HP ArcSight Risk Insight

Software Version: 1.1

Technical Note: Upgrading Risk Insight 1.0 to 1.1

January 12, 2016

Legal Notices

Warranty

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

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 Upgrade 1.0 to 1.1

This document assumes that you have ESM and Risk Insight installed and fully operational.

In preparation of installing Risk Insight 1.1, you will perform a database dump of the contents of your existing Risk Insight installation, and after deploying a Risk Insight 1.1, restore the database schema to the new version of Risk Insight.

Also, you will back up the contents of the initial Risk Insight installation for archiving and restoring purposes. Security keys and connection properties are carried over to Risk Insight 1.1 as physical files. You will use the SAP BusinessObjects web-based application to delete some old entities and allow the successful installation of Risk Insight 1.1.

Notes for Risk Insight version upgrade

- RHEL 7.1 is not a supported platform for the Risk Insight upgrade procedure presented in this document, since SAP Business Objects is not supported on RHEL 7.1.
- The Risk Insight upgrade procedure can be performed before or after an ESM upgrade since the database schemas of Risk Insight and SAP BusinessObjects in the CORR-Engine database are not affected by the ESM upgrade.
- There are some limitations concerning vulnerability dictionary features after restoring the old data schema.
- During the Risk Insight upgrade procedure, the version of SAP BusinessObjects remains unchanged, while a new Risk Insight 1.1 installation contains the latest SAP BusinessObjects version.
- ESM functioning is not affected by the Risk Insight upgrade.

Preparing to Install Risk Insight 1.1

This procedure assumes that you have ESM and Risk Insight installed and fully operational. ESM can be in a post-upgrade state. Note that you will need credentials for the CORR-Engine database (as the `arcsight` user) to be able to dump the database schema, and the administrator password for SAP BusinessObjects CmcApp access. The shared secret key should also be noted for use later in the process.

1. While ESM is running stop the RiskInsight 1.0 and SAP BusinessObjects:

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

2. Perform the database dump using the following commands:

```
cd /opt/arcsight/logger/current/arcsight/bin/

 ./mysqldump --user=arcsight --password=CORR_PASSWORD --verbose --no-create-db
--databases bri > /tmp/ri_bo_backup.sql
```

Where `CORR_PASSWORD` is your CORR-Engine password specified during installation of ESM.

3. Tar the entire /usr/local/riskinsight directory for backup purposes. Separately make backup copies of the following files:

```
/usr/local/riskinsight/conf/bo.properties
/usr/local/riskinsight/conf/db.properties
/usr/local/riskinsight/conf/encryption.properties
/usr/local/riskinsight/security/encrypt_repository
```

4. Run following script to remove the Risk Insight 1.0 service:

```
./usr/local/riskinsight/bin/remove-service.sh
```

5. Remove the contents of the directory `/usr/local/riskinsight` (keep the directory itself):

```
rm -rf /usr/local/riskinsight/*
```

6. Drop the Risk Insight 1.0 database schemas:

```
cd /opt/arcsight/logger/current/arcsight/bin/

./mysql --user=arcsight --password=CORR_PASSWORD
> drop database bri_bsf;
> drop database bri;
> quit;
```

Where `CORR_PASSWORD` is the CORR-Engine password specified during ESM installation.

7. Start SAP Business Objects:

```
/etc/init.d/BobjEnterprise120 start
```

Then navigate in your browser to http://localhost:8081/CmcApp . Use a browser running on the same machine as SAP BusinessObjects.

8. Use the administrator user account and password to log into the Central Management Console Application. Navigate to listed menus and delete the following items:

   - Go to the *Categories* menu, right click "Risk Insight Categories" and select **Delete**.
   - Go to the *Folders* menu, right click "ArcSight Risk Insight Reports" and select **Delete**.
   - Go to the *Universes* menu, right click "ArcSight Risk Insight Universe" and select **Delete**.

Now you can install Risk Insight 1.1.

Installing Risk Insight 1.1

1. Install Risk Insight. See the Chapter 2, "Install Risk Insight", in the HP ArcSight Risk Insight Deployment Guide.

2. After successful installation of Risk Insight 1.1 turn off Risk Insight and SAP Business Objects:

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

3. Reinstate previously dumped Risk Insight 1.0 schemas to the CORR-Engine:

   ```
   cd /opt/arcsight/logger/current/arcsight/bin/
   ./mysql -uroot -pCORR_PASSWORD < /tmp/ri_bo_backup.sql
   ```

4. Copy the three properties files to `/usr/local/riskinsight/conf/` and binary master key file `encrypt_repository` mentioned in step 3 of "Preparing to Install Risk Insight 1.1 " to `/usr/local/riskinsight/security/`.

   Add `.bak` to Risk Insight 1.1 files to retain them as a backup.

5. Start SAP BusinessObjects:

   ```
   ./etc/init.d/BobjEnterprise120 start
   ```

   Verify that SAP BusinessObjects are running properly by navigating to the Central Management Console at http://localhost:8081/CmcApp and viewing the **Servers** menu. There should be no warning messages.

6. Start Risk Insight 1.1:

   ```
   ./etc/init.d/riskinsight start
   ```

   Verify that Risk Insight is running properly by checking `\usr\local\riskinsight\logsall-errors.log file`.

7. For further verification, navigate through menus in Risk Insight to ensure that all features available and working properly. Again, check `\usr\local\riskinsight\logsall-errors.log file` to see if any messages of the type ERROR have been written to the log in the meantime.

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: Upgrading Risk Insight 1.0 to 1.1 (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!