# Operations Manager i

Software Version: 10.63

# Virtual Appliance Deployment Guide

Document Release Date: December 2017
Software Release Date: November 2017

Hewlett Packard Enterprise

# Legal Notices

## Warranty

The only warranties for Seattle SpinCo, Inc and its subsidiaries (“Seattle”) 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. Seattle 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. Except as specifically indicated, valid license from Seattle 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



## Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD, the AMD Arrow symbol and ATI are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPad® and iPhone® are trademarks of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

# Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

# Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

**HPE Software Solutions Now** accesses the Solution and Integration Portal website. This site enables you to explore HPE product solutions to meet your business needs, includes a full list of integrations between HPE products, as well as a listing of ITIL processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

# Contents

# Operations Manager i 10.63 Virtual Appliance

The Operations Manager i (OMi) Virtual Appliance contains a preinstalled and preconfigured OMi system and is available as an Open Virtual Appliance (OVA) file that can be deployed to VMware ESX.

> **Note:** The Virtual Appliance is delivered with the latest operating system security patches already installed. However, after you deploy the Virtual Appliance, make sure that you keep the operating system of the Virtual Appliance up to date with all security patches.

See the following sections for information about the default configuration, the file format, and the deployment:

# Default Configuration

## System Details

| | |
|---|---|
| CPU | 4 vCPUs |
| Memory | 12 GB vRAM |
| Disk | 64 GB (52 GB of which is for the data file system) |
| Swap | 8 GB |
| Operating System | CentOS 6.9 64bit |

## Notes and Recommendations

Keep in mind the following notes and recommendations:

- The **System Details** show the default sizing configuration. You can change the configuration by using standard VMware tools and procedures.
- The installed operating system is a basic server installation without desktop GUI support. This means that X11 desktop libraries are not available. A minimal set of X11 server libraries is available to allow X11 redirection to the server. The login to the operating system is only possible by using the VMware vSphere console, Web Client, or SSH.
- Do not install any other HPE products, components, or third-party software products on the virtual appliance instance.
- The installed OMi is configured for up to 2,000 nodes, the default small environment. If you want to grow and need to support a large environment, for example a distributed setup, you can copy data from the embedded PostgreSQL database to an external PostgreSQL database and install a different version of OMi. For information, see the *OMi Database Guide*.
- The database configured with the Virtual Appliance is configured for non-English environments.
- The embedded Apache web server is configured for TLS with OMi-generated certificates.

Connections to the OMi UI, web services, and JMX console are only possible by using HTTPS.

- The Virtual Appliance, CentOS, and Management Pack language version is English.

# Virtual Appliance File Format

The Virtual Appliance is available in the Open Virtual Appliance (OVA) file format.

Download the OVA file to a local directory on your computer. Make sure that you have at least 10 GB of available disk space in this directory.

The OVA file is now available and you can start further actions.

Along with the OVA file, a signature file holding an additional `.sig` suffix is provided. In order to validate the signature, follow the instructions available at GPG or RPM Signature Verification.

> **Note:** Windows users need to download and install Gpg4win in order to successfully complete the GPG Signature Verification.

# Deploying the Virtual Appliance

Use one of the following methods to deploy the Virtual Appliance:

- "Deploying from the VMware vSphere Console" below
- "Deploying from the VMware vSphere Web Client" on the next page
- "Deploying by Using the Command Line" on page 9

# Deploying from the VMware vSphere Console

To deploy the Virtual Appliance from the VMware vSphere console:

1. Log in to the VMware vSphere console.
2. Click **File > Deploy OVF Template**.

   The Deploy OVF Template window opens.
3. In Source, select the OMi Virtual Appliance (`HPE_OMi_10.63_VirtualAppliance.ova`).

4. In OVF Template Details, verify the OVF template-related information.
5. In End User License Agreement, read the End User License Agreement and accept it.
6. In Name and Location, specify the data center.
7. In Host / Cluster, select the host system from the list of available systems.
8. In Resource Pool, select the resource pool on which you want to run the OVF template.
9. In Storage, select the destination storage for the new Virtual Appliance.
10. In Disk Format, select the disk format. We recommend that you use the Thick Provision Lazy Zeroed option.

    > **Note:** Selecting the Thick Provision Lazy Zeroed option creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.

11. In Network Mapping, select the network from the list of available networks.
12. In Properties, specify the networking configuration options if you use the static IP address (leave these options blank if you use DHCP).
13. Review your settings and click **Finish** to start the deployment.

For additional information, see the ESXi and vCenter Server 5.5 Documentation.

# Deploying from the VMware vSphere Web Client

To deploy the Virtual Appliance from the VMware vSphere Web Client:

1. In a browser, open the URL of your VMware vSphere server.
2. Select your datacenter, and then click **Deploy OVF Template**.

   The Deploy OVF Template wizard window opens.
3. In Select source, select **Local file**, and then browse for the OMi Virtual Appliance (`HPE_OMi_10.63_VirtualAppliance.ova`).
4. In Review details, verify the OVF template-related information, and then click **Next**.
5. In Accept License Agreements, read the End User License Agreement and accept it.
6. In Select name and folder, enter a name and location for the deployed template.

7. In Select storage, select the storage target location and the virtual disk format.
8. In Setup networks, configure the networks.
9. In Customize template, specify the network deployment properties if you choose to use a static IP address.
10. Review your settings and click **Finish** to start the deployment.

For additional information, see the VMware vSphere 6.0 Documentation.

# Deploying by Using the Command Line

**Prerequisite:** Download the OVF tool from VMware.

To deploy the virtual appliance with OMi by using the VMware OVF tool, run the following command (if you use a static IP address):

```
ovftool --acceptAllEulas -n=<name of the appliance>
        --network=<name of the network> -ds=<data store name>
        --powerOn -dm=thin --prop:vami.ip0.OMi_VA =<static_IP_address>
        -- prop:vami.netmask0.OMi_VA =<Subnet_IP>
        -- prop:vami.gateway.OMi_VA =<gateway_IP>
        --prop:vami.DNS.OMi_VA =<dns_IP> <URL location_of_OVA_file>
          <URL vCenter host cluster location>
```

In this instance:

*<name of the appliance>* is the name to be assigned to the new virtual appliance.

*<name of the network>* is the name of the network where you want to deploy the virtual appliance.

*<static_IP_address>* is the static IP address of the virtual appliance.

*<Subnet_IP>* is the IP address of the subnet where you want to deploy the virtual appliance.

*<gateway_IP>* is the IP address of the gateway server for the virtual appliance.

*<dns_IP>* is the IP address of the DNS server for the virtual appliance.

*<URL location_of_OVA_file>* is the location where you stored the OMi OVA file.

*<URL vCenter host cluster location>* is the location in vCenter where the virtual appliance will be deployed.

# Verification

To verify the successful deployment of the OMi Virtual Appliance, log in to the deployed system's operating system as user `root` by using the VMware vSphere Console, Web Client, or SSH:

Login name: `root`

Password: `password`

> **Caution:** It is recommended that the system superuser changes this password upon first login to prevent unauthorized entry. You can use the `passwd` command to change the password of the `root` account.

OMi on the deployed server starts automatically. You can check the OMi run status by using the `opr-status.py` command-line tool:

```
/opt/HP/BSM/opr/support/opr-status.py
```

Once OMi is up and running, log in as user `admin` by using a web browser at the following URL:

`https://<FQDN_of_the_VA>/omi`

Login name: `admin`

Password: `admin`

> **Caution:** It is recommended that the system superuser changes this password upon first login to prevent unauthorized entry. For details on changing the user password, see the *OMi User Guide*. The login name cannot be changed.

> **Note:** It is also recommended to create additional administrative users to enable OMi administrators to access the system. For details on creating users in the OMi system, see the *OMi Administration Guide*.

For login troubleshooting information as well as for details on login authentication strategies that can be used in OMi and details on accessing OMi securely, see the *OMi Administration Guide*.

For additional configuration options, you can enable remote access to the JMX console. For details, see the corresponding section in the *OMi Help*.

# Firewall Configuration

The following is the status of the `iptables` firewall running on the appliance:

```
Chain INPUT (policy DROP)
target     prot opt source      destination
ACCEPT     all  --  anywhere    anywhere
ACCEPT     all  --  anywhere    anywhere     state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:echo
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:ssh
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:telnet
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:http
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:hp-collector
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:hp-alarm-mgr
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:https
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:pyrrho
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:5480
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:5488
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:5489
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:rrac
ACCEPT     tcp  --  anywhere    anywhere     tcp dpt:dccm

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

# Changing the Passwords

For details on how to change the passwords, see the following sections:

- "Changing the User Passwords for the Embedded PostgreSQL Database" on the next page
- "Changing the JMX Password" on the next page

# Changing the User Passwords for the Embedded PostgreSQL Database

To change the user passwords for the embedded PostgreSQL database, follow these steps:

1. Make sure OMi is not running.
2. Connect to the embedded PostgreSQL database:

   ```
   /opt/HP/BSM/pgsql/bin/psql –U postgres –p 5433
   ```

3. Change the password of the `postgres` database user:

   ```
   alter role postgres with encrypted password '<new password>';
   ```

   > **Note:** The default password is `installed`.

4. Change the password of the `hpbsm` database user:

   ```
   alter role hpbsm with encrypted password '<new password>';
   ```

   > **Note:** The default password is `installed`.

5. Edit the `/customizeOMiVA/postgres.xml` response file by changing all instances of the old password with the new one.
6. Reconfigure OMi:

   ```
   /opt/HP/BSM/bin/silentConfigureBSM.sh /customizeOMiVA/postgres.xml
   ```

7. Start OMi.

# Changing the JMX Password

> **Note:** Changing the JMX password affects both the OMi and RTSM JMX consoles.

To change the JMX password, follow these steps:

1. Make sure OMi is not running.
2. In the `/customizeOMiVA/postgres.xml` file, enter the administrator passwords for logging on to

OMi and the JMX console.

If you used the *<OMi_HOME>*/bin/encrypt-password tool to encrypt the password, set isEncrypted to true and enter the encrypted password as the value.

a. Set the password for the OMi administrator (admin) in the following line:

```
<property isEncrypted="false" key="adminPassword" value="<admin password>"/>
```

> **Note:** The default password is admin.

b. Set the password for the OMi administrator (admin) for the JMX console in the following line:

```
<property isEncrypted="false" key="jmxPassword" value="<JMX password>"/>
```

> **Note:** This password is valid only for the current system. The default password is admin.

3. Reconfigure OMi:

```
/opt/HP/BSM/bin/silentConfigureBSM.sh /customizeOMiVA/postgres.xml
```

4. Start OMi.

# 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 Virtual Appliance Deployment Guide (Operations Manager i 10.63)**

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 ovdoc-asm@hpe.com.

We appreciate your feedback!