Upgrade

Operations Bridge Suite 2017.11

MICRO FOCUS

Upgrade

The following upgrades are available:

- 2017.08 > 2017.11 (BVD only). You can upgrade BVD as part of your existing, containerized 2017.08 suite installation to Operations Bridge Suite 2017.11.
- BVD 10.12 > 2017.11. You can upgrade BVD 10.12 (classic deployment) to BVD 10.63 (2017.11 suite installation)

2017.08 > 2017.11 (BVD only)

Note At the moment, **only BVD can be upgraded to 2017.11**. For every other component of the Operations Bridge Suite 2017.08, a fresh installation is required.
Do the following to upgrade BVD as part of the containerized suite from 2017.08 to 2017.11:

1. Upgrade CDF to 2017.10. For details, see Upgrade CDF.
2. Upgrade the suite to 2017.11. For details, see Upgrade the suite.
3. Reconfigure the suite. For details, see Reconfigure. You do not have to make any changes in the configuration wizard, but the wizard must run once.

1. Upgrade CDF

CDF can be upgraded to version 2017.10. The upgrade will update all components such as Docker, Kubernetes, Heapster, Vault, Etcd, Flannel and the CDF core to the 2017.10 version.

Note We recommend that you do the following before the upgrade:

- Back up the entire NFS folder in which the CDF data is stored, the etcd data, and the data form the external database (if you used an external database for the CDF installation).
- Prepare a folder (by default: /tmp) that has enough free disk space. The disk space must at least be similar to the CDF K8S_Home directory size with an extra 20 GB disk space.

To upgrade CDF, do the following:

1. Download the CDF upgrade package CDF1710-00301-15001-upgrade.zip on the Software Licenses and Downloads Portal, and copy it to every master and worker node.
2. Run the following command on every master and worker node to unzip the package:

   ```
   unzip CDF1710-00301-15001-upgrade.zip
   ```

3. Make sure all CDF nodes are running.
4. On one of the master nodes, navigate to the unzipped upgrade package and run the command `upgrade.sh -g` to generate the `CDF_upgrade_parameters.txt` under the current directory.

   Note

   This step will try to remove resources from the yaml file. If you receive an error when deleting the resources, remove the resources manually before the upgrade. Otherwise, the upgrade may fail due to the existing resources.

5. Copy the `CDF_upgrade_parameters.txt` to all nodes.

6. Copy <K8S_Home>/ssl/ca.key from the first installed master node to the same directory on the additional master nodes.

7. Upgrade the first master node with the command:

   ```
   upgrade.sh -u /<Parameter file path>/CDF_upgrade_parameters.txt
   ```

8. Upgrade the rest of the master nodes one after the other (no preferred order) with the following command:

   ```
   upgrade.sh -u /<Parameter file path>/CDF_upgrade_parameters.txt
   ```

9. Upgrade the worker nodes one after the other (no preferred order) with the following command:

   ```
   upgrade.sh -u /<Parameter file path>/CDF_upgrade_parameters.txt
   ```

2. Upgrade the suite

Upgrade the suite to version 2017.11 by creating additional NFS shares and running the upgrade wizard.

1. Create two new NFS shares for OMi:

   ```
   cd /opt/kubernetes/scripts
   ./setupNFS.sh /var/vols/omi0
   ./setupNFS.sh /var/vols/omi1
   ```

2. Access the management portal and go to **Suite > Management**. For your 2017.08 suite deployment, select **Actions > Update**.

   Caution If you cannot log into the management portal after the upgrade, the CDF upgrade has probably renamed your admin user. If that happened, the file /opt/kubernetes/zip/core_conflicted_db_users.txt is created. The file contains the new admin name which looks similar to admin_c3922df106b2444b8587464169247658.

3. Download the zip file as instructed in the wizard, and unzip it.

4. On the (first) master node, run the following command:

   ```
   ./downloadimages.sh
   ```

   You are prompted for the following information:

Suite	`OpsBridge`
User name and password	Enter your Docker Hub account credentials. If the master node does not have an internet connection, press Ctrl+C, and continue with the steps described in Download suite images to another machine.
Suite version	Enter the suite version `2017.11`

5. Accept the overwrite by entering **y**.
6. Wait until the download is finished (this may take approximately 10 minutes).
7. Copy the content from the ./suite_images folder to the /var/opt/kubernetes/offline/suite_images folder on the (first) master node.
   You can skip this step if you downloaded the images on the server where you want to install them.
8. On the (first) master node, run the uploadimages.sh script:

   ```
   cd /opt/kubernetes/scripts
   ./uploadimages.sh
   ```

9. After the upload is finished, you can verify the imported suite images on the management portal. Then click **Next**.
10. Specify the mount points for the two new OMi NFS shares and click **Next**.
11. Review the update overview and click **Next**.
12. Once the update is finished, click **Finish**.

3. Reconfigure the suite

As the last step, reconfigure the suite. For details, see Reconfigure. You do not have to make any changes in the configuration wizard, but the wizard must run once.

BVD 10.12 (classic) > 2017.11

You can migrate your BVD 10.12 data to Operations Bridge Suite 2017.11. Note that an upgrade is only possible if you used an external PostgreSQL for your previous BVD version.

a. Stop your existing BVD deployment. BVD must no longer be active on the database.

b. Use a database tool, for example `PgAdmin`, to open the BVD database.

i. Edit the table `bvdLdapServerConfigurations`.

ii. Remove the single line that the table contains. This is the LDAP server configuration for 10.12, which is no longer required.

Do **not** drop the table.

1. Install and configure the Operations Bridge Suite 2017.11. When configuring the database connection for BVD, specify the external PostgreSQL database of your former deployment. For details, see Install the suite.

2. *Optional*. To also migrate your LDAP user permissions and assignments, specify the LDAP server you previously used for BVD during the LDAP configuration. If the same LDAP server is configured, BVD will apply the already configured permissions and role assignments.