running the same version of BSA Essentials.

- **Use Core Server:** Select this option to download the BSA Essentials Client from the same server to which you want to log in.
 - **Use:** Enter a core server you want to use to download the BSA Essentials Client.
 - **Proxies:** By default, the BSA Essentials Client uses the proxy server settings configured for the default browser on your local system. For example, if your default browser has no proxy server settings configured, neither will the BSA Essentials Client. You can change those proxy server settings by configuring the following options:
 - **None:** Do not use a proxy server to connect to the BSA Essentials Client.
 - **Use Browser:** Use the proxy server settings specified in your default browser.
 - **Manual:** Enter the proxy server hostname and port.
 - **No Proxy Hosts:** If you want to add proxy server overrides, add them here, separated by commas. (This is only enabled when proxy server settings is set to Manual.)
 - **HP BSA Essentials Home:**
 - **Location:** The location where the BSA Essentials Client is downloaded and saved on your local computer, along with all log files generated when the BSA Essentials Client runs.

Note: The default home location is `<user_home>\Application Data\HP BSA`, which is private to each user. If you choose to change this location, be aware that other users may have access to the new directory. You are responsible for setting the permissions on the new directory if you want to prevent unwanted access to your BSA Essentials Client home.
 - **Delete Application Cache:** Clicking this completely removes all downloaded copies of the BSA Essentials Client. This ensures the launcher will download the latest BSA Essentials Client from the core the next time the user logs in.
 - **Delete Logs:** Delete all log files created by previous sessions of the BSA Essentials Client. All BSA Essentials Client log files are located at `<user_home>\Application Data\HP BSA\deployment\log\javaws*.log`.
4. When you finish setting your options, click **OK**.
 5. Click **Log In** to log in to the BSA Essentials Java Client.

Chapter 2

Managing Users and User Groups

In BSA Essentials, group permissions control all user actions and access to viewing data in reports.

In order to use BSA Essentials features - such as create and view reports, create Cross Item Groups, and so on - you need to create users and then add them to groups. Once users have been added to groups, you can assign the appropriate permissions to the group so all its members can perform the actions allowed by the group's data access and application privileges.

Managing user and user groups consists of the following tasks:

- ["First Time User and Group Setup" \(on page 16\)](#)
- ["Working with User Accounts" \(on page 21\)](#)
- ["Creating User Groups" \(on page 23\)](#)
- ["Assigning Permissions to Groups" \(on page 26\)](#)

First Time User and Group Setup

When you first install BSA Essentials, an admin user is created who has the credentials to log in to the application and set up user and group accounts. Before people can start using the product, the admin user must create user groups, add users to the groups, and then apply permissions to the groups.

If your BSA Essentials was setup using an external authentication system, those users and groups will appear in the Administration tab of the client when you first log in.

Setting up users and groups in BSA Essentials requires performing (or understanding) the following topics:

- ["The BSA Essentials Web Client" \(on page 9\)](#)
- ["The Admin User" \(on page 19\)](#)
- ["Default Users and Groups" \(on page 24\)](#)
- ["Permission Types" \(on page 19\)](#)
- ["Working with User Accounts" \(on page 21\)](#)
- ["Creating User Groups" \(on page 23\)](#)
- ["Assigning Permissions to Groups" \(on page 26\)](#)

Enabling LDAP Authentication

If you want to configure BSA Essentials to use an external authentication system such as LDAP, you can do so by performing the following task.

Note: After you perform this task to enable LDAP authentication, you still will need to create user and group accounts for your LDAP users. For more information, see "[Working with User Accounts](#)" (on page 21).

Configuring to Use an LDAP Authentication System

1. Log in to the BSA Essentials Core Server.
2. Change your user to become the BSA Essentials super user on the server. For example:

```
su - omdb
```
3. Change your directory to the following location:

```
cd /opt/opsware/omdb/bin
```
4. Execute the following command:

```
./loginconfig.sh add
```
5. Use a local administrative account to connect to the BSA Essentials Core Server.
6. Select LDAP from the list of choices.
7. The interview will ask you to enter values for the following parameters:
 - Host: The IP address or host name of LDAPserver
 - Enable SSL [yes]:
 - Port: The port used to connect to LDAP server
8. If the answer to Enable SSL is **yes**, the following parameters need to be configured:
 - Full file name of server CA certificate: LDAP server certificate
 - Enable use client certificate [no]:
9. If the answer to Enable use client certificate is **yes**, the following parameters need to be configured:
 - Full file name of client certificate: LDAP client certificate
10. Finally, the interview will ask you if you want to enable the following options:
 - Enable use starttls [no]: Enable this option if you want to upgrade plain text connections to encrypted connections.
 - Enable debug [no]: Enable this option if you want more verbose output.
11. After you have finished entering the values, exit the shell.

Importing Users From Server Automation

If you are using Server Automation (SA) as your user authentication system for BSA Essentials, you can perform the following tasks in order to import all of your pre-existing users and user groups into BSA Essentials.

Adding the SA Authentication Source

1. Log in to the BSA Essentials Core Server.

2. Change your user to become the BSA Essentials super user on the server. For example:

```
su - omdb
```

3. Change your directory to the following location:

```
cd /opt/opsware/omdb/bin
```

4. Execute the following command:

```
./loginconfig.sh add
```

You are prompted for the user name and password for the BSA Essentials application level administrator.

5. Specify the admin credentials for the BSA Essentials application level administrator. The choices for import are displayed.
6. Select 2 for HP-SA. This initiates the interview prompts.
7. Specify the following information at the prompts:

- **Auth Source Name:** Enter the hostname for the SA Server hosting the SA Web Services Data Access Engine ("twist").
- **Auth Source Display Name:** Enter a display name of your choice.
- **Host:** Enter the Fully Qualified Domain Name (FQDN) for the SA Server hosting the SA Web Services Data Access Engine ("twist").
- **Port [443]:** Accept the default port value if it is not in use.
- **Enable debug [no]:** Accept the default debug option if you do not want to enable debugging.

When you have finished entering the required information, you will see the "Successfully added the new authentication source" message displayed.

Note: You can use the `loginconfig.sh` command to delete, update, and list authentication sources. Execute `./loginconfig.sh help` to list all of the command options.

Setting the 'User Importing Enabled' Property

Note: If during the installation procedure, you selected the **Enable user import** option, which creates and updates user and group information from data collected by the data miner from Server Automation, there is no need to follow this procedure. See the "Installing BSA Essentials" chapter in the *BSA Essentials Installation Guide*.

1. Log in to the BSA Essentials Core Server.
2. Change your user to become the BSA Essentials super user on the server. For example:

```
su - omdb
```

3. Using a text editor, open the following file so you can edit it. For example:

```
vi /etc/opt/opsware/omdb/omdb.properties
```

4. Set the following parameter to "true":

```
com.opsware.cmdb.security.importusers.enabled=true
```

5. Save the file.
6. Change to the root user:

```
su - root
```

7. Restart the BSA Essentials core services:

```
/etc/init.d/opsware-omdb restart
```

Note: SA user import into BSA Essentials is an ongoing process, supported by standard SA data mining.

The Admin User

The admin user in BSA Essentials is created during installation and enables you to set up and manage users and groups and their permissions, as well as set up reporting data delivered with the product. The admin password is also set during install time, so to access this password consult your BSA Essentials administrator.

The BSA Essentials admin user is pre-configured to be able to perform all the necessary steps to allow your team to use the product, including the following:

- Access to all application and data permissions, and the ability to grant permissions to User Groups

For more information, see ["Permission Types" \(on page 19\)](#) and ["Assigning Permissions to Groups" \(on page 26\)](#)

- Ability to create and delete users (except the admin user itself) and user groups

For more information, see ["Working with User Accounts" \(on page 21\)](#) and ["Creating User Groups" \(on page 23\)](#)

- Ability to create security boundaries in the BSA Essentials Java Client

For more information, see ["Setting Data Access Security Boundaries" \(on page 27\)](#)

Permission Types

In BSA Essentials, group permissions regulate the actions that users in a group are able to perform, as well as control the types of data that a user can view in a report.

There are two kinds of permissions you can apply to groups:

- An *application permission* allows members of a group to perform specific actions, such as run reports, schedule reports, or manage report folders, and so on.
- A *data access permission* allows members of a group to view specific kinds of data from the different automation applications. For example, you can allow a group to view Network Automation and Server Automation Device Groups, virtual servers, and so on.

For more information on setting security boundaries on data types, see ["Creating Security Boundaries" \(on page 28\)](#).

The following two tables list all of the application and data access permissions that you can associate with a group.

Application Permissions

Application Permission Name	Actions
BSA Essentials Reporting Application	Create Web Intelligence Documents and running report queries using the InfoView Java reporting panel.
BIRT Reporting Enterprise Report Scheduling Management	Manage all BIRT report scheduling in the BSA Essentials Client. For more information, see "The BSA Essentials Java Client" (on page 11) .
BIRT Reporting Personal Report Scheduling Management	Manage your own user's BIRT report scheduling in the BSA Essentials Client. For more information, see "The BSA Essentials Java Client" (on page 11) .
Report Folder Access Control Management	Set permissions on report folders in the Document List in the Reporting panel.

Data Access Permissions

Data Access Permission Category	Data Types
ASAS (Storage Visibility and Automation)	Agent, Database, Disk Drive, Fibre Alias, Fibre Fabric, Fibre Zone, Fibre Zone Set, File System, Port, Port Controller, Replication Group, Service, Storage Device, Storage Extent, Storage Pool
Item Groups	Access to all Cross Item Group Data (Devices, Policies, and Jobs)
NAS (Network Automation)	Approval Rule, Configuration Policy, Configuration Rule, Core, Custom Script, Device, Device File System, Device Group, Device View, Event, Event Rule, Role, Satellite, Satellite Realm, Site, Software Image, Software Policy, Task, Task Types, Template, User, UserGroup
PAS (Operations Orchestration)	Flow Runs, Flows, Run Steps
SAS (Server Automation)	Application Configuration, Application Installation, Audit, Audit Exclusion (exception), Audit Policy, Audit Result, Authentication Source, Business Applications, Customer, Facility, Feature, Folder, Job, Job Type, OPE (APX), Operating System, Patch Exception, Patch Policy, SMO, Security Boundary, Security Boundary EORV Value, Security Boundary Field Value, Server, Server Group, Snapshot, Software Package, Software Policy, User, User Group, Virtual Server

Folder Permissions

In the Document List of the reporting panel, each folder structure is governed by permissions that are controlled by the BusinessObjects Enterprise Central Management Console (CMC). For information on how to use the CMC, consult the BusinessObjects Enterprise documentation.

Consider the following rules when working with folders in the Document List:

- Users may view all report results that are stored in folders that they have Read access to, regardless of whether they have data permissions for the report results.
- A user's configured data permissions are applied at the time that a report is run (not viewed).
- Users with the necessary permissions to modify permissions of report folders should pay close attention to the group permissions to which they are assigned access.
- Newly-created report folders by default inherit the permissions of the parent folder.

Working with User Accounts

Create user accounts for all people you want to be able to view, edit, create and run reports, create cross item groups, and so on.

Each newly-created user is placed automatically into the "Everyone" group, which by default has the "BSA Essentials Reporting Application" permission but no data permissions.


In order to receive permissions beyond the default reporting permissions, such as data access permissions and so on, you will need to add new users to groups and then assign permissions to those groups.

For instructions on how to create a user group, see ["Creating User Groups" \(on page 23\)](#). For more information on permission types, see ["Permission Types" \(on page 19\)](#).

Creating a user account consists of the following tasks:

Task 1: Creating a User Account

To create a user account, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Users.
3. On the right side of the page, select the new user  button.
4. In the New User dialog, enter the following user information:
 - **First Name:** Must be at least two characters long.
 - **Last Name:** Must be at least two characters long.
 - **Full Name:** Enter user's full name.
 - **Authentication Source:** If your BSA Essentials Core Server has more than one authentication source configured, then you can choose from this list. If you choose LDAP as your authentication source, you will be asked for a Distinguished Name (DN) instead of a password. The format of the DN needed will depend on the LDAP or Active Directory server configuration. For more information on configuring an LDAP authentication source for BSA Essentials, see ["Enabling LDAP Authentication" \(on page 16\)](#).
 - **Email:** This is a required field.
 - **Username:** Username must be at least four characters long and contain no special


characters.

- **Password:** Password can contain regular and special characters.

5. Click **Save**.




Task 2: Changing Login Password

To change a user's login password, perform the following steps:

1. From the BSA Essentials Administration tab, select **Security** → **Users**.
2. Select a user.
3. Below the user, select the Login tab.
4. Enter the new user password twice.
5. Click Save  (far right of lower pane) to save your changes.

Task 3: Modifying Group Membership


To modify a user's group membership, perform the following steps:

1. From the BSA Essentials Administration tab, select **Security** → **Users**.
2. Select a user.
3. Below the user, select the Group Membership tab.
4. To assign the user to a group, click the Add  icon.
5. In the Add Group dialog, select the check box next to the group name to which you want to add the user and click **Add**. (Do this for every group to which you want to add the user.)
6. Click **OK**. The user's profile Group Membership displays all the groups to which the user is a member.
7. To remove the user from a group, select the check box next to the user's name and then click the Remove  icon.
8. Click the Save  button (far right of lower pane) to save your changes.

Task 4: Editing User Preferences

To edit a user's preferences, such as time zone and data format, perform the following steps:

1. From the BSA Essentials Administration tab, select **Security** → **Users**.
2. Select a user.
3. Below the user, select the Preferences tab.
4. From the Time Zone selector, choose a time zone appropriate to your location.
5. From the Long Date Format selector, select a date format for when the user interface displays the full date.
6. From the Short Date Format selector, select a date format for when the user interface displays

7. Click the Save  button (far right of lower pane) to save your changes.


Creating User Groups

In BSA Essentials, all user permissions are applied to user groups. When you add permissions to a group, and then add users to the group, all users that belong to the group receive all the permissions associated with the group. With group-based authentication (or often called "role-based authentication"), you can create groups of users that you want to be able to perform specific actions and access specific data.

Creating user groups consists of the following tasks:



Task 1: Creating a User Group

To create a user group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the New Group  button.
4. In the New Group dialog, enter a Name and Description (optional) for the group, and then click **Save**.

Task 2: Adding Users to a Group

To add users to a group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the group to which you want to add members and click the Add Users  button.
4. In the add User dialog, select a user or multiple users and then click **Add**. (To select multiple users, you can hold the SHIFT or CTRL key while you select users.)
5. When you are finished adding users, click **OK**.
6. Click **Save**  (far right of lower pane) to save your changes.

Adding Users To Groups

After you create a group, you need to add users to the group.


For more information on assigning permissions to groups, see ["Assigning Permissions to Groups" \(on page 26\)](#).

Adding Users to a Group

To add users to a group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the group to which you want to add members and click the

Add Users  button.

4. In the add User dialog, select a user or multiple users and then click **Add**. (To select multiple users, you can hold the SHIFT or CTRL key while you select users.)
5. When you are finished adding users, click **OK**.
6. Click **Save**  (far right of lower pane) to save your changes.

Default Users and Groups

When you install BSA Essentials and log in for the first time, some default users and user groups are already created. These user groups and users help you get started using the product and setting up user accounts.

Default Users

By default, two users are created during installation (these user account names are all lower case and are case-sensitive):

- **admin**: The admin user is the first user that is created during installation, is given automatic group membership to the default user groups, and has the ability to create users and groups and grant all permissions. This user is also granted extra permissions that no other user has that enables this user to configure BSA Essentials, such as setting security boundaries for data items from the BSA Essentials Java Client. The admin account cannot be deleted.
- **guest**: The guest user is a basic user who is created during installation, but whose account is disabled. This account can be used for generic users who may not be typical BSA Essentials users but who may need access to reports. This account needs to be activated to be functional and cannot be deleted.

Default User Information	
User	Description
admin	The first-time user created upon installing the product, which enables you to set up all other user accounts, user groups, permissions, cross item groups, and so on.
Group Membership	Everyone, System-Administrators
Hidden permissions	Access to the Admin console Access to the BSA Essentials Java Client and ability to set security boundaries on data items

Default User Information	
User	Description
guest	This account allows any user to log in to the BSA Essentials Web Client. This account is disabled by default. For information on how to activate a user account, see " Activating or Suspending User Accounts " (on page 26).

Default User Information		Description
Group membership		Guest

Default Groups

By default, there are three user groups created during install that the admin user can use to set up the kinds of users that can access the BSA Essentials features. They are the following:

- **Everyone:** Default group designed for permissions you want all users to have.
- **Guest:** Default group designed for guest users who might need to access Reports. By default, this account is disabled.
- **System-Administrators:** Default group designed for BSA Essentials super users.

Default Group Information	Description
Everyone	
Application Permissions	BSA Essentials Reporting Application
Data Access Permissions	None
Hidden Permissions	Access to the BSA Essentials Client , but no ability to set security boundaries on data items
Default Member	admin

Default Group Information	Description
Guest	
Application Permissions	BSA Essentials Reporting Application
Data Access Permissions	None
Default Member	guest

Default Group Information	Description
System-Administrators	
Application Permissions	BSA Essentials Reporting Application BIRT Reporting Enterprise Report Scheduling Management BIRT Reporting Personal Report Scheduling Management


Default Group Information	Description
	Report Folder Access Control Management
Data Access Permissions	All
Hidden Permissions	Access to and ability to set security boundaries on data items
Default Member	admin

Activating or Suspending User Accounts

If you need to block access for a user account, you can suspend the account. When a user account is suspended, that user will not be able to log in to the BSA Essentials Web Client.

If you want the user to have access, you can activate the user account, and then the user will be able to log in to BSA Essentials.

To suspend or activate a user account, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Users.
3. From the Users list, select the user account you want to suspend.
4. Click **Suspend** at the top of the user list.
5. When the user account is suspended, the user icon has a red  through it .
6. To reactivate the account,select the user and click **Activate**.

Assigning Permissions to Groups

Permissions in BSA Essentials are controlled by groups. A user must belong to a group that has the appropriate permissions before the user can perform an action, such as viewing data in a report or creating a new report.

There are two kinds of permissions you can apply to groups:



- An *application permission* allows members of a group to perform specific actions, such as run reports, schedule reports, or manage report folders, and so on.
- A *data access permission* allows members of a group to view specific kinds of data from the different automation applications. For example, you can allow a group to view Network Automation and Server Automation Device Groups, virtual servers, and so on.

For more information on permissions, see "[Permission Types](#)" (on page 19).

For more information on creating data item security boundaries, see "[Setting Data Access Security Boundaries](#)" (on page 27).



Assigning Application Permissions to a User Group

To assign application permissions to a group, perform the following steps:

1. From the BSA Essentials Administration tab, select **Security** → **Groups**.
2. Select a group to which you want to add application permissions.
3. Below the group, select the Application Permissions tab.
4. Click the Add Application Permission  button.
5. In the Add Application Permission dialog, select a feature name by clicking the checkbox next to the name. You can use CTRL + select or SHIFT + select to select more than one permission to add to the group.
6. To add the selected application permissions, click **Add**.
7. Click **Save**  (far right of lower pane) to save your changes.

Assigning Data Access Permissions to a User Group

To assign data access permissions to a group, perform the following steps:

1. From the BSA Essentials Administration tab, select **Security** → **Groups**.
2. Select a group to which you want to add application permissions.
3. Below the group, select the Data Access Permissions tab.
4. Click the Add Data Access Permission  button.
5. In the Add Data Permission dialog to add access to all data for the group, select All Data Permissions.
6. To add specific data access permissions, from the Item Type drop-down list, select a data item type.
7. If the data type has any security boundaries associated with it, you will be able to select from one of the items listed under the main data type. For more information on creating data item security boundaries, see "[Setting Data Access Security Boundaries](#)" (on page 27).
8. To add the selected application permissions, click **Add**.
9. Click **Save**  (far right of lower pane) to save your changes.

Setting Data Access Security Boundaries

Data Access permissions in BSA Essentials allow you to control the types of data your users will be able to see and use inside of reports. Creating *security boundaries* around data items allows you to control the exact type of data item and the exact kinds of attributes related to the item.

Note: In this release, security boundaries are created in the BSA Essentials Java Client.

For example, if your implementation of BSA Essentials is configured to work with Server Automation (SA), you very likely want your users to be able to report on SA servers.

Granting data access permissions to SA servers and Network Automation (NA) devices is probably too general and would yield too much information in reports. You might want a specific BSA Essentials user group to be able to report on and display a specific set of servers and of those servers, only be able to see specific server attributes. To achieve this, you would create security boundaries for the Server data item.

For example, using the BSA Essentials Java Client you might only want users in a group to be able to report on SA virtual servers from a specific Customer and Facility, only list server information regarding hostname, open ports, and only those servers that yield more than five failed checks when they are scanned during a compliance audit.

Once you create the security item in the BSA Essentials Java Client, you can see the security boundary when you create a data access permission in the BSA Essentials Web Client.

In order to create security boundaries, you need to perform the tasks described in the following topics:

- ["Installing the BSA Essentials Java Client" \(on page 11\)](#)
- ["Logging In to the BSA Essentials Java Client" \(on page 13\)](#)
- ["Creating Security Boundaries" \(on page 28\)](#)

Creating Security Boundaries

From inside the BSA Essentials Java Client, you can create security boundaries around data items, which allows you to restrict the kinds of data item attributes upon which users in BSA Essentials can report.

When you create security boundaries around data items from inside the BSA Essentials Java Client, those security boundaries become available when you create *data access* permissions in the BSA Essentials Web Client and apply those permissions to user groups.

For example, you might want users in a group to be able to report only on Server Automation (SA) virtual servers from a specific Customer and Facility, and then list server information regarding only hostname and open ports, and finally restrict this information to only those servers that yield more than five failed checks when they are scanned during a compliance audit.

You could create security boundaries for each of these restrictions using the BSA Essentials Java Client, and then using the BSA Essentials Web Client, you can apply those security boundaries to a group through data access permissions.

Configuration Items and their Attributes

The following terms are important to know when setting BSA Essentials security boundaries on data items:

- **Configuration Item:** An object which can be viewed and managed with BSA Essentials. For example SA Server, Network Automation (NA) Device, SA Patch Policy, and so on.
- **Attribute:** A single property of a configuration item, the value of which describes the behavior of the item. Configuration items can have one or more attributes. For example, some of the attributes for the SA Server configuration item include hostname, life cycle, agent status, and management IP.

A custom attribute is displayed only with the data item with which it is defined. For example, a custom attribute of a Facility is not displayed when viewing a server that is a member of that facility.

Create Security Boundaries for Data Access Permissions

To create security boundaries in the BSA Essentials Java Client, perform the following steps:

1. Log in to the BSA Essentials Java Client. See ["Logging In to the BSA Essentials Java Client" \(on page 13\)](#).
2. From the **View** menu, select **BSAE Administration** → **Security Boundaries**.
3. From the Define Security Boundary around Configuration Item drop-down list, select a data item. For example, SAS Server (SA Server).
4. In the Match the following criteria section, from the drop-down lists, select an Attribute (for example, Hypervisor), an operator (equals, contains, does not contain, and so on), and parameters for the security boundary.
5. Depending upon the operator selected, you might have to enter a value, text, or select from a list of values. In the text field, type the appropriate value.
6. (Optional) Click **+** to define a second criteria. (You can create as many rules as you want.)
7. Click Preview Security Boundary to view the current items defined within the security boundary.
8. Click **Save** to save the security boundary. Once the security boundary is saved, it becomes available as a data access permission item in the BSA Essentials Web Client.

For information on how to assign data access permissions on groups in the BSA Essentials Web Client, see ["Assigning Permissions to Groups" \(on page 26\)](#).

Chapter 3

Configuring Cross Device, Policy, and Job Groups

Cross device, policy, and job groups allow you to create cross-product groupings of various devices, policies, and jobs from each of the BSA products deployed in your data center — Server Automation (SA), Network Automation (NA) and Operations Orchestration (OO) — so that you can control the information provided to you in BSA Essentials reports.

For example, you might be responsible for a high profile business application in your data center. You want to be able to report on all of the servers and devices that make up the application for the following reasons:

- To ensure that these devices meet the specific compliance criteria defined by your organization
- To see how well these devices are delivering the return on investment (ROI) you expect from the application those devices support

You can achieve this result by creating the following cross groups:

- a cross device group for all of the devices (servers, network devices, and storage devices) that make up the application
- a cross policy group that contains audits and software policy checks on the servers and devices
- a cross job group that provides job results for each compliance audit

There are three kinds of groups types in BSA Essentials:

- **"Creating Cross Device Groups" (on page 30)**: Allow you to group together devices of the BSA product suite deployed in your data center and use in reports. For example, you can use a cross device group to group servers and device groups from SA and network devices and device groups from NA.
- **"Creating Cross Policy Groups" (on page 31)**: Allow you to group together important policies from the BSA product suite deployed in your data center and use them in your reports.
- **"Creating Cross Job Groups" (on page 32)**: Allow you to group together important job types from the BSA product suite deployed in your data center and use them in your reports.



Creating Cross Device Groups

Cross device groups allow you to group together devices and device groups from both Server Automation (SA) and Network Automation (NA). Once you group together devices and device groups, these groups can be used in reports.

Create a Cross Device Group

To create a cross device group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configuration folder, select Cross Device Groups.

3. In the right side of the window, click the New Device Group  icon.
4. In the New Cross Device Group dialog, enter a name and description for the group, and then click **Save**.
5. To add items to the group, select the new group from the list.
6. Below the group, select the General and Devices and Device Groups tab.
7. Click **Add+** to add devices or device groups to the group.
8. In the Add Device/ Groups dialog, select the type of device from the Item Type drop-down list. For example, NAS Device, SAS Server Group, and so on.
9. Once the list has been populated with items, to select an item to add to the group, select the check box next to the name of the item.
10. Click **Add**. Repeat as many times as needed for all the item types you want to add to the device group.
11. When you have finished selecting items to the group, click **OK**.
12. Click **Save**  (far right of lower pane) to save your changes.


Creating Cross Policy Groups

Cross policy groups allow you to group together policies from Network Automation (NA) and Server Automation (SA). Specifically, you can combine NA Configuration Policies, SA Application Configurations, Audits, Patch Policies, and Software Policies into individual groups.

Once you create a cross policy group, it can be used in reports. For more information on creating reports, see "Creating a Report" in the *BSA Essentials User Guide*.

Create a Cross Policy Group

To create a cross policy group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configuration folder, select Cross Policy Groups.
3. In the right side of the window, click the New Policy Group  icon.
4. In the New Cross Policy Group dialog, enter a name and description for the group, and then click **Save**.
5. To add items to the group, select the new group from the list.
6. Below the group, select the Policies tab.
7. Click **Add+** to add polices to the group.
8. In the Add Policy dialog, select a policy type from Item Type drop-down list. For example, NAS Configuration Policy, SAS Application Configuration, SAS Audit, and so on.
9. Once the list has been populated with items, to select an item to add to the group, select the check box next to the name of the item.
10. Click **Add**. Repeat as many times as needed for all the item types you want to add to the

policy group.

11. When you have finished selecting items to the group, click **OK**.

Creating Cross Job Groups

Cross job groups allow you to group together important job types from the BSA product suite deployed in your data center and to use them in your reports.

For example, you can create groups and add such diverse job types as Network Automation (NA) tasks like Backup Device Software, Check Policy Compliance, Data Pruning; and Server Automation (SA) jobs like Audit Server, Remediate Software Policy, Agent Communications Test, Install Software, and so on.



Additionally, you have the ability to set a return on investment (ROI) unit for all cross job groups, which allows you to indicate the value you are getting from the jobs being run by the BSA software suite. For example, you could set the ROI unit to dollars, and when you create and configure a cross job group, you can specify a value amount for the group which will be labeled in dollars. For information on setting the cross job group ROI unit, see ["Setting Cross Job Groups ROI Unit" \(on page 33\)](#)

Note: ROI unit applies globally across all job groups, but each group can be set with a unique ROI value.

For more information on creating reports, see "Creating a Report" in the *BSA Essentials User Guide*.

Create a Job Group

To create a cross job group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configurations folder, select Cross Job Groups.
3. In the right side of the window, click the New Job Group  icon.
4. In the New Cross Job Group dialog, enter a name and description for the group, and then click **Save**.
5. Select the new group from the list, and below the group, select the General tab.
6. In the ROI Multiplier field, enter a value for the label. For example, if your global ROI unit was set to dollars, you can enter 500 for this group to indicate how much money is saved when the jobs in this group run successfully.
7. Next, to add job types to the group, select the Jobs tab and then click **Add+**.
8. In the Add Job dialog, select a job type filter, such as NAS Job Types or SAS job Types.
9. Once the list has been populated with job items, to select an item to add to the group, select the check box next to the name of the item and then click **Add**. Repeat as many times as needed for all the item types you want to add to the job group.
10. When you have finished selecting items to the group, click **OK**.
11. Click **Save**  (far right of lower pane) to save your changes.

Setting Cross Job Groups ROI Unit

Before you create and configure cross job groups, you want to set a return on investment (ROI) unit for all job groups. The cross job group ROI unit allows you to indicate the value you are getting from the jobs being run by the BSA software suite.

For example, you can set the ROI unit to dollars, and when you create and configure a cross job group, you can specify a value amount for the group, which will be labeled in dollars. Or, you might want to represent the savings created running specific jobs in time, as in how many hours were saved when a group of related jobs run successfully.

Note: ROI unit applies globally across all job groups, but each group can be set with a unique ROI value.

Set Cross Job Groups ROI Unit

To set the cross job group ROI unit, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configurations folder, select Cross Job Groups.
3. At the top of the Job Groups list, click **Set ROI Unit**.
4. In the Specify Return on Investment Unit dialog, enter the label for units to be expressed for all cross job groups. For example, you can set "dollars" or "hours" or any unit label you want.
5. Click **OK**. The ROI unit label has been set for all cross job groups. For information on how to create a cross job group and set the ROI unit value for a group, see "[Creating Cross Job Groups](#)" (on page 32).

Chapter 4

Core Server Administration

This section contains several administrative tasks that are routinely performed to ensure the proper running of your BSA Essentials Core Server. It contains the following topics:

- ["Starting and Stopping the Core Services" \(on page 35\)](#)
- ["Enabling BSA Essentials Java Client Access on SA Server" \(on page 36\)](#)
- ["Configuring Additional Memory" \(on page 36\)](#)
- ["Configuring BSA Essentials Ports" \(on page 37\)](#)
- ["Setting Up Live Content Downloads" \(on page 40\)](#)
- ["Changing the Keystore Passphrase" \(on page 40\)](#)
- ["Changing BSA Essentials Passwords" \(on page 42\)](#)
- ["Importing a Third Party SSL Certificate" \(on page 48\)](#)
- ["Viewing OMDB Versioning Information" \(on page 52\)](#)
- ["Running and Configuring SA Compliance Universe Nightly Jobs" \(on page 52\)](#)
- ["Viewing Oracle User Connectivity Diagnostics" \(on page 53\)](#)
- ["Unlocking Oracle User Accounts" \(on page 54\)](#)
- ["Purging the BSA Essentials Database" \(on page 54\)](#)
- ["Central Management Console Admin Tasks" \(on page 57\)](#)
- ["Monitoring BSA Essentials" \(on page 62\)](#)
- ["Backing Up BSA Essentials on Linux" \(on page 73\)](#)
- ["Restoring BSA Essentials on Linux" \(on page 76\)](#)

Running Scripts in a Dual Server Configuration

If you have a dual server configuration, in some cases, you will have to execute a given script on the database server. When this is necessary, it will be noted in the description of the script. The following procedure describes how to copy over the script, log in, and run the script from the database server.

To execute a script in a dual server configuration, perform the following steps:

1. Copy the script to the database server by executing the following command:

```
scp -p /opt/opsware/omdb/contrib/<script>.sh <DB_
Server>:<directory>
```

If the instructions for running the script indicate that the script must be located in a specific directory on the database server, the value of `<directory>` must be set to that location. If the directory structure does not exist on the database server, you must create it.

Ensure you set the file and directory permissions correctly when you copy files over to the database server. Also, review the scripts to ensure that required environment variables are correctly set.

2. Log in to the database server and go to location where you have copied the script.
3. Run the script following the steps specified for a single server configuration.

Starting and Stopping the Core Services

You can use the `opsware-omdb` script to start, stop, or restart your BSA Essentials core services. You can also use this script to check the current status of your core server, the core version number, and more. You must log in as root to run this script.

Location

The script is located in the following directory:

```
/etc/init.d/opsware-omdb
```

Syntax

```
opsware-omdb <option>
```

Note: If you are restarting your core services in a dual server configuration (one server runs the BSA Essentials core services and the other runs Oracle), make sure that your Oracle Database Server and all of its processes are running before restarting the BSA Essentials core services.

Options

The `opsware-omdb` script has the following command line options:

- `start` - Starts the BSA Essentials core services.
- `stop` - Stops the BSA Essentials core services.
- `startsync` - Starts the core services. The prompt is not returned until the core services are fully started.
- `restart` - Restarts the BSA Essentials core services.
- `list` - Lists the services that are run by the `opsware-omdb` script (core and rsync).
- `status` - Gives the current status of BSA Essentials services if running or not running. Also the PID of the process is displayed if the service is running.
- `version` - Displays installation build version numbers for the installed components and the Meta schema and data versions of the BSA Essentials Database.
- `help` - Lists full set of command options and syntax.

Enabling BSA Essentials Java Client Access on SA Server

If you want your SA-authenticated users to have access to the BSA Essentials Java Client on the SA Core Server, you must enable communication between the BSA Essentials Core Server and the SA Core Server by performing the following procedure:

1. On the SA Core Server, log in as root.
2. Copy the `/opt/ospware/omdb/bin/enable_omdb_client.sh` file on the BSA Essentials Core Server to the SA Core Server.
3. Run the script in the directory where you copied the file on the SA Core Server by executing the following command:

```
./enable_omdb_client.sh
```

4. Restart the twist on the SA Core Server by executing the following command:

```
/etc/init.d/ospware_sas restart twist
```

NOTE: If the SA Core Server is installed as a multiple slice configuration, the `enable_omdb_client.sh` script must be run on all slices of the SA Core Server.

5. On the BSA Essentials Core Server, log in as root.
6. Restart the BSA Essentials core services by executing the following command:

```
/etc/init.d/ospware-omdb restart core
```

Configuring Additional Memory

After you install BSA Essentials, you may determine that you need additional memory beyond the default memory setting of 8 GB (8192m), which is the recommended sizing value for a small BSA Essentials deployment. See the "Sizing Recommendations" chapter in the *BSA Essentials Installation Guide*.

Changing the Maximum Memory Setting

BSA Essentials memory settings are kept in the `omdb.sh` file located in `/opt/ospware/omdb/bin` directory. You must edit this file to change the memory setting for your deployment.

To change the maximum memory setting, perform the following steps:

1. Log in to the BSA EssentialsCore Server.
2. Stop the BSA Essentials core services and BusinessObjects reporting engine by executing the following commands:

```
/etc/init.d/ospware-omdb stop
```

```
/etc/init.d/bsae-bo stop
```

3. Open the `omdb.sh` file in a text editor.
4. Search for the string **-Xmx** in the file. It can be found under the comment header of **#JVM memory setting**. This is the setting for maximum memory. For example, the string may look like the following:

```
-Xmx8192m
```

5. Modify the value for the maximum memory setting to one that is appropriate for the size of your BSA Essentials deployment.
6. Save the edited file.
7. Start the BSA Essentials core services and BusinessObjects reporting engine by executing the following commands:

```
/etc/init.d/opsware-omdb start
```

```
/etc/init.d/bsae-bo start
```

Configuring BSA Essentials Ports

After you have installed BSA Essentials, you might need to change some of the port numbers being used by the BSA Essentials core or database. BSA Essentials configuration is retained in the `omdb.properties` file, and also in the system configuration files that are created or modified during an installation or upgrade of BSA Essentials. The following sections show you how to change port numbers for the product components.

Changing BSA Essentials Web Client Port

To change the BSA Essentials web client port, perform the following steps:

1. Log in to the BSA Essentials Core Server.
2. Select the new port number, (in our example, we are using the value 2653) and execute the `netstat` command to prove that the port is not in use as follows:

```
netstat -a | grep 2653
```

NOTE: The Linux man page for "services" states the following: Port numbers below 1024 (so-called 'low numbered' ports) can only be bound to by root (see **bind(2)**, **tcp(7)**, and **udp(7)**). This is so clients connecting to low numbered ports can trust that the service running on the port is the standard implementation and not a rogue service run by a user of the machine. Well-known port numbers specified by the IANA are normally located in this root-only space. The BSA Essentials core server runs as "omdb" so you should not select a port in this lower range.

3. Stop the data miners by performing the following tasks:
 - Open a window and log in to the data miner server.
 - Change directory to the data miner install directory.
 - Execute the following command:

```
./dataminer.sh stop
```
4. Back up the original `dataminer.conf` file for safekeeping.
5. Open the `dataminer.conf` file in a text editor and do the following:
 - Find the `CMDBLocation` parameter.
 - Change the value of this parameter to the Fully Qualified Domain Name of the BSA

Essentials core server, appending a colon (":") and the new port number at the end.

Example: `CMDBLocation=sa_svr.mycompany.com:2653`

- Save the file.

6. Shut down the BSA Essentials core services and the BusinessObjects reporting engine by executing the following commands:

```
/etc/init.d/opsware-omdb stop
```

```
/etc/init.d/bsae-bo stop
```

7. Back up the original `/opt/opsware/omdb/omdb/deploy/jboss-web.deployer/server.xml` file for safekeeping.
8. Open the `/opt/opsware/omdb/omdb/deploy/jboss-web.deployer/server.xml` file in a text editor and do the following:

- Find the comment: Define a SSL HTTP/1.1 Connector on port 8443.
- Below the comment, change the specified port in the block to the new port value.

Example:

```
<Connector port="2653" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
address="{jboss.bind.address}"
strategy="ms" maxHttpHeaderSize="8192" emptySessionPath="true"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_
RSA_WITH
_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_
WITH
_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_
3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
securityDomain="java:/jaas/RMI+SSL" clientAuth="false"
sslProtocol="TLS"
SSLImplementation="org.jboss.net.ssl.JBossImplementation" />
```

- Save the file.

9. Back up the original `/etc/opt/opsware/omdb/omdb.properties` file for safekeeping.
10. Open the `/etc/opt/opsware/omdb/omdb.properties` file in a text editor and do the following:

- Find the `com.opsware.cmbd.interview.omcs.port` setting.
- Set the new port number.

Example: `com.opsware.cmbd.interview.omcs.port=2653`

- Save the file.

11. Start the BSA Essentials core services and the BusinessObjects reporting engine by executing the following commands:

```
/etc/init.d/opsware-omdb start
```

```
/etc/init.d/bsae-bo start
```

12. View the server log file to ensure a successful start by executing the following command:

```
tail -40f /var/log/opsware/omdb/server.log
```

13. Open a window on the data miner server and restart the data miner by executing the following command:

```
./dataminer.sh start
```

14. View the data miner log file to ensure a successful start by executing the following command:

```
tail -40f dataminer.log
```

15. When the server log file indicates that all services are up and running, log in to the web client using the new port number.

Example: `https://<BSAE_core_server>:2653`

Changing BSA Essentials Database Port

By default BSA Essentials uses port 1521 to connect BSA Essentials Core services to the BSA Essentials Database. Since the BSA Essentials Database port is not set during the installation, the port number is not part of the BSA Essentials response file, and you cannot change the BSA Essentials Database port using the steps in the previous procedure.

To change the database port number used by BSA Essentials, perform the following steps:

1. Log in to the BSA Essentials Core Server.
2. To shut down the BSA Essentials core services and the BusinessObjects reporting engine, enter the following commands:

```
/etc/init.d/opsware-omdb stop
```

```
/etc/init.d/bsae-bo stop
```

3. For each of the files in the following list, open the file using a text editor, change the database port from the default value of 1521 to the required value, and save the file.

- `/etc/opt/opsware/omdb/omdb.properties`
- `/opt/opsware/omdb/bin/dmconfig.properties`
- `/opt/opsware/omdb/deploy/cmdb-aaa-ds.xml`
- `/opt/opsware/omdb/deploy/cmdb-admin-ds.xml`
- `/opt/opsware/omdb/deploy/cmdb-deployer-ds.xml`
- `/opt/opsware/omdb/deploy/cmdb-ds.xml`
- `/opt/opsware/omdb/deploy/omdb-reporter-ds.xml`

4. To start the BSA Essentials core services and the BusinessObjects reporting engine, enter the following commands:

```
/etc/init.d/opsware-omdb start
```

```
/etc/init.d/bsae-bo start
```

Setting Up Live Content Downloads

HP Live Network (HPLN) is a subscription service that enables you to obtain the most current content for BSA Essentials. This service automatically downloads and imports new content from an HP content distribution server to your BSA Essentials Server. Your BSA Essentials Server can be configured to automatically download and import new BSA Essentials 9.20-related live content into a running BSA Essentials Server without user involvement, since the live content is published on HP content distribution servers. The content that is updated includes the following:

- BusinessObjects reports
- Legacy BIRT reports
- Data miner ETL/Model updates
- BusinessObjects Universe updates

For more information about HPLN, visit the HP Live Network connector (LNC) home page at <https://h20034.www2.hp.com/>. This page contains quick links for downloading the HP LNC software and for the LNC Users Guide, which explains how to install and configure the product.

For the latest content, announcements, and forums, visit the BSA Essentials Community LNC home page at <https://h20036.www2.hp.com/>.

Changing the Keystore Passphrase

The keystore passphrase is used to protect certificates that will be used by the core platform for secure communications. Additionally, it is used to encrypt and decrypt passwords that have been configured for the system.

The default keystore passphrase for BSA Essentials is specified during installation. After the product is installed, administrators may need to change this passphrase according to internal security policies.

To change the keystore passphrase, you must use the `/opt/opsware/jdk1.6/bin/keytool` command. This command updates the keystore with the new passphrase. After you update the passphrase on the keystore, you must encrypt it and add this encrypted version to the BSA Essentials properties file.

Once you have changed your keystore passphrase, you must also re-encrypt your admin and datasource passwords and your shared secret.

The following sections explain how to perform these tasks.

Step 1: How to Change the Keystore Passphrase

To change the keystore passphrase, complete the following steps:

1. Change your directory to `/opt/opsware/jdk1.6/bin/`.
2. Execute the following three `keytool` commands as the root user:

```
./keytool -keystore /var/opt/opsware/crypto/omdb/server.keystore  
-storepass <old_passphrase>
```



```
-new <new_passphrase>
-keypasswd
-keypass <old_passphrase>
-alias omdb

./keytool -keystore /var/opt/opsware/crypto/omdb/server.keystore
-storepass <old_passphrase>
-new <new_passphrase>
-keypasswd
-keypass <old_passphrase>
-alias tomcatbo

./keytool -keystore /var/opt/opsware/crypto/omdb/server.keystore
-storepass <old_passphrase>
-new <new_passphrase>
-storepasswd
```

Note: The keystore passphrase must be at least 6 characters in length.

Step 2: How to Generate the Encrypted Keystore Passphrase

To generate the encrypted keystore passphrase, complete the following steps:

1. Change your directory to `/opt/opsware/omdb/lib`.
2. Execute the following command as the root user:

```
/opt/opsware/jdk1.6/bin/java -jar securityUtil.jar -keystore
```

3. Enter your clear text keystore passphrase at the prompt. You will have to do this twice.

The command returns the encrypted passphrase. Use this encrypted passphrase in the next procedure.

Step 3: How to Modify the BSA Essentials Properties Files

To modify the properties file, complete the following steps:

1. Open the `omdb.properties` file in a text editor. This file is located in the `/etc/opt/opsware/omdb` directory.
2. Search for the property value pair for the `com.opsware.cmdb.security.keystore.passphrase` property. It looks like the following:

```
com.opsware.cmdb.security.keystore.passphrase="<old_encrypted_
password>"
```

3. Replace the old encrypted passphrase value for the `com.opsware.cmdb.security.keystore.passphrase` property with the newly encrypted one generated in the previous procedure.

After you replace the old encrypted passphrase with the newly encrypted one, the entry looks like the following:

```
com.opsware.cmdb.security.keystore.passphrase="<new_encrypted_password>"
```

Step 4: How to Encrypt Passwords and Shared Secret

After you change your keystore passphrase, you must re-encrypt your admin and datasource passwords as described in ["Encrypting Passwords" \(on page 46\)](#) and your shared secret as described in ["Updating the Shared Secret" \(on page 60\)](#). You must perform these tasks next for your system to be functional.

Once you have completed these steps, your BSA Essentials core services should be up and running and your keystore passphrase successfully changed.

Changing BSA Essentials Passwords

The default passwords for the BSA Essentials database users are initialized during installation. After the product is installed, administrators may need to change these passwords according to internal security policies.

The following users are created during the installation process:

User	Description	Create Session
ASAS_RPT_USER	Owner of the staging area for ASAS data.	Yes
BO_ADMIN	Owner of Business Objects schema.	Yes
CMDB_AAA	Owner of the security schema used for authentication and authorization.	Yes
CMDB_ADMIN	Has full access to all CMDB database schemas for administrative purposes. Has administrative privileges on all CMDB roles.	Yes
CMDB_APPL	Provides access for applications through data access layer. Similar to CMDB_ADMIN without administrative privileges.	Yes
CMDB_CUSTOM	Owner of 'custom' reporting data schema. Has no connection privileges. May be temporarily granted the schema_admin role for schema management purposes.	No
CMDB_DATA	Owner of reporting data schema. Has no connection privileges. May be temporarily granted the schema_admin role for schema management purposes.	No
CMDB_DEPLOYER	Used by the deployer and upgrade services for adding additional content through HP LiveNetwork.	Yes
CMDB_META	Owner of metadata schema. Has no connection privileges. May be temporarily granted the schema_admin role for schema management purposes.	No
CMDB_REPORTER	Read-only access to tables and views in the cmdb_data schema.	Yes

In addition, the Oracle sys and system passwords are initialized to the same value as CMDB_ADMIN.

The following sections describe the steps the administrator must perform to change system passwords:

- ["Changing the BSA Essentials Application Level Administrator Password" \(on page 43\)](#)
- ["Changing the Oracle User Passwords" \(on page 43\)](#)
- ["Changing the BusinessObjects Administrator Password" \(on page 44\)](#)

Changing the BSA Essentials Application Level Administrator Password

If you want to change the application level administrator password, perform the following steps:

1. Access the BSA Essentials Web Client by using the following URL:
`https://<host>:<port>/bsae/`.
where *<port>* is the value for the BSA Essentials host port set during installation.
2. Log in as the administrator using the existing password.
3. Click the Administration tab in the top left of the Web Client.
4. Click the Users option under the Security group.
5. Click the admin user.
6. Click the Login tab in the middle of the Web Client window.
7. Enter the new BSA Essentials administrator password in the Password text box.
8. Enter the new password in the Confirm Password text box.
9. Click the save icon on the right side of the Web Client page.
10. Log out.

Changing the Oracle User Passwords

If you want to change the Oracle BSA Essentials user passwords, perform the following steps:

1. Stop the OMDB and BSA Essentials core services by executing the following commands:
 - `/etc/init.d/opsware-omdb stop`
 - `/etc/init.d/bsae-bo stop`
2. Log in to the BSA Essentials database using a database tool such as SQL*Plus.
3. Run the following command for each BSA Essentials database user whose password you want to change:
 - `alter user cmdb_aaa identified by <New CMDB_ADMIN password>;`
 - `alter user cmdb_admin identified by <New CMDB_ADMIN password>;`
 - `alter user cmdb_deployer identified by <New CMDB_ADMIN password>;`

- `alter user cmdb_appl identified by <New CMDB_ADMIN password>;`
 - `alter user cmdb_reporter identified by <New CMDB_ADMIN password>;`
4. Start the the OMDB and BSA Essentials core services by executing the following commands:
 - `/etc/init.d/opsware-omdb start`
 - `/etc/init.d/bsae-bo start`
 5. After changing the `cmdb_reporter` password (in the `alter user cmdb_reporter` SQL statement in the previous step), you must reset the BO password by doing the following:
 - a. As the root user, change directory to `/opt/opsware/omdb/components`.
 - b. Execute `./BOPassword.sh`. You will be prompted to do the following:
 - Enter the administrator password. The administrator password is the password to which the application level administrator password is currently set. See ["Changing the BSA Essentials Application Level Administrator Password"](#) (on page 43).
 - Enter the new `cmdb_reporter` password. The new `cmdb_reporter` password is the new password to which you changed the `cmdb_reporter` in the `alter user cmdb_reporter` SQL statement in the previous step.
 - Verify the new `cmdb_reporter` password.

Upon completion, you will see the "BO Password updated" message.
 6. After changing the Oracle user passwords, you must encrypt them following the procedure described in ["Encrypting Passwords"](#) (on page 46).

Changing the BusinessObjects Administrator Password

The BusinessObjects administrator password is another Oracle user password which is used by BusinessObjects exclusively. If you want to change the BusinessObjects administrator password, perform the following steps:

1. Stop the OMDB and BSA Essentials core services by executing the following commands:
 - `/etc/init.d/opsware-omdb stop`
 - `/etc/init.d/bsae-bo stop`
2. Log in to the BSA Essentials database server using a database tool such as SQL*Plus.
3. Run the following command:

```
alter user bo_admin identified by <New CMDB_ADMIN password>;
```
4. On the BSA Essentials core server, change to the oracle user by executing the following:

```
su - oracle
```
5. On the BSA Essentials core server, execute the following command:

```
/opt/opsware/omdb/bo/bobje/cmsdbsetup.sh
```

 - a. The first screen asks for the Server Intelligence Agent. Type **bsae**, and press Enter.
 - b. The next screen asks what you want to do with the Server Intelligence Agent. (You will get

errors on this screen that it is unable to connect to the database. These are benign errors, as BusinessObjects was stopped in an earlier step. This does not affect the working of the script.) The default is **update**. Press Enter to continue.

- c. The next screen is essentially a warning message that you should only update datasources for this cluster. Type **yes**, and press Enter to continue.
- d. The next screen asks for the database connection type. The default is **Oracle**. Press Enter to continue.
- e. The next screen asks for the tnsname. Enter **bsaedb**, (or your tnsname if you have a custom installation), and press Enter to continue.
- f. The next screen asks for the user name to connect to the database. The default is **bo_admin**. Press Enter to continue.
- g. The next screen asks for the bo_admin password. Enter the new CMDB_ADMIN password, and press Enter to continue.

NOTE: The key strokes will not show on the screen, and there is no confirmation – so be very careful!

- h. Type **exit**, and press Enter to return to a root session.
6. Start the the OMDB and BSA Essentials core services by executing the following commands:
 - `/etc/init.d/opsware-omdb start`
 - `/etc/init.d/bsae-bo start`

Resetting the BSA Essentials Application Level Administrator Password

You can use the `reset_admin_password.sh` script to reset the password for the BSA Essentials application level administrator back to the original password for this user. The user name for application level administrator is **admin**. The original password for the application level administrator user is also **admin**. You will need to use this script if you do not know or have lost the password for the application level administrator.

After resetting the application level administrator's password back to the original value of **admin**, you can use this value for the password credential in step 7 of the procedure below where it indicates how you log in to the BSA Essentials Web Client as the **admin** user and then change the password to a more secure value.

Note: If you have a dual server configuration, you must copy this script to the database server and execute it from there. See "[Running Scripts in a Dual Server Configuration](#)" (on page 34). After running the script on the database server, you must perform the steps in the following procedure on the core server to properly reset the password.

Syntax

```
./reset_admin_password.sh
```

After you execute the script, follow the steps provided in its output on the core server.

How to Use the Script

1. Log in to the BSA Essentials Core Server.
 2. Change your directory to the following path:

```
/opt/opsware/omdb/contrib
```
 3. Execute the following command:

```
./reset_admin_password.sh
```
 4. Edit the `/etc/opt/opsware/omdb/omdb.properties` file and add the following parameter:

```
com.opsware.cmdb.security.allow_internal_user_modification_enabled=true
```
 5. Restart the BSA Essentials core services by executing the following command:

```
/etc/init.d/opsware-omdb restart
```

Wait for the BSA Essentials system to start completely.
 6. Edit the `/etc/opt/opsware/omdb/omdb.properties` file and set the following property back to the original value:

```
com.opsware.cmdb.security.allow_internal_user_modification_enabled=false
```
 7. Log in to BSA Essentials Web Client as the **admin** user with the original password value of **admin** and change the password as described in ["Changing the BSA Essentials Application Level Administrator Password" \(on page 43\)](#).
- Tip:** To use a SID other than the default "cmdb", define and export the `ORACLE_SID` variable before running this script as follows:
- `export ORACLE_SID=mycmdbsid;`
 - `./reset_admin_password.sh`

Encrypting Passwords

You will need to re-encrypt your admin and/or datasource passwords if you have done one of the following:

- Changed the password for your datasources as described in ["Changing the Oracle User Passwords" \(on page 43\)](#).
- Changed the admin password as described in ["Changing the BSA Essentials Application Level Administrator Password" \(on page 43\)](#).
- Changed your keystore passphrase as described in ["Changing the Keystore Passphrase" \(on page 40\)](#).

An executable jar file has been provided that allows you to generate an encrypted password. If you change your datasource passwords, you must specify the newly encrypted password in the login configuration file. If you change your admin password, you must specify the newly encrypted password in the admin password file.

The steps are explained in the following procedures.

Step 1: How to Generate an Encrypted Datasource or Admin Password

To generate an encrypted password for the datasource or the admin user, complete the following steps:

1. Change your directory to `/opt/opsware/omdb/lib`.
2. Execute the following command as the root user:

```
/opt/opsware/jdk1.6/bin/java -jar securityUtil.jar
```

3. Enter the clear text password for the datasource user or the admin user (depending on the password you want to encrypt) at the prompt. You will have to do this twice.

The command returns the encrypted password. Use this encrypted password in the procedure for modifying the login configuration file (for datasource user) or the admin password file (for admin user).

Step 2: How to Stop the BSA Essentials Core Services

To ensure that the OMDB and BSA Essentials core services are not running, execute the following commands:

- `/etc/init.d/opsware-omdb stop`
- `/etc/init.d/bsae-bo stop`

Step 3 for Datasource Passwords: How to Modify the Login Configuration File

To modify the login configuration file, complete the following steps:

1. Open the `login-config.xml` file in a text editor. This file is located in the `/opt/opsware/omdb/omdb/conf` directory.
2. Search for the `application-policy` xml-elements in this file that have any of the following name attributes:
 - `cmdbAdminDS`
 - `cmdbDeployerDS`
 - `cmdbDS`
 - `omdbReporterDS`
 - `cmdbAAADS`

For example, an application policy in `login-config.xml` for `omdbReporterDS` looks like the following:

```
<application-policy name="omdbReporterDS">
  <authentication>
    <login-module
code="org.jboss.resource.security.BSAELoginModule" flag="required">
      <module-option name="username">cmdb_reporter</module-
option>
      <module-option name="password">old_encrypted_
password</module-option>
      <module-option name="managedConnectionFactoryName">
```

```

        jboss.jca:service=LocalTxCM,name=omdbReporterDS</module-
option>
    </login-module>
</authentication>
</application-policy>

```

3. Replace the old encrypted password in `module-option name="password"` for the relevant application policy with the newly encrypted one generated in the previous procedure. You will have to do this for each application policy named in the preceding step.

After you replace the old encrypted password with the newly encrypted one, the entry looks like the following:

```

<application-policy name="omdbReporterDS">
  <authentication>
    <login-module
code="org.jboss.resource.security.BSAELoginModule" flag="required">
      <module-option name="username">cmdb_reporter</module-option>
      <module-option name="password">new_encrypted_password</module-
option>
      <module-option name="managedConnectionFactoryName">
        jboss.jca:service=LocalTxCM,name=omdbReporterDS</module-
option>
    </login-module>
  </authentication>
</application-policy>

```

Step 3 for Admin Password: How to Modify the Admin Password File

To modify the admin password file, complete the following steps:

1. Open the `adminpwd` file in a text editor. This file is located in the `/var/opt/opsware/crypto/omdb` directory.
2. Replace the existing encrypted password with the newly encrypted admin password.

Step 4: How to Start the BSA Essentials Core Services

To start the BSAE core services, execute the following commands:

- `/etc/init.d/opsware-omdb start`
- `/etc/init.d/bsae-bo start`

Importing a Third Party SSL Certificate

This section describes how you can import a third party SSL certificate on 9.20 BSA Essentials servers. It covers the following topics:

- ["Third Party Certificate Criteria" \(on page 49\)](#)
- ["How to Import the Third Party Certificate" \(on page 49\)](#)

Note: A description of how to request the third party certificate from a commercial authentication service is outside the scope of this guide.

It is recommended that you have a system backup before importing the certificate.

Third Party Certificate Criteria

The third party certificate must satisfy the following criteria:

1. You will need to import both the private key and signed certificate into the `server.keystore` of the BSA Essentials server.
2. Both must be in Privacy-Enhanced Mail (PEM) format. For example:

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBANNflBxHwr9vhaLW
.....
1AGE1D4atW2dwQ==
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGPjCCBaegAwIBAgIQCotArl9hwWm41yD8DAH1ITANBgkqhkiG9w0BAQUFADCB
.....
WADcFZ5Ui0K73Ax3CKATpAQc
-----END CERTIFICATE-----
```

3. If the private key is encrypted, that is, the contents of the private key is bracketed with "BEGIN RSA PRIVATE KEY" and "END RSA PRIVATE KEY", you must change its format to remove the RSA before it can be imported. This can be done by executing the following command:

```
/opt/opsware/bin/openssl pkcs8
-topk8 -nocrypt -in <pkey in>.pem
-inform PEM -out <pkey out>.pem
-outform PEM
```

4. You will need the crypto password that was specified when BSA Essentials was installed to import the certificate.

How to Import the Third Party Certificate

To import the third party certificate, perform the following steps:

1. Place the two certificates you want to import in a temporary location, for example, `/var/tmp`.
2. Stop all running BSA Essentials data miners. Log in to each system where a data miner is installed and do the following:

- a. Change to the directory where the data miner is installed. For example:

```
cd /opt/opsware/dataminer
```

- b. Stop the data miner by executing the following command:

```
./dataminer.sh stop
```

3. Have all data miners complete any pending file transfers. On each system where a data miner is installed, execute the following commands:

- a. Change to the directory to where the data miner is installed. For example:

```
cd /opt/opsware/dataminer
```

- b. Complete any pending file transfers as follows:

```
./dataminer.sh start --flushdatafiles ; tail -f dataminer.log
```

When all pending files are successfully transferred, the log file will record "All existing files transferred to server. Exiting..." and the data miner will automatically exit.

4. On the server, wait for the any pending data to load by checking the `/var/log/opsware/omdb/server.log` file to see if any data is being processed. Make sure no failure has occurred by executing a `"find /var/opt/opsware/omdb/collect"`. Unless the flag is set to keep data files, there should be zero files found.

5. Stop BSA Essentials services on the server by executing the following commands:

```
/etc/init.d/opsware-omdb stop
```

```
/etc/init.d/bsae-bo stop
```

6. Backup the current `server.keystore` and `dmboot.pem` files on the server by executing the following commands:

```
cd /var/opt/opsware/crypto/omdb
```

```
cp server.keystore server.keystore_save
```

```
cd /opt/opsware/omdb/dist
```

```
mv dmboot.pem dmboot.pem_save
```

Note: The existing `server.keystore` will have the omdb entry replaced with the third party certificate when it is imported. All other certificates in the file will be maintained. The `dmboot.pem` file will need to be regenerated, which is why the current one is moved instead of copied to `dmboot.pem_save`.

7. Import the third party certificate on the server by executing the following commands:

Note: To properly execute these commands, you must enter each one on a single line.

- a. Change directory to the temporary location. For example:

```
cd /var/tmp
```

- b. Execute the tool that will import the certificates as follows:

```
/opt/opsware/jdk1.6/bin/java -jar  
/opt/opsware/omdb/bin/certimport.jar  
<private key>.pem  
<signed certificate>.pem  
/var/opt/opsware/crypto/omdb/server.keystore  
<crypto password>
```

- c. Regenerate the `dmboot.pem` file from the imported certificate by executing the following commands:

```
cd /opt/opsware/omdb/dist
```

```
/opt/opsware/jdk1.6/bin/keytool -export -rfc -alias omdb
```

```
-keystore /var/opt/opsware/crypto/omdb/server.keystore
-storepass <crypto password>
-file dmboot.pem

chown omdb:omdb dmboot.pem
```

8. On the BSA Essentials server, reset all of the registered data miners by executing the following commands:

- a. Change directory as follows:

```
cd /opt/opsware/omdb/bin
```

- b. List the registered data miners to determine their names as follows:

```
./dmconfig.sh -list
```

- c. Reset each registered data miner as follows:

```
./dmconfig.sh -reset -name <registered Data Miner name>
```

9. Start BSA Essentials services on the server by executing the following commands:

```
/etc/init.d/bsae-bo start
```

```
/etc/init.d/opsware-omdb start
```

10. Log into each system where a data miner is installed and execute the following commands:

- a. Change to the directory where the data miner is installed. For example:

```
cd /opt/opsware/dataminer
```

- b. Save the current data miner keystore as follows:

```
mv dataminer.keystore dataminer.keystore_save
```

- c. Replace the `dmboot.pem` file with the one that was generated on the BSA Essentials server after saving the current one by executing the following commands:

```
mv dmboot.pem dmboot.pem_save
```

```
scp root@<BSAE server>:/opt/opsware/omdb/dist/dmboot.pem
dmboot.pem
```

```
chown root:root dmboot.pem
```

- d. Start the data miner by executing the following command:

```
./dataminer.sh start
```

The data miner should successfully connect and you should see that it has registered with the BSA Essentials server.

- e. You can verify the data miner successfully registered by executing the following commands on the BSA Essentials server:

```
cd /opt/opsware/omdb/bin
```

```
./dmconfig.sh -list
```

The active flag (set to 0 by the reset done previously) should now be set to 1.

Viewing OMDB Versioning Information

You can use the `omdbver.sh` script to see the version of BSA Essentials core services that you have installed on your system.

Location

This script is located on the BSA Essentials Core Server in the `/opt/opsware/omdb/bin` directory.

How to Use the Script

```
./omdbver.sh
```

Script Output

```
Currently installed software of interest to OMDB:
```

```
OMDB Core Services      : 9.2.0
```

Running and Configuring SA Compliance Universe Nightly Jobs

You can use the following scripts to understand, troubleshoot, and modify the regularly scheduled Server Automation (SA) compliance fact table calculation used in the SA Compliance Universe.

- `bsae_run_nightly_job.sh` - allows you to view current SA Compliance data in your reports that have not yet been picked up by the latest table calculations.
- `bsae_set_max_fact_days.sh` - allows you to change how many days worth of calculated SA compliance data that the BSA Essentials database can store. The default is 30 days.

Note: If you have a dual server configuration, you must copy each script to the database server and execute it from there. In addition, you must copy the `bsae_nightly_job.sql` SQL script to the database server for the `bsae_run_nightly_job.sh` shell script to execute correctly. The shell and SQL scripts must be copied to the `/opt/opsware/omdb/contrib` directory on the database server. See "[Running Scripts in a Dual Server Configuration](#)" (on [page 34](#)).

Location

These scripts are located on the BSA Essentials Core Server in the `/opt/opsware/omdb/contrib` directory.

Note: Make sure that you do *not* use the script named `bsae_setup_nightly_compliance_job.sh`.

Running Nightly Fact Table Calculation Job

BSA Essentials stores calculated SA compliance data for 30 days. By the default, the calculation job is run at midnight daily. However, if you have made some compliance data changes in SA, and you want these changes to be reflected in the compliance reports that are built from the SA Compliance Universe, you need to invoke the calculation job in order to see the changes before the following day when the job is run at midnight.

The `bsae_run_nightly_job.sh` script will do the calculation for SA compliance data for a specific number of days depending on the input.

For example:

```
/opt/opsware/omdb/contrib/bsae_run_nightly_job.sh
```

Setting Maximum Number of Days Compliance Data is Stored

Also by default, the BSA Essentials job stores no more than 30 days of calculated compliance data, which means that SA compliance reports that use data from the SA Compliance Universe can only display 30 days of history. So if you want to report on data for more than 30 days, you can run `bsae_set_max_fact_days.sh` to configure the number of days that BSA Essentials will store calculated compliance data.

For example, if you want to set the maximum number days of stored data to 60 days, and you already have more than 60 days worth of SA data mined into BSA Essentials, you can run the `bsae_set_max_fact_days.sh` to increase the number to 60 by performing the following steps:

1. Change your directory to the following location:

```
/opt/opsware/omdb/contrib
```

2. Execute the following script:

```
./bsae_set_max_fact_days.sh 60
```

3. Run the calculation from the past 30 days to the past 60 days, since by default, you will have the history for the past 30 days:

```
./bsae_run_nightly_job.sh 30 60
```

4. Alternatively, run this command;

```
./bsae_run_nightly_job.sh 60
```

The script will calculate for the past 60 days.

Viewing Oracle User Connectivity Diagnostics

You can use the `test_datasource_accounts.sh` script to validate that your BSA Essentials users can log in and have the appropriate permissions, as defined in their user profiles.

Note: If you have a dual server configuration, you must copy this script to the database server and execute it from there. See "[Running Scripts in a Dual Server Configuration](#)" (on page 34).

Location

This script is located on the BSA Essentials Core Server in the `/opt/opsware/omdb/contrib` directory.

Syntax

```
./test_datasource_accounts.sh
```

How to Use the Script

1. Change directory to `/opt/opsware/omdb/contrib`.
2. Execute the following command:

```
./opt/opsware/omdb/contrib
```

3. At the prompt, enter the password for `<cmdb_appl>`.
4. At the following prompt, enter the password for `<cmdb_reporter>`.

The script outputs connectivity information for the `cmdb_appl` and `cmdb_reporter` accounts.

Unlocking Oracle User Accounts

You can use the `unlock_oracle_accounts.sh` script to unlock the user accounts if the locking event should occur.

For example, by default a user with an Oracle account will be locked out after 10 unsuccessful login attempts. This script allows you to reset the account so the user can log in to BSA Essentials.

You can discover which accounts are locked by examining the `DBA_USER` table. The following is an example of an SQL query that displays account status:

```
SQL> SELECT USERNAME, ACCOUNT_STATUS, to_char(LOCK_DATE, 'MM-DD-YYYY  
HH24:Mi:SS') as LOCK_DATE FROM DBA_USERS;
```

Note: If you have a dual server configuration, you must copy this script to the database server and execute it from there. See ["Running Scripts in a Dual Server Configuration" \(on page 34\)](#).

Location

This script is located on the BSA Essentials Core Server in the `/opt/opsware/omdb/contrib` directory.

How to Use the Script

You must run this script as **root**, and the `ORACLE_HOME` and `ORACLE_SID` environment variables must have been defined and exported in the **root** user's environment.

To execute the script, run the following command:

```
./unlock_oracle_accounts.sh
```

Tip: To use a SID other than the default `cmdb`, redefine and export the `ORACLE_SID` variable before running this script.

Finally, you must restart the BSA Essentials core services and the BusinessObjects reporting engine in order for the changes to take effect. To restart them, perform the following commands:

```
# /etc/init.d/opsware-omdb stop  
# /etc/init.d/bsae-bo stop  
# /etc/init.d/opsware-omdb start  
# /etc/init.d/bsae-bo start
```

Purging the BSA Essentials Database

You can use the following two scripts to purge your BSA Essentials database of old or unneeded data and tables enabling your core server to run more efficiently.

- `delete_datatables.sql`
- `purge_sar_data.sh`

Use these two scripts to do the following tasks:

- Purge all data from `cmdb_data` and the related `cmdb_meta` data tables for a given data source
Or
- Purge all data from `cmdb_data` and the related `cmdb_meta` data tables for a given data source if the data is longer than X number of days in the database.

Note: You can only purge data from the database on a per-data source basis. In other words, if you are running a Server Automation (SA) data miner and a Network Automation (NA) data miner, you need to run the scripts for each data source. For more information about stopping and starting data miners, see the *BSA Essentials Installation Guide*.

Note: This script is designed to run on a single server configuration only.

Location

These two scripts are located on your BSA Essentials Core Server in the `/opt/opsware/omdb/contrib` directory.

How to Use the Scripts

Purging All Data from Your BSA Essentials Database

1. Log in to the BSA Essentials Core Server as root.
2. Copy the two scripts `delete_datatables.sql` and `purge_sar_data.sh` from:

```
/opt/opsware/omdb/contrib
```

to

```
/opt/opsware/omdb/bin
```

3. Set the following permissions for the two scripts:

```
chmod o+rx delete_datatables.sql
```

```
chmod u+rx purge_sar_data.sh
```

4. Stop the data miner of the data source type you want to purge from the database. (For information on how to stop a data miner, see the *BSA Essentials Installation Guide*).
5. Run the purge script (as root, the only user that has the permission to run the script) by executing the following command:

```
/opt/opsware/omdb/bin/purge_sar_data.sh
```

6. Answer the questions of the script interview:

Specify a data source from (SAS, ASAS, NAS, PAS, CA, SE) where you want the data to be purged.

[Type the name of one of the listed data sources from which you want to purge data.]

7. What is the maximum days that you want to keep the data in the database?
[Type 0 to purge all data.]
8. What is the desired ORACLE_SID?
[Enter the default cmdb, unless you are using a different SID]
9. Are you sure that you want to purge all SAR data?
[Type y to purge all data of the selected data source from the database.]
10. After the data is purged, answer the following interview question:
Do you want to remove all data files in collect received directory? (y/n)
[Type y to remove all data files in collect received directory, otherwise type n.]
11. When the interview is finished, start the BSA Essentials core services by executing the following command:

```
/etc/init.d/opsware-omdb start
```
12. Delete the `DMSSettingsCache.properties` and all `*.ser` data miner files located in the directory where the data miner was un-tarred.
13. Restart the data miner.

Purging All Data from Your BSA Essentials Database After X Days

1. Log in to the BSA Essentials Core Server as root.
2. Copy the two scripts `delete_datatables.sql` and `purge_sar_data.sh` from:

```
/opt/opsware/omdb/contrib
```


to

```
/opt/opsware/omdb/bin
```
3. Set the following permissions for the two scripts:

```
chmod o+rx delete_datatables.sql
```



```
chmod u+rx purge_sar_data.sh
```
4. Run the purge script (as root, the only user that has the permission to run the script) by executing the following command:

```
/opt/opsware/omdb/bin/purge_sar_data.sh
```
5. Answer the questions of the script interview:
Specify a data source from (SAS, ASAS, NAS, PAS, CA, SE) where you want the data to be purged:
[Choose a data source by entering the name from the list.]
6. What is the maximum days that you want to keep the data in the database?
[Select any numerical value except zero - zero means purge all data. This indicates the number

of days the data will be stored in the database.]

7. What is the desired ORACLE_SID?

[Type the name of the Oracle SID. The default is cmdb.]

8. Are you sure that you want to purge all SAR data?

[Enter y for yes, n for no.]

9. When the script finished, start the BSA Essentials core services by executing the following script:

```
/etc/init.d/opsware-omdb start
```

Notes

1. In the case of purging data longer than X days, these scripts only purge `historical` and `historical_full` tables in `cmdb_data`. Those `historical` and `historical_full` tables have common columns, namely, `begin_date` and `end_date`. The row will be purged if `end_date` is less than `sysdate - x` days for a given data source. In addition, data from `cmdb_meta.item_loads`, `cmdb_meta.table_loads`, and `cmdb_meta.data_loads` are purged accordingly if `cmdb_meta.data_loads.begin_date` is less than `sysdate - x` days.
2. The purge script does not delete "updatable" data (for example, all past PAS/OO runs and runsteps will be kept, since that data is updatable).
3. Under no conditions will the scripts delete data files from `collect/failures`. If it is desired to remove these files, it must be done manually.

Central Management Console Admin Tasks

The BusinessObjects Enterprise Central Management Console (CMC) is a web-based tool that enables you to perform basic administrative tasks for the reporting panel in the BSA Essentials Web Client. These tasks include setting or changing the mail server, scheduling reports, and configuring report publication and publishing.

This section contains the following tasks:

- ["Starting and Stopping the Tomcat Server" \(on page 57\)](#)
- ["Configuring the Reporting Mail Server" \(on page 58\)](#)
- ["Setting the Default Path for Saved Files on the Core Server" \(on page 59\)](#)
- ["Updating the Shared Secret" \(on page 60\)](#)

For more information on these topics and using the CMC console for administration, see the *BusinessObjects Enterprise Administrator's Guide*.

Starting and Stopping the Tomcat Server

Before you can access the Central Management Console (CMC), you need to start the Tomcat Server where you installed the BSA Essentials core services.

Once you start the Tomcat Server, you can then log in to the CMC and perform your administrative tasks. As soon as you finished with your CMC tasks, you need to log back in to the BSA Essentials Core Server and stop the Tomcat Server as indicated in the following task.

Starting and Stopping the BSA Essentials Tomcat Server

1. Log in to the BSA Essentials Core Server.
2. Execute the following command to start the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat start
```

You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat Server as indicated in the next step.

3. Execute the following command to stop the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat stop
```

4. Exit the shell.

Configuring the Reporting Mail Server

This task shows you how to configure a mail server for the BSA Essentials reporting feature.

Configuring a Reporting Mail Server

1. Log in to the BSA Essentials Core Server.
2. Execute the following command to start the Tomcat Server:

```
/etc/init.d/bsae-tomcat start
```

You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat server as indicated in the last step of this task.

3. Access the CMC at the following URL:

```
http://<BSA_Essentials_server>:8080/CmcApp
```

4. Log in as administrator. The password is the same as the admin user for the BSA Essentials Web Client.
5. From the Organize column, select Servers.
6. Select bsae.AdaptiveJobServer.
7. From the **Manage** menu, select **Properties**.
8. From the left column list, select **Destination**.
9. In the Destination drop-down list, select **Email**.
10. Click **Add**.
11. Enter the Domain Name, Host and Port information.
12. Select the authentication method and authentication information if required by your mail server.
13. Click **Save**.
14. From the Organize column, select Servers.
15. Select bsae.DestinationJobServer.
16. From the **Manage** menu, select **Properties**.

17. From the left column list, select **Destination**.
18. In the Destination drop-down list, select **Email**.
19. Click **Add**.
20. Enter the Domain Name, Host and Port information.
21. Select the authentication method and authentication information if required by your mail server.
22. Click **Save** and close CMC.
23. Return to the BSA Essentials Core Server and log in.
24. Execute the following command to stop the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat stop
```

Setting the Default Path for Saved Files on the Core Server

If you want to set a default file path on the BSA Essentials Core Server for saving reports, you can use the Central Management Console (CMC) to configure this path on your core.

Setting Default Path for Save Files on the Core

1. Log in to the BSA Essentials Core Server.
2. Execute the following command to start the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat start
```

You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat server as indicated in the last step of this task.

3. Access the CMC by using the following URL:

```
http://<BSA_Essentials_server>:8080/CmcApp
```
4. Log in as administrator. The password is the same as the admin user for the BSA Essentials Web Client.
5. From the Organize column, select Servers.
6. Select bsae.AdaptiveJobServer.
7. From the **Manage** menu, select **Properties**.
8. In the Destination drop-down list, select File System.
9. Click **Add**.
10. Enter the path name on the Core Server in the Directory field.
11. For a username and password, it is recommended to leave these fields blank, in which case the CMC will use the BSA Essentials Admin user.
12. Click **Save** and close the CMC.
13. Return to the BSA Essentials Core Server and log in.
14. Execute the following command to stop the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat stop
```

Updating the Shared Secret

BSA Essentials implements BusinessObjects Trusted Authentication by using a shared secret. If you need to encrypt the shared secret because you have changed your keystore passphrase, you must update this value in the BusinessObjects Enterprise Central Management Console (CMC). This updated shared secret is the value you pass to the encryption tool. The encrypted shared secret that is generated must be stored in the `/var/opt/opsware/bo/sharedsecret` file.

The following procedures explain how to perform these tasks.

Updating the BusinessObjects Shared Secret

1. Log in to the BSA Essentials Core Server.
2. Execute the following command to start the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat start
```

You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat server as indicated in the last step of this task.

3. Access the CMC by using the following URL:

```
http://<BSA_Essentials_server>:8080/CmcApp
```
4. Log in with user name **Administrator**. The password is the same as the admin user for the BSA Essentials Web Client.
5. In the drop-down menu, select **Authentication**.
6. Double-click **Enterprise**. Under Trusted Authentication, the **Trusted Authentication is enabled** checkbox should already be enabled.
7. Type the updated shared secret in the **Shared secret** field on the Enterprise page.
8. Click **Update** to update the shared secret.
9. Execute the following command to stop the BSA Essentials Tomcat Server:

```
/etc/init.d/bsae-tomcat stop
```

Encrypting the Shared Secret

To generate an encrypted shared secret, complete the following steps:

1. Change your directory to `/opt/opsware/omdb/lib`.
2. Execute the following command as the root user:

```
/opt/opsware/jdk1.6/bin/java -jar securityUtil.jar
```
3. Enter your clear text shared secret that you updated in the CMC at the prompt. You will have to do this twice.

The command returns the encrypted shared secret. Use this encrypted shared secret in the next procedure.

Editing the Shared Secret File

To modify the shared secret file, complete the following steps:

1. Open the `sharedsecret` file in a text editor. This file is located in the `/var/opt/opsware/bo` directory.
2. Replace the encrypted share secret in this file with the newly generated shared secret.

Restarting the BSA Essentials Core Services

To restart the BSA Essentials core services, complete the following steps:

- `/etc/init.d/opsware-omdb stop`
- `/etc/init.d/bsae-bo stop`
- `/etc/init.d/opsware-omdb start`
- `/etc/init.d/bsae-bo start`

Monitoring BSA Essentials

Monitoring your BSA Essentials servers and processes can help you avoid problems because you can act on early warning signs and you can catch problems quickly if they do occur. You can use the monitoring tool provided, or you can use your own tools to monitor your core server, database, and data miners.

- ["Monitoring with BSA Essentials Tool" \(on page 62\)](#)
- ["Integrating with Internal Tools" \(on page 69\)](#)

Monitoring with BSA Essentials Tool

The BSA Essentials monitoring tool is a collection of scripts created to help you monitor the health of your BSA Essentials installation. The scripts provide three types of monitoring:

- Core server
- Data miner
- Database

These scripts require Java 1.4 or later. The Java classes are called from shell scripts, so you can use a scheduling utility such as cron to run them.

Each script can write an alert file and send a notification email if it encounters a potential problem, and these are configured in the settings file. For example, one of the scripts monitors available disk space, and when the available disk space falls below the value configured in the file, an alert can be written to a file and an email can be sent to one or more addresses.

Installing the Monitoring Tool

The monitoring tool should be installed on your core server, database server, and the servers where you have data miners that you want to monitor.

You must have Java installed on each server where you set up these scripts. The JRE installed with BSA Essentials, Server Automation, or Network Automation will work with the monitoring tool.

To set up the monitoring component, perform the following steps:

1. Log in as root on the server where you want to install the monitoring component.
2. Create a directory for the monitoring component:

```
# mkdir -p /opt/opsware/omdb/contrib/healthcheck/monitor
```
3. Change directories to the directory you just created.
4. Copy the file `bsae-healthcheck-bin.tar.gz` from the BSA Essentials installation media to the current directory.
5. Uncompress the contents of `bsae-healthcheck-bin.tar.gz`:

```
# gunzip bsae-healthcheck-bin.tar.gz
```
6. Extract the files for the monitoring component:

```
# tar -xvf bsae-healthcheck-bin.tar
```

- Review the script configuration settings in the `/opt/opsware/omdb/contrib/healthcheck/monitor/bsae-healthcheck/bin/conf/conf.properties` file and change them according to your preferences. See ["Configuring the Monitoring Scripts" \(on page 63\)](#).

Configuring the Monitoring Scripts

You can configure the monitoring component by modifying the following file:

```
/opt/opsware/omdb/contrib/healthcheck/monitor/bsae-healthcheck/bin/conf/conf.properties
```

Note: In the case of a dual server installation, the default directory location for the log files (namely, `/var/log/opsware/omdb`) may not exist. For the database monitoring scripts to work correctly, ensure that the directory specified for the `monitoring.alert_file_directory` property exists and has the proper permissions.

These properties determine the threshold conditions for the test scripts. You should review these settings periodically and adjust them to fit your current needs.

General Settings

Property and Description	Default Value
<code>monitoring.id</code> A name that you can use to help identify the type of monitoring that this configuration file is used with. Example names are <code>test_database</code> , <code>production_database</code> , <code>dataminer_xyz</code> , etc.	<code>prod_core</code>
<code>monitoring.save_alerts_to_file</code> Set this value to <code>true</code> if you want the monitoring failure notifications to be logged in a text file.	<code>true</code>
<code>monitoring.alert_file_directory</code> The directory where alert text files are created when <code>monitoring.save_alerts_to_file</code> is set to <code>true</code> .	<code>/var/log/opsware/omdb</code>
<code>monitoring.send_alerts_in_email</code> Set this value to <code>true</code> if you want the monitoring failure notifications to be sent by email.	<code>false</code>
<code>monitoring.alert_email_addresses</code> The list of email addresses to which to send alerts if <code>monitoring.alert_email_addresses</code> is set to <code>true</code> . You can separate email addresses with commas, semi-colons, or blank spaces.	<code>bsae_admin@company.com</code>
<code>monitoring.sender_email_address</code> The sender email address to use when sending alerts by email if <code>monitoring.alert_email_addresses</code> is set to <code>true</code> .	<code>bsae_monitor@company.com</code>
<code>monitoring.sender_username</code> The sender user name to use if the mail server requires a user name and password and if <code>monitoring.alert_email_addresses</code> is set to <code>true</code> .	<code>username</code>
<code>monitoring.sender_password</code>	<code>password</code>

Property and Description	Default Value
The sender password to use if the mail server requires user name and password and if <code>monitoring.alert_email_addresses</code> is set to true.	
<code>monitoring.smtp_provider</code> The value determines whether secured or unsecured SMTP is used. Set to <code>monitoring.unsecure_smtp</code> to use unsecure SMTP or <code>monitoring.secure_smtp</code> to use secure SMTP.	<code>monitoring.unsecure_smtp</code>
<code>monitoring.unsecure_smtp.hostname</code> The fully qualified domain name of the SMTP server.	<code>monitoring.unsecure_smtp</code>
<code>monitoring.unsecure_smtp.port</code> The port number of the SMTP server.	25

Settings for Core Server Monitoring

Property and Description	Default Value
<code>DiskSpaceOnCoreModule.byte_threshold</code> The expected amount of usable disk space (in megabytes) for <code>/var/opt/opsware/omdb/collect</code> . An alert will be triggered if the usable disk space is less than the value.	100
<code>ReceivedDirOnCoreModule.file_threshold</code> The highest expected number of files in <code>/var/opt/opsware/omdb/collect/received</code> . An alert will be triggered if the number of files exceeds the value.	100
<code>FailuresDirOnCoreModule.file_threshold</code> The highest expected number of files in <code>/var/opt/opsware/omdb/collect/failures</code> . An alert will be triggered if the number of files exceeds the value.	0
<code>BOProcessesOnCoreModule.Process_threshold</code> The lowest expected number of processes running for Business Objects. An alert will be triggered if the number of processes is lower than the value	10
<code>RsyncProcessOnCoreModule.Process_threshold</code> The lowest expected number of processes running as rsync. An alert will be triggered if the number of processes is lower than the value.	1
<code>JBossProcessOnCoreModule.Process_threshold</code> The lowest expected number of processes running as JBoss Application Server. An alert will be triggered if the number of processes is lower than the value.	1

Settings for Database Monitoring

Property and Description	Default Value
<code>DiskSpaceOnDBModule.Orau02Path</code> The directory where <code>cmdb</code> database files for Oracle's second data directory is	<code>/u02/oradata/cmdb</code>

Property and Description	Default Value
located. This directory is configured during installation.	
<code>DiskSpaceOnDBModule.byte_threshold</code> The expected amount of usable disk space (in megabytes) where the cmdb database files are kept under Oracle's second data directory. An alert will be triggered if the amount of disk space is less than the value.	100
<code>OraPMONProcessOnDBModule.Process_threshold</code> The lowest expected number of processes running as Oracle pmon.	1
<code>OraListenerProcessOnDBModule.Process_threshold</code> The lowest expected number of processes running as Oracle listener.	1
<code>OraListenerPortOnDBModule.Port</code> The port used by the Oracle listener.	1521

Settings for Data Miner Monitoring

Property and Description	Default Value
<code>DataMinerPath</code> The directory where the data miner is installed.	<code>/opt/opsware/dataminer</code>
<code>DiskSpaceOnDMModule.byte_threshold</code> The expected amount of usable disk space (in megabytes) for dataminer directory. An alert will be triggered if the usable disk space is less than the value.	100
<code>DMPProcessOnDMModule.Process_threshold</code> The lowest expected number of data miner processes. An alert will be triggered if the number of processes is lower than the value.	1
<code>TransferAgeOnDMModule.getTransferDaysThreshold</code> The maximum number of days that a data file can exist without transfer on the data miner. An alert will be triggered if the number of days the file has existed exceeds the value.	1

Running the Monitoring Scripts

You should run these scripts automatically using a scheduler such as cron.

To manually run the scripts, perform the following steps:

1. Log in as root on the server.
2. Change directories to the directory where you extracted the scripts.
3. Execute the script that you want to use.

Core Server Monitoring Scripts

You can use the following scripts to monitor your core server.

Note: You should adjust the script configuration settings in the `/opt/opsware/omdb/contrib/healthcheck/monitor/bsae-healthcheck/bin/conf/conf.properties` file according to your needs. See ["Configuring the Monitoring Scripts" \(on page 63\)](#).

Disk Space Test

Script name:	<code>diskspace_on_core_module.sh</code>
Detects:	If disk space on the core server below the threshold
Purpose:	Running out of available disk space in <code>/var/opt/opsware/omdb</code> will prevent data and model files from loading. Running out of available disk space at <code>/var/log/opsware/omdb</code> will prevent logging.

Out of Memory Test

Script name:	<code>oom_on_core_module.sh</code>
Detects:	Out of memory errors in the <code>server.log*</code> files
Purpose:	If the core server has an out of memory exception, then it is likely that some other error has happened due to the memory loss.

JBoss Process Test

Script name:	<code>jboss_process_on_core_module.sh</code>
Detects:	If the JBoss process is running on the core server
Purpose:	If the JBoss process is not running, then the data miner(s) will not be able to get configuration and ETL or datamodel updates from the core server.

rsync Process Test

Script name:	<code>rsync_process_on_core_module.sh</code>
Detects:	If the rsync process is running on the core server
Purpose:	If the jboss process is not running, then the data miner(s) will not be able to get configuration and ETL or datamodel updates from the core server.

BusinessObjects Processes Test

Script name:	<code>bo_processes_on_core_module.sh</code>
Detects:	If the number of BusinessObjects processes running on the core server correct
Purpose:	If BusinessObjects is not running, then Web reporting is not possible and certain security management functions will not be possible.

Loader Backlog Test

Script name:	<code>received_dir_on_core_module.sh</code>
Detects:	If the number of files in the <code>/var/opt/opsware/omdb/collect/</code> directory is above the specified threshold
Purpose:	If the number of unloaded data files in the loader collect directory exceeds a certain threshold, then this may be a sign of a loader or environment problem.

Loader Failures Test

Script name:	<code>Failures_dir_on_core_module.sh</code>
Detects:	If the number of files in the <code>/var/opt/opsware/omdb/ collect/failures</code> directory is above the specified threshold
Purpose:	If the number of unloaded data files in the loader collect directory exceeds a certain threshold, then this may be a sign of a loader or environment problem.

Database Monitoring Scripts

You can use the following scripts to monitor your database.

Note: The database monitoring scripts are supported on a single-node database instance only. They are not supported on a RAC database instance.

Note: You should adjust the script configuration settings in the `/opt/opsware/omdb/contrib/healthcheck/monitor/bsae-healthcheck/bin/conf/conf.properties` file according to your needs. See ["Configuring the Monitoring Scripts" \(on page 63\)](#).

Disk Space Test

Script name:	<code>diskspace_on_DB_module.sh</code>
Detects:	If the available disk space on the database server is less than the specified threshold
Purpose:	Running out of available database disk space can cause data load failures, reporting and administration problems, and overall problems with your database.

Database Listener Process Test

Script name:	<code>ora_listener_process_on_DB_module.sh</code>
Detects:	If the Oracle database listener is running
Purpose:	When the database listener is stopped, database-dependent components such as reporting, loader, security, etc., will stop functioning as expected.

Database Listener Port Test

Script name:	<code>ora_listener_port_on_DB_module.sh</code>
--------------	--

Detects:	If the Oracle database listener is listening on the specified port
Purpose:	When BSA Essentials cannot connect to the database because the specified port is blocked, database-dependent components such as reporting, loader, security, etc., will stop functioning as expected.

Database pmon Process Test

Script name:	<code>orapmon_process_on_DB_module.sh</code>
Detects:	If the Oracle pmon process is running
Purpose:	When the database is stopped, database-dependent components such as reporting, loader, security, etc., will stop functioning as expected.

Data Miner Monitoring Scripts

You can use the following scripts to monitor your data miner.

Note: You should adjust the script configuration settings in the `/opt/opsware/omdb/contrib/healthcheck/monitor/bsae-healthcheck/bin/conf/conf.properties` file according to your needs. See ["Configuring the Monitoring Scripts" \(on page 63\)](#).

Disk Space Test

Script name:	<code>diskspace_on_DM_module.sh</code>
Detects:	If the available disk space on the data miner server is less than the specified threshold
Purpose:	Running out of available disk space will prevent the data miner from collecting the data from the source system and adding new log entries.

Data Miner Process Test

Script name:	<code>dm_process_on_DM_module.sh</code>
Detects:	If the data miner is process running
Purpose:	It is very important that the data miner always runs in order to collect data. If it is not running, then the source system may discard data before it can be mined.

Data Miner Transfer Age Test

Script name:	<code>dm_file_transfer_age_on_DM_module.sh</code>
Detects:	If it has been longer than the specified amount of time since a file was transferred
Purpose:	If the data miner is unable to transfer data to the core server, then the data in your reports will be inaccurate.

Data Miner Out of Memory Test

Script name:	dm_oom_on_DM_module.sh
Detects:	If there is an out of memory message in the <code>dataminer.log</code> file
Purpose:	If the data miner has an out of memory exception, then it is likely that some other error has occurred that is related to the memory failure.

Integrating with Internal Tools

The following tables provide tips and examples on how to monitor your BSA Essentials Core Server using your own tools.

BSA Essentials Core Monitoring Details

To Monitor	Location	Tools	Reason
Database Disk-space	Database file system	Using system tools such as <code>df</code> , <code>mail</code> and <code>cron</code> is one way to monitor database disk space. See the "Integrating with Internal Tools" (on page 69) script sample for more information, Note: Consult with your Oracle DBA before monitoring.	Running out of available database disk-space can cause data load failures, reporting and administration problems, and overall problems with your database.
Database Listener	Database server	Using a system tool such as <code>ps</code> , <code>mail</code> , and <code>cron</code> is one way to monitor database listener. See the "Integrating with Internal Tools" (on page 69) script sample for more information. Note: Consult with your Oracle DBA before monitoring.	When the database listener is stopped, database-dependent components (reporting, loader, security, and so on) will stop functioning as expected.
Oracle RDBMS Processes	Database server	<code>ps -ef grep ora_pmon</code> (Include other Oracle processes, if desired.) Note: Consult with your Oracle DBA before monitoring.	When Oracle is stopped, database-dependent components (reporting, loader, security, and so on) will stop functioning as expected.
Oracle RDBMS Ports	Database server	<code>netstat -patn grep 1521</code> (Or other configured port.) If Oracle is remote from your BSA Essentials Core, a firewall hole must be allowed for the core to connect. Note: Consult with your network administrator for more information.	When you cannot connect to Oracle because port 1521 is blocked, database-dependant components (reporting, loader, security, and so on) will stop functioning as expected.
BSA Essentials	BSA Essentials	Using a system tool like <code>df</code> , <code>mail</code> , and <code>cron</code> is	Running out of available disk space at

To Monitor	Location	Tools	Reason
Core disk-space	Core file system	<p>one way to monitor BSA Essentials core disk space.</p> <p>See the "Integrating with Internal Tools" (on page 69) script example .</p> <p>Note: Consult with your storage administrator for more information.</p>	<p><code>/var/opt/opsware/omdb</code> will prevent data and model files from loading. Running out of available disk space at <code>/var/log/opsware/omdb</code> will prevent logging.</p>
BSA Essentials Core memory	BSA Essentials Core Server	<pre>grep OutOfMemory /var/log/opsware/omdb/server.log</pre>	<p>If the BSA Essentials Core Application Server has an out of memory exception, it is likely that some other error has happened due to the memory loss.</p>
BSA Essentials Core ports	BSA Essentials Core Server	<pre>netstat -patn grep 8443</pre> <p>(Or other configured port)</p> <p>A firewall hole must be allowed for externally available core ports.</p> <p>Note: Consult with your network administrator for more information.</p>	<p>When connections to BSA Essentials Core are prevented because port 8443 is blocked, Web reporting is not possible.</p>
Business Objects Processes	BSA Essentials Core Server	<p>One method to determine if BusinessObjects processes are running is to check the total number of processes that are running (greater than 10).</p> <p>For example:</p> <pre>ps -aef grep bo/bobje wc -l</pre> <p>Note: Consult with your Business objects Administrator before monitoring.</p>	<p>If BusinessObjects is not running, Web reporting is not possible and certain security management functions will not be possible.</p>
Model Deployer	BSA Essentials Core Server	<p>Using system tools such <code>ls</code>, <code>wc</code>, <code>mail</code>, and <code>cron</code> is one way to monitor failed model deployment.</p> <p>See the "Integrating with Internal Tools" (on page 69) script example for more information.</p>	<p>When the datamodel and ETL fails to deploy, the consequences can vary from unexpected reporting results to data load failures.</p>
Data Loader	BSA Essentials Core Server	<p>Using a system tool such as <code>ls</code>, <code>wc</code>, <code>mail</code>, and <code>cron</code> is one way to monitor failed data loads.</p> <p>See the "Integrating with Internal Tools" (on page 69) script example for more information.</p>	<p>When data fails to load, the integrity of report results is reduced. When failed data files are found, the problem can be diagnosed and fixed.</p>

To Monitor	Location	Tools	Reason
Rsync (core)	BSA Essentials Core Server	Check for the rsync process running from <code>/opt/opsware/omdb/bin</code> <code>ps -ef grep /opt/opsware/omdb/bin/rsync</code>	When the core-side rsync process is stopped, each data miner will accumulate data files (potential disk space issues) and the loader will not be able to load data.
Dataminer Disk-space	Dataminer filesystem	Using a system tool such as <code>df</code> , <code>mail</code> , and <code>cron</code> is one way to monitor Dataminer disk space. See the "Integrating with Internal Tools" (on page 69) script example for more information. Note: Consult with your storage administrator before monitoring.	Running out of available disk space will cause the data miner to not collect the data from the source system and not add new log entries.
Dataminer Memory	Dataminer system	<code>grep OutOfMemory dataminer.log</code>	If the data miner has an out of memory exception, it is likely that some other error has occurred related to the memory failure.
Dataminer Process	Dataminer system	<code>dmwatch.sh</code> script can be located on the Core Server at <code>/opt/opsware/omdb/contrib/dmwatch.</code> See the "Integrating with Internal Tools" (on page 69) file for more information, or see "Dataminer Watchdog Script" for more information on syntax and usage.	It is very important to have the data miner always running in order to collect data. If not, there is potential that the source system will remove the data before it can be mined.
Rsync (Dataminer)	Dataminer system	<code>dmwatch</code> script, located on the BSA Essentials Core Server at <code>/opt/opsware/omdb/contrib/dmwatch.sh</code> . See the "Integrating with Internal Tools" (on page 69) file for more information.	When the data miner-side rsync process is stopped, that data miner will accumulate data files (potential disk space issues) and the loader will not be able to load that Dataminer's data.
Compliance Checks Rollup Job	BSA Essentials Core Server	Use the following SQL query to determine if any errors occurred when running the compliance calculation package for the current day. <pre>select description, exception, source, source_id, create_date, category from cmdb_meta.application_events where source like 'compliance_fact_pkg%' and create_date >= sysdate -1 and create_date < sysdate+1</pre>	Failed compliance rollup calculations will cause report result integrity problems and is a sign that ETL data is either missing or incorrect.

To Monitor	Location	Tools	Reason
Loader Backlog	Core file system	Using a system tool such as <code>ls</code> , <code>wc</code> , <code>mail</code> and <code>cron</code> is one way to monitor excessive loader backlogs. See " Integrating with Internal Tools " (on page 69) for more information. Note: Consult with your storage administrator before monitoring.	If the number of unloaded data files in the loader collect directory exceeds a certain threshold, this might be a sign of a loader or environment problem.

Backing Up BSA Essentials on Linux

The BSA Essentials Core Server and database instance should both be backed up. The recommended backup frequency depends on the type of data you are collecting.

Note: These instructions are only for backing up BSA Essentials on Linux.

Server Automation (SA) keeps data for the number of days configured in the `vault.garbageCollector.daysToPreserve` parameter. You can find this parameter in the `vault.conf` file, which is located in `/etc/opt/opsware/vault/`. You should back up more frequently than this setting to avoid any gaps in your data in the event of a disaster and recovery.

Network Automation (NA) data is kept for two days, so backups done every two days or less are less likely to suffer from a loss of data.

Note: The data miners can remain online while you back up the core and the database instance.

- ["Backing Up the BSA Essentials Core Server" \(on page 73\)](#)
- ["Backing Up the BSA Essentials Database Instance" \(on page 74\)](#)

Backing Up the BSA Essentials Core Server

To back up the BSA Essentials Core Server, perform the following steps:

1. Log in as root on the server where you installed the BSA Essentials Core Server.

You can shut down the core or leave it running while you back it up.

2. Check the size of the BSA Essentials directories:

```
# du -sk /etc/opt/opsware /opt/opsware /var/opt/opsware
```

3. Verify that you have enough disk space for the backup tar file.

The amount of space needed is the sum of the three values returned in the previous step.

4. Make a directory where you want to write the backup files, such as `/var/tmp/backup`.
5. Change directories into the directory you created in the previous step.

6. Back up the BSA Essentials directories in a tar package:

```
# tar -cvf <bsae_backup.tar> /var/opt/opsware /etc/opt/opsware /opt/opsware
```

Where `<bsae_backup.tar>` is any file name you wish.

Note: If the backup size is a critical consideration, you can exclude the files in `/var/opt/opsware/omdb/collect`; however, excluding these files may leave a larger gap in historical data when the backup data is restored on a new server.

7. Compress the tar package using gzip:

```
# gzip <bsae_backup.tar>
```

Where `<bsae_backup.tar>` is the name of the tar file you created in the previous step.

8. Move the compressed tar file to a safe location on a different system.

Backing Up the BSA Essentials Database Instance

To back up the database instance, perform the following steps:

1. Log in as root on the Oracle server.
2. Make a directory where you want to write the backup files, such as `/var/tmp/backup`.
3. Make the directory writable for oracle:

```
# chmod -R ugo+rw /var/tmp/backup
```

Replace `/var/tmp/backup` with the name of the directory you created for your backup in the previous step.

4. Switch to the oracle user:

```
# su - oracle
```

5. Set the SID environment setting for the BSA Essentials database instance:

```
$ export ORACLE_SID=<BSAE_SID>
```

Where `<BSAE_SID>` is the SID of the BSA Essentials instance.

6. Start SQL*Plus:

```
$ sqlplus '/ as sysdba'
```

7. Create a backup directory for Oracle. In our example, we are using `/var/tmp/backup`:

```
SQL> CREATE DIRECTORY dmpdir AS '/var/tmp/backup';
```

Replace `/var/tmp/backup` with the name of the directory you created for your backup in step 2.

8. Check the size of the BSA Essentials instance:

```
SQL> select round(sum(seg.bytes) / 1024 / 1024 / 1024, 1) data_gb  
from dba_segments seg where seg.owner in ('CMDB_META', 'CMDB_DATA',  
'BO_ADMIN', 'ASAS_RPT_USER', 'CMDB_CUSTOM', 'CMDB_AAA')
```

9. Exit SQL*Plus.

10. Verify that you have enough disk space for the database dump file that will be created.

11. Export the database using the Oracle-supplied datapump tool:

```
$ expdp system/<password> full=Y DIRECTORY=dmpdir  
DUMPFILE=fullexp.dmp LOGFILE=fullexp.log
```

12. Switch back to the root user:

```
$ su - root
```

13. Back up the database directories in a tar package:

```
# tar -cvf <db_backup.tar> /var/tmp/backup
```

Where `<db_backup.tar>` is any file name you wish.

Replace `/var/tmp/backup` with the name of the directory you created for your backup in step 2.

14. Compress the tar package using gzip:

```
# gzip <db_backup.tar>
```

Where `<db_backup.tar>` is the name of the tar file you created in the previous step.

15. Move the compressed tar file to a safe location on a different system.

Restoring BSA Essentials on Linux

Note: These instructions are only for restoring a backup on Linux.

As soon as you realize that a recovery is necessary, you should do the following:

- Stop the data miners. If the data miners continue to run, you may use a significant amount of disk space and collect duplicate transactions. The duplicates are not a problem, but will cause a backlog.
- Make a note of the approximate time when the problem or failure first occurred. This time will help you identify any transactions that have happened since your last backup.

To restore BSA Essentials after a disaster, you should perform the following steps:

1. ["Preparing the Server or Servers for Restore" \(on page 76\)](#)
2. ["Restoring the BSA Essentials Database Instance" \(on page 77\)](#)
3. ["Restoring the BSA Essentials Core Server" \(on page 78\)](#)
4. ["Verifying BSA Essentials Functionality After Restore" \(on page 78\)](#)
5. ["Recovering New Data Collected Since the Last Backup" \(on page 79\)](#)

Preparing the Server or Servers for Restore

To prepare the server or servers before restoring the core or database instance, perform the following steps:

1. Restore the operating system to the server or servers where you will restore the BSA Essentials Core Server and database instance.
2. Assign the previously-used IP addresses to the server or servers where you will restore the BSA Essentials Core Server and database instance.

Note: You must restore to a server with the same hostname or IP address as the original installation.

3. Follow the *BSA Essentials Installation Guide* to create the database instance and install the BSA Essentials Core Server as you would for a new installation.

Note: You must install BSA Essentials because the required users, user groups, startup scripts, and symbolic links are not included in the backup.

4. Shut down the BSA Essentials Core Server by executing the following commands:

```
# /etc/init.d/bsae-bo stop
# /etc/init.d/opsware-omdb stop
```

5. Disconnect any other external connections to the BSA Essentials database.

You can use `netstat` to display the IP address of all established connections to the Oracle listener port:

```
# netstat -na | grep <listener port>
```

Where `<listener port>` is the Oracle listener port number.

Now you are ready to restore the database instance.

Restoring the BSA Essentials Database Instance

To restore the database instance, perform the following steps:

1. Log in as root on the Oracle server.
2. Copy the database backup file from the backup location to your current directory.
3. Unpack the backup file:

```
# tar -zxvf <db_backup.tar.gz> -C /
```

Where `<db_backup.tar.gz>` is the name of the backup file.

Note the directory created when the file is unpacked.

4. Log in as the oracle user:

```
# su - oracle
```

5. Change directories to the backup directory.

Create a script named `drop-users.sql` with the following contents:

```
drop user asas_rpt_user cascade;
drop user bo_admin cascade;
drop user cmdb_aaa cascade;
drop user cmdb_admin cascade;
drop user cmdb_appl cascade;
drop user cmdb_custom cascade;
drop user cmdb_data cascade;
drop user cmdb_deployer cascade;
drop user cmdb_meta cascade;
drop user cmdb_reporter cascade;
```

6. Set the SID environment setting for the BSA Essentials database instance:

```
$ export ORACLE_SID=<BSAE_SID>
```

Where `<BSAE_SID>` is the SID of the BSA Essentials instance.

7. Start SQL*Plus:

```
$ sqlplus '/ as sysdba'
```

8. Run the script to drop users:

```
SQL> start drop-users.sql
```

9. Create a directory from which the backup will be restored. In our example, we are using `/var/tmp/restore`:

```
SQL> CREATE DIRECTORY dmpdir AS '/var/tmp/restore';
```

Replace `/var/tmp/restore` with the directory that was created when the backup tar file was unpacked in step 3.

10. Exit SQL*Plus.
11. Import the database using the Oracle-supplied datapump tool:

```
$ impdp system/<password> DIRECTORY=dmpdir DUMPFILE=fullexp.dmp  
LOGFILE=fullimp.log TABLE_EXISTS_ACTION=REPLACE
```

12. Change to the oracle user:

```
# su - oracle
```

13. Start SQL*Plus:

```
$ sqlplus '/ as sysdba'
```

14. Run the `utlrip.sql` script:

```
SQL> start $ORACLE_HOME/rdbms/admin/utlrip.sql
```

When the script is done, you can exit SQL*Plus.

You are now ready to restore the BSA Essentials Core Server.

Restoring the BSA Essentials Core Server

To restore the core server, perform the following steps:

1. Log in as root on the server where you want to restore the BSA Essentials Core Server.
2. Change directories into the directory where you want to unpack the tar file.
3. Copy the core backup file from the backup location to your current directory.
4. Unpack the backup file:

```
# tar -zxvf <bsae_backup.tar.gz> -C /
```

Where `<bsae_backup.tar.gz>` is the name of the backup file.

5. Start the core server:

```
# /etc/init.d/bsae-bo start  
# /etc/init.d/opsware-omdb start
```

6. Check the `/var/opt/opsware/omdb/collect/failures` directory for zip/dat files.

Move any failed zip/dat files back to `/var/opt/opsware/omdb/collect` so they will be processed again.

Verifying BSA Essentials Functionality After Restore

To verify functionality after restoring a backup, perform the following steps:

1. Verify data miners by inspecting each `dataminer.log` file for connectivity to the core and for data file transfer.
2. Verify that AAA users and permissions are intact and correct by looking at the Administration tab in the BSA Essentials Web Client. Check users, groups, and permissions to verify that they are correct.
3. Launch the BSA Essentials Java Client and verify that the data it reports is correct.
4. Launch the BSA Essentials Web Client and verify that the data it reports is correct.
5. Check that changes made on a source system are mined and reported correctly.

Recovering New Data Collected Since the Last Backup

The data miners will likely collect new data between the time you made your last backup and the time when you restore the backup.

Note: You may not be able to recover all data that was generated during the recovery.

Recovering New Data For Server Automation (SA)

For Server Automation sources it may be possible to recover the new data by resetting the data miner to start mining from a transaction ID prior to the last backup.

You must recover data from Server Automation within the number of days set in the `vault.garbageCollector.daysToPreserve` setting in Server Automation. The default is seven days. Data will be lost if you have not recovered it within this window.

To recover new data for Server Automation, perform the following steps:

1. Log on as root to the system where the SA data miner is running.
2. Change to the oracle user:

```
# su - oracle
```

3. Set the ORACLE_SID environment setting for the SA database instance:

```
$ export ORACLE_SID=<SA_SID>
```

Where `<SA_SID>` is the SID of the SA database instance.

4. Start SQL*Plus:

```
$ sqlplus '/ as sysdba'
```

5. Identify the last transaction that was sent to BSA Essentials:

```
SQL> select max(tran_id) from lcrep.transactions where create_dt <=
to_date('<crash date>', 'mm/dd/yyyy:hh:mi:ss');
```

Where `<crash date>` is the approximate date and timestamp of the failure.

For example, the following would find the last transaction sent on January 25, 2011 at 10:25:00:

```
SQL> select max(tran_id) from lcrep.transactions where create_dt <=
to_date('01/25/2011:10:25:00', 'mm/dd/yyyy:hh:mi:ss');
```

6. Record the value returned in the last step, which may be presented as an exponential number.
7. Exit SQL*Plus and change back to the root user.
8. Change directories to the data miner directory.
9. Stop the data miner:

```
# /etc/init.d/opsware-dataminer stop
```

10. Remove cached data:

```
# rm -f *.ser
```

```
# rm -f DMSettingsCache.properties
# rm -f collect/*.xml collect/*.zip
```

11. Log in as root to the BSA Essentials server.

12. Change directories to `/opt/opsware/omdb/bin`.

13. Get the name of the Server Automation data source as configured on the system being restored:

```
# dmconfig --list
```

14. Reset the last processed transaction ID:

```
# ./dmconfig.sh --update --name <sa data source> --settings
LASTPROCESSEDTRANID=<value from select>
```

Where `<sa data source>` is the name of the Server Automation data source that you retrieved in the previous step and `<value from select>` is the transaction ID that was found in step 6, expressed as a decimal.

15. Start the SA data miner on the system where it is installed:

```
# /etc/init.d/opsware-dataminer start
```

Recovering New Data For Network Automation (NA) or Operation Orchestration (OO)

You must recover data for Network Automation and Operations Orchestration within the number of days configured in `dmconfig` setting `TriggerMineHistoryDays`. The default is two days. Data will be lost if you have not recovered it within this window.

To recover new data for Network Automation or Operation Orchestration, perform the following steps:

1. Connect to the Network Automation or Operation Orchestration database server.

- If you are using an Oracle database, run the following SQL command:

```
SQL> update opsw_omdbxm.omdb_dml_rows set processed=0 where dml_
date > (sysdate - <days since failure>)
```

- If you are using a SQLServer database, run the following SQL command:

```
SQL> update [db qualifier].opsw_omdbxm.omdb_dml_rows set
processed=0 where dml_date > (dateadd( dd, -<days since failure>,
getdate() ) )
```

Where `<days since failure>` is the numbers of days since the failure.

See your SQL guide or database administrator if you need to focus on a period of time smaller than one day.

