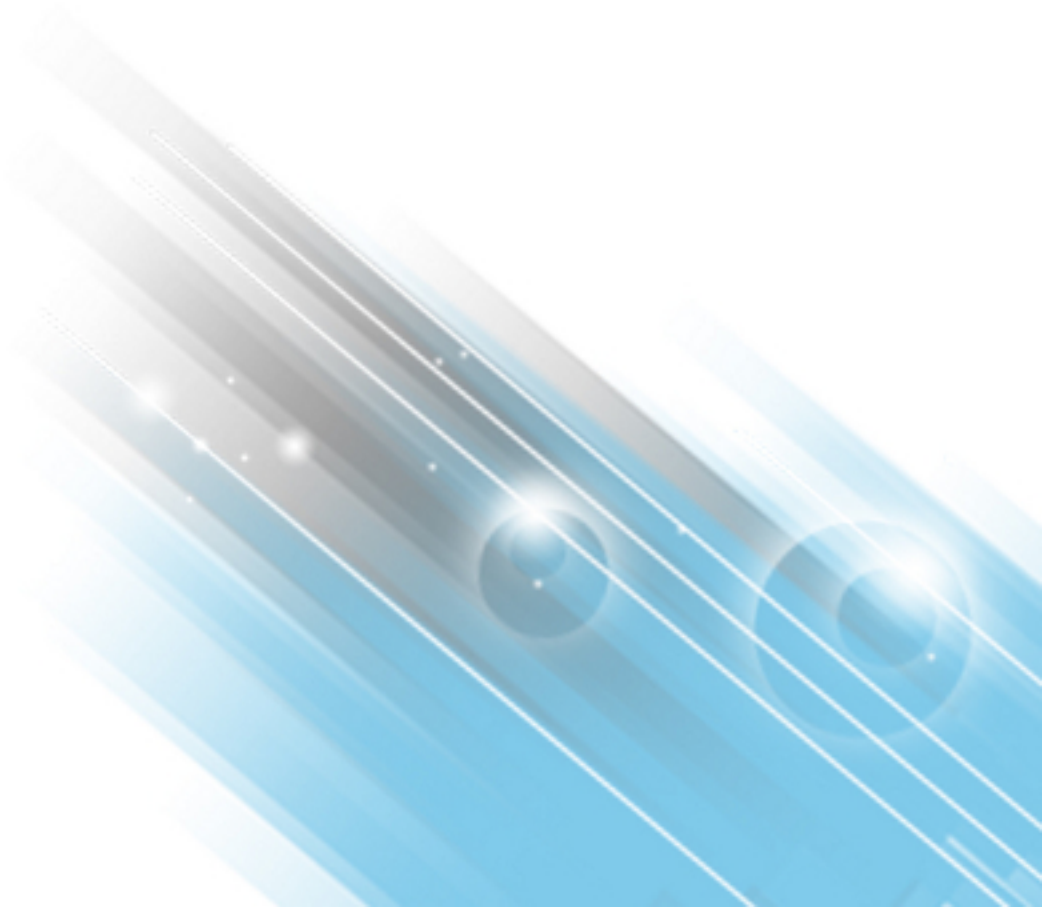
HP ArcSight Risk Insight

Software Version: 1.1

Technical Note: Setting Up Risk Insight for HA



January 7, 2016

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.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

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

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Risk Insight Introduction

This guide assumes that you already have ESM set up with the High Availability (HA) module and two machines and all the required cabling and so on.

In this procedure you install Risk Insight on the two ESM machines in two different ways. In both cases you install on the primary, so for this discussion "ESM1" is one machine and "ESM2" is the other machine regardless of which one of them is the primary.

You install Risk Insight on the first machine (ESM1) when it is the primary, using the normal Risk Insight installation program. Then you initiate a failover to the second machine (ESM2). This installation includes manually copying files from ESM1 to ESM2 and running scripts manually. This enables you to intervene in what the installation program would do so you can ensure that the two installations are identical.

If Risk Insight is already installed with ESM, designate that machine as ESM1 for the purposes of this appendix and skip the topic. "The First Risk Insight Installation."

Notes for Risk Insight with HA

- After a failover, you copy your reports over and manually start Risk Insight and its components on the new primary. See "Post-Failover Tasks" on page 20.
- The Risk Insight log and Audit log are not configured to log HA events.
- SAP BusinessObjects installation can be performed Automatically (using a script) on the first ESM1, and should be done manually on second ESM2, as described in "Installing SAP BusinessObjects" on page 7.
- The SAP BusinessObjects reports folder is not replicated, therefore, if you create a custom report, manually find the report file in the BusinessObjects on the primary and copy it to the BusinessObjects on the secondary. That way it will already be there if there is a failover.

Supported Implementation and Upgrade

Risk Insight 1.1 is compatible only with HA 6.9.1 on RHEL 6.7. Only a new installation of Risk Insight 1.1 is supported; there is no upgrade from Risk Insight 1.0 to Risk Insight 1.1 running on HA.

Supported Platforms

Risk Insight 1.1 is compatible with ArcSight ESM 6.9.1c.

See the HP Arcsight Risk Insight Support Matrix available on the Protect 724 site for details on Risk Insight platform support.

The First Risk Insight Installation

For this procedure it is assumed that ESM1 is the primary in a functioning HA environment. If Risk Insight is already installed on this machine, you can skip steps 1 and 2, but you must have the "Shared Secret" key you used when you installed Risk Insight, because you will need it when you install Risk Insight on ESM2.

1. Install SAP BusinessObjects. Refer to the topic on installing SAP BusinessObjects Enterprise in the *ArcSight Risk Insight Deployment Guide*.

2. Install Risk Insight.
   - Refer to the chapter on installing Risk Insight in the *ArcSight Risk Insight Deployment Guide*.
   - Make a note of the "Shared Secret" key; you will need it for installing on ESM2.
   - Use “localhost” as the **Server name or IP Address** in the SAP BusinessObjects connection step.

3. On the primary, run this command to get the UID and GID for user *sapbo*.

   ```
   id sapbo
   ```

   In the output, make a note of the numerals that follow `uid=` and `gid=`. You will use these IDs when creating this user and group on the secondary.

4. As user arcsight, edit the file `/usr/local/riskinsight/conf/db.properties`. You want the following property to use `localhost`, as shown:
   `db.url=jdbc\:mysql\://localhost\:3306/bri`

   Then, edit the file `/usr/local/riskinsight/conf/bo.properties`. You want the following property to use `localhost`, as shown:
   `bo.server.name=localhost`

5. Log in to Risk Insight and go to **Administration > Configuration**.

   Modify the connector parameters to use `localhost` instead of the machine hostname or IP address. The parameters to modify are **Asset Sync job** and **Risk Factors jobs** under the **Integrations** and **Risk Factors** folders of the configurations.

The Second Risk Insight Installation

At this point you have The ESM HA Module installed on two machines, ESM1 and ESM2, and you have Risk Insight and its required components installed on ESM1, which is currently operating as the primary. This section describes how to install Risk Insight on ESM2, which is currently operating as the secondary.

Installing SAP BusinessObjects

Installing SAP BusinessObjects is different on the second machine (ESM2) than it was on the first (ESM1). Do not install it as directed in the *ArcSight Risk Insight Deployment Guide*.

Preparing to Install SAP BusinessObjects on ESM2

1. Initiate a failover to ESM2. Once ESM2 is running as the primary, proceed with these steps for installing SAP BusinessObjects.

2. Verify that the SELinux status is "Permissive" or "Disabled" by running the following commands as user *root*:

   ```
   setenforce 0

   getenforce
   ```

   Verify that the status is listed as "Permissive" or "Disabled."

3. If the following file exists on your Linux machine: `/usr/share/Modules/init/bash`
   As user *root*, comment the following line in this file: `#export -f module`
   Save the file. You can uncomment this line when the installation completes.

4. Verify that the following TCP ports are not in use by another application or service: 8081, 6005, 8444, 6410, 6400

5. Create the *sapbo* user, group, and installation directory. Have the sapbo user and group IDs you obtained in "The First Risk Insight Installation" on the previous page.
   As user *root*, run the following commands:

   ```
   groupadd -g <GID> sapbo

   useradd -c "sapbo_software_owner" -g sapbo -d /home/sapbo -m
   -s /bin/bash -g <GID> -u <UID> sapbo
   ```

```
passwd sapbo

mkdir /usr/local/sapbo/UPDATE72
```

6. Transfer the following three SAP BusinessObjects installation files from the Risk Insight DVD at:
   `ArcSight RiskInsight 1.1\Installations\SAP BusinessObjects\Deployment`
   to ESM2 at
   `/usr/local/sapbo`
   The files are:

   ```
   ENTERPRISE07.zip
   ENTERPRISE0P_2-10007478.TGZ
   mysql-connector-java-5.1.35.jar
   sapbo.conf
   ```

7. As user *root* install the following five Linux package updates from the `required_RPMs` directory:

   ```
   compat-libstdc++-33.i686
   glibc.i686
   libXext.i686
   libXext-devel.i686
   ncurses-libs.i686
   ```

   Use the command `yum install <package filename>.rpm`

   If you are missing some dependency packages, the directory `additional_RPMs` contains all of them.

8. As user *root*, unpack the SAP BusinessObjects installation package and fix pack to a separate directory:

   ```
   unzip -o ENTERPRISE07.zip
   tar –zxvf ENTERPRISE07P_2-10007478.TGZ -C /usr/local/sapbo/UPDATE72
   ```

9. As user *root*, make `sapbo` the owner of the `sapbo` directory:

   ```
   chown -R sapbo:sapbo /usr/local/sapbo/
   chmod -R 755 /usr/local/sapbo/
   ```

10. As user *root*, modify the language file, /etc/sysconfig/i18n, by adding the following entries:

    ```
    LANG=en_US.utf8
    export LC_ALL=en_US.utf8
    ```

    Verify this configuration by running this command: `locale`

11. As user *sapbo* modify the profile file (`vi ~/.bash_profile`) to contain the following three rows:

```
export MYSQL_HOME=/opt/arcsight/logger/data/mysql
LANG="en_US.utf8"
export LANG
```

Source the file: `source ~/.bash_profile`

Verify the configuration as follows:

`echo $MYSQL_HOME` (you should see: `/opt/arcsight/logger/data/mysql`)
`echo $LANG` (you should see: `en_US.utf8`)

Installing SAP BusinessObjects on ESM2

1. As user sapbo run the following:
   ```
   cd /usr/local/sapbo/DISK_1
   ./install.sh
   ```
2. Press **Enter** to install the English version.
3. Press **y** for the License agreement.
4. Paste the License Key code **CSZ0F-13KG93M-Y40A00Y-1TCF** and press **Enter**.
5. Type the installation directory `/usr/local/sapbo` and press **Enter**.
6. Press **Enter** to install only the **English** version.
7. Select **System** and press **Enter**.
8. Select **New** and press **Enter**.(Keep the [X] Enable servers….)
9. CMS Port number: leave as **default** (6400), Type the Administrator password twice (admin123) and press **Enter**.
10. Select **Use an existing database** and press **Enter**.
11. Select **MySQL** and press **Enter**.
12. MySQL Host Name **127.0.0.1**, DB name **ri_ sapbo_data**, UserId: **ri_sapbo_user**, Password: (use the same password you entered for the first BusinessObjects installation on ESM1), port number: **Default 3306** and press **Enter**.
13. Select **Do not install Auditing Database…** and press **Enter**.
14. For “Would you like to re-initialize the database you have supplied to the install?” It is MOST IMPORTANT that you select **NO**. Press **Enter**.
15. Type the agent name **cms1**, leave the port number **6410**, and press **Enter**.

16. Select **Install Tomcat** and press **Enter**.

17. Type the SAP BO ports, **Receive HTTP requests: 8081**, **Redirect jsp requests: 8444**, **Shutdown hook: 8006**, and press **Enter**.

18. Type the installation directory `/usr/local/sapbo` and press **Enter**.
    The installation Begins… Continue upon completion:

19. Verify that the installation completed with no errors. As user *root*, run:
    `/usr/local/sapbo/bobje/init/setupinit.sh`
    verify that you get: "System initialization scripts created."

20. As user *sapbo* run the following to install the fix pack:

    ```
    cd /usr/local/sapbo/UPDATE72
    ./install.sh /usr/local/sapbo
    ```

21. Press **Enter** to install the English version.

22. Press **Y** to accept the License agreement.

23. Confirm the credentials from point 9, including hostname as **localhost** and press **Enter**.

24. Select **Yes**and press **Enter** to redeploy web applications.

25. Press **Enter** to confirm that the installation to the `/usr/local/sapbo` folder can begin.

26. Confirm that the installation completed successfully in the last dialog by pressing **Enter**.

SAP BusinessObjects Post-Installation Procedure on ESM2

1. Configure the MySQL driver Path.
   a. As user *sapbo*, run these commands:
      ```
      cd /usr/local/sapbo/
      chmod 777 mysql-connector-java-5.1.35.jar
      ```

   b. As user *sapbo*, edit the following file:
      `/usr/local/sapbo/bobje/enterprise120/linux_x86/dataAccess/RDBMS/connectionServer/jdbc/jdbc.sbo`
      Find the MySQL5 block and add the <ClassPath> section (below), and modify the `Array fetch size` parameter to 500 (in **bold**).

      ```
      <DataBase Active="Yes" Name="MySQL 5">
      <Aliases>
      <Alias>MySQL 4</Alias>
      </Aliases>
      <JDBCDriver>
      <ClassPath>
      ```

```
<Path>/usr/local/sapbo/mysql-connector-java-5.1.35.jar</Path>
</ClassPath>
<Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
<Parameter Name="URL
Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</Parameter>
</JDBCDriver>
<Parameter Name="Family">Sun</Parameter>
<Parameter Name="Version">mysql_jdbc.setup</Parameter>
<Parameter Name="SQL External File">mysql</Parameter>
<Parameter Name="SQL Parameter File">mysql</Parameter>
<Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
<Parameter Name="Force Execute">Procedures</Parameter>
<Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
<Parameter Name="Array Fetch Size">500</Parameter>
</DataBase>
```

2. Configure maximum number of document states kept in memory. As user *sapbo*, edit the following file:
   `/usr/local/sapbo/bobje/tomcat7/webapps/AnalyticalReporting/WEB-INF/classes/webi.properties`
   Uncomment the following lines (remove the #) and modify them to obtain the following values:
   ```
   WID_FAILOVER_SIZE=150
   WID_STORAGE_TOKEN_STACK_SIZE=150
   ```

3. Configure the "Maximum" parameters.
   a. Log in to the BusinessObjects Enterprise Central Management Console (CMC) at http://<Server_hostname>:8081/CmcApp
   credentials: administrator / admin123

   b. Click on **Servers**, expand Service Categories, and click on **Web Intelligence**.

   c. Under Server name, double-click on **WebIntelligenceProcessingServer**.

   In Properties window, under Web Intelligence Processing Service, modify these parameters as follows:
   ```
   Maximum Document Cache Size (KB) =10000000
   Maximum Documents per User=20
   Maximum Connections = 1000
   ```

   Restart the **WebIntelligenceProcessingServer**.

   d. Under Server name, double-click on **AdaptiveJobServer** in the **Properties** window, and modify the following parameter:
   ```
   Maximum Concurrent Jobs = 10
   ```
   Restart the **AdaptiveJobServer**.

4. Configure the Shared Secret key.
   a. In the BusinessObjects Enterprise Central Management Console (CMC) select Authentication.

   b. Double click on **Enterprise**.

   c. Check **Trusted Authentication option is enabled**.

   d. Type the Shared Secret key used in the Risk Insight installation wizard and click on **Update**.

5. Configure SAP BusinessObjects to start on reboot (after the Database is up):
   As user *root*, put the file `sapbo.conf` into the `/etc/init` directory and run this command:
   `chkconfig BobjEnterprise120 off`

Installing Risk Insight

Install Risk Insight on ESM2, which should be the running as the primary.

1. Copy the Risk Insight installation directory from ESM1 to ESM2. The path is /usr/local/riskinsight

2. Verify the files integrity by checking that they have the same user, user group, and permissions on ESM2 as they do on ESM1.

3. As user root, run the risk insight service script:
   /usr/local/riskinsight/bin/setup-service.sh

4. Copy the SAP BusinessObjects reports from ESM1 to ESM2. They go in the same directory, which is `/usr/local/sapbo/bobje/data/frsinput`.

5. Verify the files integrity by checking that they have the same user, user group, and permissions on ESM2 as they do on ESM1.

6. Repeat this for directory `/usr/local/sapbo/bobje/data/frsoutput`.

7. Verify the files integrity by checking that they have the same user, user group, and permissions on ESM2 as they do on ESM1.

Configuring SAP BusinessObjects

Configure SAP BusinessObjects on ESM2, which should still be the running as the primary. However, be careful: the last step is on ESM1. Issue these commands as user *root*.

1. Edit the SAP BO configuration file:
   `vi /usr/local/sapbo/bobje/ccm.config`
   ...by adding the cluster name. For example, if the cluster name is "BOPROD." the parameter would be
   `CLUSTER_NAMESERVER="BOPROD"`

2. Restart the SAP Business Objects service:
   `/etc/init.d/BobjEnterprise120 stop`
   `/etc/init.d/BobjEnterprise120 start`
   It might take several minutes for SAP BusinessObjects to come up.

3. On ESM1, the secondary, server, edit the SAP BusinessObjects configuration file:
   vi /usr/local/sapbo/bobje/ccm.config
   ...by adding the cluster name, as above. For example, if the cluster name is "BOPROD." the parameter would be
   `CLUSTER_NAMESERVER="BOPROD"`

Do *not* restart the SAP BusinessObjects service on ESM1.

Configuring Connectors

This topic describes how to set up connectors for Risk Insight so that they remain connected to the Risk Insight on the primary after a failover. You can install several connectors on one box (Linux or Windows), using a different directory for each connector.

> The Risk Insight HA solution supports one mount source. That means you should use one machine for connectors; either Windows or Linux.

Risk Insight supports the following five Scanners/Connectors, as described in the *Risk Insight Deployment Guide:*

- Tenable Nessus Vulnerability Scanner
- McAfee Vulnerability Manager (Foundscan)
- Qualys Guard
- HP WebInspect
- Rapid7 Nexpose

Configuring Connectors on Linux

This includes configuring the connectors themselves on the Linux machine and then configuring both of the ESM machines used by the HA solution.

Configuring the Connectors on Linux

Perform the following steps on a Linux machine. It can be one of the ESM machines. Do these steps as user *root*:

1. Install the Network File System (NFS) tool:
   `yum install nfs-utils nfs-utils-lib`
2. Create the *arcsight* user and group:
   a. Get the arcsight user ID (UID) and group ID (GID) from the ESM machines by running `id arcsight`. Use these IDs in the following commands as shown:

   b. `groupadd -g <GID> arcsight`

   c. `useradd -c “arcsight_esm_owner”-g arcsight -d /home/arcsight -m -s /bin/bash`

```
-g <GID> -u <UID> arcsight
```

d. `passwd arcsight`

3. Create the following folders:
   `/usr/local/vm/import/pending`
   `/usr/local/vm/import/done`
   `/usr/local/vm/import/errors`
   `/usr/local/vm/import/dictionary`

4. Set group and permissions:
   `chown -R arcsight:arcsight /usr/local/vm`
   `chmod -R 777 /usr/local/vm`

5. Edit the `/etc/exports` file to include the ESM machines by adding the following two lines:
   `/usr/local/vm/ <ESM1_Hostname>(rw,sync,no_root_squash)`
   `/usr/local/vm/ <ESM2_Hostname>(rw,sync,no_root_squash)`

6. Start the NFS service:
   `/etc/init.d/nfs start`

7. Export the configuration:
   `exportfs –ra`

8. Configure the NFS service to run at system startup:
   `chkconfig nfs on`

9. Install the ArcSight Smart Connector as described in the *Risk Insight Deployment Guide*. Configure the Connector output file folder to be: `/usr/local/vm/import/pending`

Configuring the ESM Machines for Connectors on Linux

1. Install the Network File System (NFS) tool:
   `yum install nfs-utils nfs-utils-lib`

2. Start the NFS service
   `/etc/init.d/nfs start`

3. Configure the NFS service to run at system startup:
   `chkconfig nfs on`

4. Check that the Smart Connector machine is running:
   `showmount -e <ArcSight_Smart_Connector_Hostname>`

   The output should be as follows:
   `Export list for <ArcSAight_Smart_Connector_Hostname>:`
   `/usr/local/vm <ESM1_Hostname>,<ESM2_Hostname>`

5. Configure the `/etc/fstab` file for mounting the SmartConnector folders by adding the following line to the `/etc/fstab` file:
   `<ArcSAight_Smart_Connector_Hostname>:/usr/local/vm /usr/local/riskinsight/vm nfs defaults 0 0`

6. Reboot the ESM machine. When it is up, run the command `mount` and verify the following output:
   `<ArcSAight_Smart_Connector_Hostname>:/usr/local/vm on /usr/local/riskinsight/vm type nfs (rw,vers=4,addr=<ArcSAight_Smart_Connector_IP_Address>,clientaddr=<ESM_IP_Address>)`

7. Run the ArcSight SmartConnector.

Configuring Connectors on Windows

This includes configuring the connectors themselves on the Windows machine and then configuring both of the ESM machines used by the HA solution.

Configuring the Connectors on Windows

1. Create the following folders on the Windows machine:
   `C:\vm\import\dictionary`
   `C:\vm\import\pending`
   `C:\vm\import\done`
   `C:\vm\import\errors`

2. Configure share for `C:\vm` (and sub-folders) and read/write permissions. You can share with "Everyone" or user *arcsight*. To share with user *arcsight*, you have to create that user on the Windows machine.

3. Install the connector as described in the *Risk Insight Deployment Guide*.

4. Configure the connector output file folder to be `C:\vm\import\pending`.

Configuring the ESM Machines for Connectors on Windows

1. Get the arcsight user ID (UID) and group ID (GID) from the ESM machines by running `id arcsight`.

2. Add a mount from both the primary and secondary systems to the Windows connector machine as follows: As user *root*, edit and save the `/etc/fstab` file on both systems to include the following line, the arcsight UID and GID are for each ESM.
   `//<Windows_Connector_Hostname>/vm /usr/local/riskinsight/vm cifs username=arcsight, password=<arcsight_password>,uid=<arcsight_uid>,gid=<arcsight_gid>,file_mode=0777,dir_mode=0777 0 0`

3. On both ESM machines, verify that the owner and group are *arcsight* for the following folder and its sub-folders: `/usr/local/riskinsight/vm`.

4. Reboot the ESM machines. When each is up, run the `mount` command and verify the following output:
   `//[Windows_Connector_Hostname]/vm on /usr/local/riskinsight/vm type cifs (rw)`

5. Run the ArcSight SmartConnector.

Health Check

1. On ESM2, still running as the primary, restart the SAP BusinessObjects and the Risk Insight services:
   ```
   /etc/init.d/BobjEnterprise120 stop
   /etc/init.d/BobjEnterprise120 start
   /etc/init.d/riskinsight restart
   ```

2. Log in to the ESM ArcSight Command Center and verify that Risk Insight is available and verify that reports are displayed on the dashboards.

3. Failover to ESM1 and repeat step 1.

SAP BusinessObjects Services Issues

When you stop the SAP BusinessObjects service (`/etc/init.d/BobjEnterprise120 stop`), it might hang. If that happens, check for other running SAP BusinessObjects processes and stop them:

```
ps –ef | grep boe
kill -9 <process_id>
```

```
ps -ef | grep cms
kill -9 <process_id>
```

Also use the following command to stop all running SAP BusinessObjects services:

```
rm -f /usr/local/sapbo/bobje/serverpids
```

Post-Failover Tasks

When ESM fails over, you manually restart Risk Insight and its components on the new primary. On the new primary, restart the SAP BusinessObjects and the Risk Insight services:

```
/etc/init.d/BobjEnterprise120 stop
/etc/init.d/BobjEnterprise120 start
/etc/init.d/riskinsight restart
```

Send Documentation Feedback

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

Feedback on Technical Note: Setting Up Risk Insight for HA (Risk Insight 1.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!