Operations Bridge Suite

Software Version: 2017.04

Administration Guide

Document Release Date: April 2017

Software Release Date: April 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

© 2015 - 2017 Hewlett Packard Enterprise Development LP

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

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.

Disclaimer

Certain versions of documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Contents

Administration

This guide describes administration tasks that you can perform on the ITOM Platform. On the ITOM Platform, you can manage the shared services infrastructure and all suite products, including the Operations Bridge Suite deployment and configuration.

To access, open `https://<external_access_host>:5443` in a supported web browser and provide the administrator password.

For more information on the ITOM Platform administration, see "Administer the ITOM Platform" on page 6.

For more information on the suite administration, see "Administer the Operations Bridge Suite" on page 36.

Administer the ITOM Platform

You can perform the following tasks to administer the ITOM Platform:

"Access the ITOM Platform" on page 7

"Manage users" on page 8

"Monitor infrastructure status" on page 9

" Manage nodes" on page 10

"Manage licenses" on page 14

"View the existing images" on page 16

"Set up LW-SSO" on page 17

"Manage resources" on page 18

"Security" on page 27

Access the ITOM Platform

To access the ITOM Platform, do the following:

1. Launch the ITOM Platform from a supported web browser:

   https://*<external_access_host>*:5443

   <external_access_host> is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

   As a result, the ITOM Suites login screen should be displayed.

2. Log in to the ITOM Platform as the admin user.

   Use the password that you specified at initial login. See Step 6. Verify the installation.

Manage users

This section provides information on how to manage a user.

How to display, create, delete, or edit a user

Click **ADMINISTRATION** > **User Management**. The User page opens.

For each user, this page displays the user name, display name, e-mail, and user group.

- **Create a user.** To create a user, click **ADD**. Enter the user name, password, email, group, and (optionally) a display name. Click **SAVE**.
- **Delete a user.** To delete a user, click ⋮ and select **Delete**.
- **Edit a user.** To edit or view a user information, click ⋮ and select **View/Edit**.

Monitor infrastructure status

You can monitor the infrastructure status of your namespaces, nodes, and persistent volumes.

To access, click **ADMINISTRATION** > **Admin**.

The Admin page displays:

- **Namespaces.** The list of the current default namespaces as well as the namespaces for the suites. Every suite on the same Kubernetes cluster is deployed in a different namespace.
- **Nodes.** The composition of the Kubernetes cluster in terms of servers on which the cluster were installed (master and worker nodes, the physical servers or the VMs).
- **Persistent volumes.** The persistent volume configuration for one or more suites. These volumes contain the data that needs to live outside of the containers.

Manage nodes

The Nodes page provides the CPU and Memory usage history of the selected Namespace, a list of the predefined labels, and the list of nodes of the selected Namespace.

> **Tip:** When the CPU load is over 80%, it significantly impacts the efficiency of network transmission between the base infrastructure environment. HPE recommends to control the CPU load so it is less than 80% by separating the suite instance into multiple worker nodes: adding more worker nodes and killing the pods on heavy-load nodes and deploying those pods on the newly added worker nodes.

This section includes the following tasks:

- "View the existing nodes" below
- "Add/delete labels" on the next page
- "Assign labels to nodes" on the next page
- "Add a node" on the next page

View the existing nodes

1. Click **ADMINISTRATION** > **Nodes**.
2. The area displays the CPU and memory usage of the selected namespace during the past 15 minutes, the list of the node labels, and the status, labels, readiness, and creation timestamp of the nodes corresponding to the selected namespace.

   You can do the following:

   - Define a set of labels you want to use and then assign them to nodes by dragging them to the node. See "Add/delete labels" on the next page and "Assign labels to nodes" on the next page.
   - Add a node. See "Add a node" on the next page.
   - **REFRESH.** Click to refresh the display.
   - Click the relevant node to see its details. See "View the node details" on page 12.

Add/delete labels

1. Click **ADMINISTRATION** > **Nodes**.
2. To add a label in the **Predefined Labels** area, enter the **value** and click **[+]**. The label is added to the list.
3. To delete a label: in the **Predefined Labels** area, click **[-]** for the relevant label.

Assign labels to nodes

To manage node labels:

1. Click **ADMINISTRATION** > **Nodes**.
2. **To assign a label to a node:** drag the relevant label the **Predefined Labels** area to the relevant node in the **Nodes** area.
3. **To create a new label and assign it to a node:** in the relevant node row, click **[+]** below the list of labels, enter the **key** and click **OK**. You do not need to add the **value** of the label.
4. **To unassign a label:** in the **Nodes** area, click **[-]** for the relevant label and node.
5. **To filter the labels:** enter the relevant string or keyword in the Labels box in the table header. The labels with names that include the relevant string are listed.

Add a node

1. Click **ADMINISTRATION** > **Nodes**.
2. In the Nodes area, click **+ ADD**.

   Enter the host name of the node, the name of a user that can remotely execute commands on the host (typically the root user), and the password of the specified user, and click **ADD** to remotely install the extra node.

You can also add a remote node manually as follows:

1. Copy the core platform binary file to the remote (worker) node as well as the client certificates that are required so the worker node can talk to the master node.
2. Unzip the core platform binary file.
3. Change to the relevant directory:
   `cd HPESW_ITOM_Suite_Platform_<timestamp_ID>`.

The install.properties file is the same as on the master node.

4. Copy the files specified in the `CLIENT_CA_FILE`, the `CLIENT_CERT_FILE`, and the `CLIENT_KEY_FILE` parameters in the `install.properties` file from the master node to the worker node:

   a. `scp root@<master node ip>:/opt/kubernetes/ssl/ca.crt /tmp` when prompted, enter the password.

   b. `scp root@<master node ip>:/opt/kubernetes/ssl/server.crt /tmp` when prompted, enter the password.

   c. `scp root@<master node ip>:/opt/kubernetes/ssl/server.key /tmp` when prompted, enter the password.

   d. `ls /tmp` to verify that the files have been copied.

5. Run the installation: `./install`.

6. Run `docker ps` to list the current container.

> **Tip:** Go to the master node and run `kubectl get nodes`. You should see two nodes.
>
> Go to the master node and run `kubectl describe nodes <worker_node_IP>` to get detailed information about the worker node. It is only running two pods `kube-proxy` and `kube-registry`.

View the node details

1. Click **ADMINISTRATION** > **Nodes**.

2. In the Nodes area, select a node name from nodes list.

   The page displays the CPU and memory usage history of the selected node for the past 15 minutes.

   The **Details** area displays details about the selected node as well as system information.

   The **Allocated resources** area displays the minimum CPU requests, CPU limits, memory requests, and memory limits for the container as well as the percentage of <what is in use>/<what is available>. By default, pods run with unbounded CPU and memory limits. The format is: <what is in use>/<what is available>.

   The **Conditions** area displays the type, status, last heartbeat and transaction time, reason, and message.

The **Pods** area displays the CPU and memory usage history of the pod for the past 15 minutes, the name of the pod, the status, number of restarts in the cycle, the amount of time passed since the pod has been created, the cluster IP, as well as the CPU and memory usage of the pod.

You can do the following:

- Click a Pod name to open the Workloads - Pods page for the pod.
- Click the menu icon to review the pod log.
- Click ⋮ **Actions** and select **Delete** to delete the pod.

The **Events** area displays the message, source, sub-object, count, first seen, and last seen information.

Manage licenses

The License page enables you to manage your suite licenses.

This section includes the following tasks:

- "View existing licenses" below
- "Install licenses" below
- "Archive a license" below
- "Restore an archived license" on the next page
- "Delete a license from the License Manager" on the next page
- "View the Licenses Report" on the next page

View existing licenses

1. Click **ADMINISTRATION** >**License** > **View Licenses**.

   Select the relevant product in **Select Product**. The page displays the license's feature ID and version, product number, capacity, start date, expiry date, the date when it was installed, who installed it, and the Lock Code.

Install licenses

1. Click **ADMINISTRATION** >**License** > **Install Licenses**.
2. Click **Choose file** to select the license file in your local system.
3. Click **Add More Files** to select another license file in your local system.
4. Click **Next**.

   The licenses that have been installed are displayed.

   You can select the license keys and click **Install Licenses** to install the licenses.

Archive a license

1. In the **View Licenses** tab, select the unused licenses you want to archive.

2. Click **Archive**.

The licenses are removed from the list of installed licenses in the License Management table and become unavailable for customers to fetch and activate the products.

Restore an archived license

1. In the **Archived Licenses** tab, select the product whose archived licenses you want to restore.
2. Select the licenses that you want to restore.
3. Click **Restore**.

The licenses are again displayed in the License Management pane and customers can check them out.

> **Note:** If ID locked licenses are auto archived, they cannot be restored unless all the licenses locked to a lock value belonging to same feature are either deleted or archived.

Delete a license from the License Manager

1. In the **Archived Licenses** tab, select the product whose licenses you want to delete.
2. Select the license to delete.
3. Click **Delete** and confirm the deletion.

View the Licenses Report

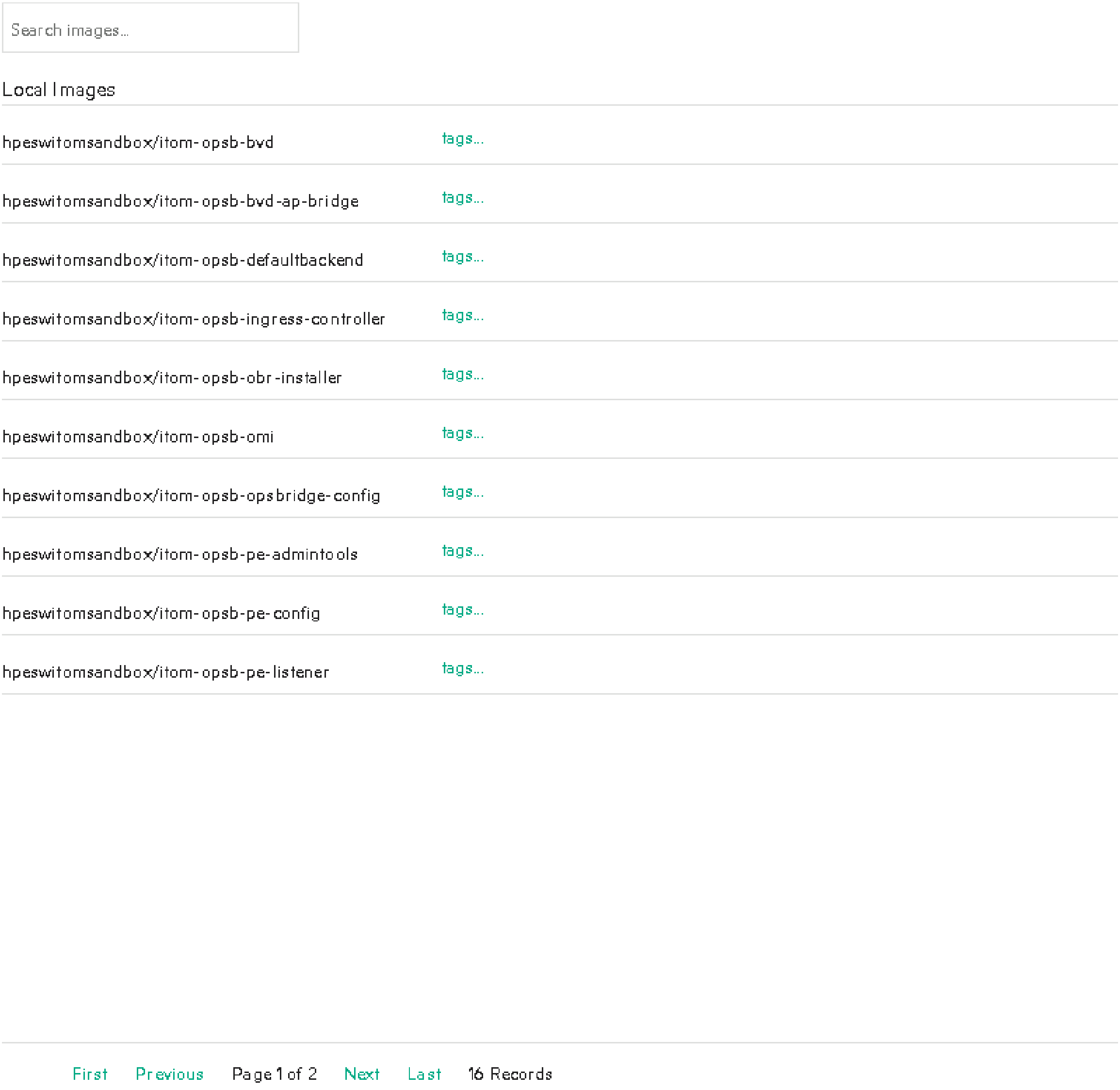
Click **ADMINISTRATION** > **LICENSE REPORT**.

The license report page tracks and displays the licenses currently installed and used on the License Manager. It also displays specific check out information about a feature license including the product name and version, the requester ID, and the timestamp of when it was accessed last.

You can export the license report details to Excel.

View the existing images

You can view the existing images in the local registry. Click **ADMINISTRATION > Local Registry**. The following page is displayed.



Search images...

Local Images

hpeswitomsandbox/itom-opsb-bvd	tags...
hpeswitomsandbox/itom-opsb-bvd-ap-bridge	tags...
hpeswitomsandbox/itom-opsb-defaultbackend	tags...
hpeswitomsandbox/itom-opsb-ingress-controller	tags...
hpeswitomsandbox/itom-opsb-obr-installer	tags...
hpeswitomsandbox/itom-opsb-omi	tags...
hpeswitomsandbox/itom-opsb-opsbridge-config	tags...
hpeswitomsandbox/itom-opsb-pe-admintools	tags...
hpeswitomsandbox/itom-opsb-pe-config	tags...
hpeswitomsandbox/itom-opsb-pe-listener	tags...

First Previous Page 1 of 2 Next Last 16 Records

Set up LW-SSO

The LWSSO page enables you to set up a single sign-on with other products.

> **Note:** The InitString and Domain of **LWSSO** have their own default values. You can also change these default values according to your needs.

1. Click **ADMINISTRATION** > **LWSSO**.
2. Enter the InitString and Domain and click **UPDATE**.

Manage resources

The **Resources** menu enables you to deploy containerized applications to a Kubernetes cluster, troubleshoot them, and manage the cluster and its resources itself. You can use it to get an overview of applications running on the cluster, as well as for creating or modifying individual Kubernetes resources and workloads, such as Daemon sets, Pet sets, Replica sets, Jobs, Replication controllers and corresponding Services, or Pods.

It also provides information on the state of Pods, Replication controllers, etc. and on any errors that might have occurred. You can inspect and manage the Kubernetes resources, as well as your deployed containerized applications. You can also change the number of replicated Pods, delete Pods, and deploy new applications using a deploy wizard.

Namespace

This section provides details about the selected Namespace.

Kubernetes supports multiple virtual clusters backed by the same physical cluster. These virtual clusters are called namespaces.

Select the namespace

You select a namespace to filter the information in the pages of the UI and display only the items related to the namespace.

1. Click **RESOURCES** > **Namespace** and select the relevant namespace.

   Resources will be displayed filtered by the specific namespace.

   The page shows the CPU and memory usage history for the selected namespace, for the past 15 minutes, the name of the namespace, its labels, pods, the timestamp of the creation of the namespace and its images.

   Click the relevant namespace to display more details.

View the namespace details

1. Click **RESOURCES** > **Namespace** and select the relevant namespace. You can also click **Workloads** > **Namespaces**, and click the relevant namespace.

The page shows details about the namespace and details about the events occurring in the core such as messages, source, count, first seen and last seen.

Workloads

This section displays information about Namespaces, Deployments, Replica Sets, Replication Controllers, Daemon Sets, Jobs, Pods, filtered by the selected namespace.

Click **RESOURCES** > **Workloads**.

The page displays all the resources filtered by the selected namespace:

- The CPU and memory usage of the selected namespace during the past 15 minutes.
- The list of replication controllers linked to the selected namespace.
- The list of pods linked to the selected namespace.

Deployments

You create and manage sets of replicated containers (actually, replicated Pods) using Deployments.

A Deployment provides declarative updates for Pods and Replica Sets (the next-generation Replication Controller).

A Deployment simply ensures that a specified number of pod “replicas” are running at any one time. If there are too many, it will kill some. If there are too few, it will start more.

You can select another namespace.

View the deployments

Click **RESOURCES** > **Workloads > Deployments**.

The page displays the CPU and memory usage history of the selected namespace during the past 15 minutes, the name of the available deployments, their labels, the number of pods, the creation timestamp of the deployment, and its images.

You can:

- Click a deployment to display its details.

  The details include information about the new replica set, the old replica sets, and the events that took place.

- Click ⋮ **Actions** and select **Delete**, to delete the deployment.

Replica Sets

Replica Sets are the next-generation Replication Controller. The only difference between a Replica Set and a Replication Controller is the selector support. Replica Sets support the new set-based selector requirements whereas a Replication Controller only supports equality-based selector requirements.

This section displays information about replica sets of the selected namespace.

View replica sets

1. Click **RESOURCES** > **Workloads** > **Replica Sets**.

   The page shows the CPU and memory usage history of the selected namespace during the past 15 minutes, the name of the available replica sets for the selected namespace, its labels, pods, images and creation timestamp.

   You can click ⋮ **Actions** and select **Delete** to delete a replica set.

View a replica set's details

1. Click **RESOURCES** > **Workloads > Replica Sets**.
2. Click the relevant replica set.

   The page shows details about the selected replica set, the services, pods, and events related to the replica set.

Replication controllers

The Replication Controllers page provides details about the Replication Controllers.

View the Replication Controllers

1. Click **RESOURCES** > **Workloads** > **Replication Controllers** to display the current Replication Controllers.

The page displays the CPU and memory usage of the selected namespace during the past 15 minutes, the list of replication controllers with their name, labels, pods, age, and images of the replication controllers associated with the selected namespace.

You can do the following:

- Click the relevant replication controller to view its details.

  The details display the CPU and memory usage history of the selected replication controller for the past 15 minutes, and the services provided by the selected replication controller.

- Click ⋮ **Actions** and select:

  - **View details.** You can also click the relevant replication controller.
  - **Scale.** See "Replication controllers" on the previous page.
  - **Delete.** The replication controller is deleted.

Scale the number of pods linked to the replication controller

1. Click **RESOURCES** > **Workloads** > **Replication Controllers**.

2. Click ⋮ and select **Scale**. Enter the relevant number of pods and click **OK**.

Daemon Sets

The Daemon Sets page provides information about the Daemon Sets for the selected Namespace.

A Daemon Set ensures that all (or some) nodes run a copy of a pod. As nodes are added to the cluster, pods are added to them. As nodes are removed from the cluster, those pods are garbage collected. Deleting a Daemon Set will clean up the pods it created.

View the daemon sets

1. Click **RESOURCES** > **Workloads** > **Daemon Sets** to display the current daemon sets.
2. Click the relevant daemon set to view its details.

Pet Sets

The Pet Sets page provides information about pet sets.

A Pet Set is a Controller that provides a unique identity to its Pods. It provides guarantees about the ordering of deployment and scaling.

View the Pet Sets

1. Click **RESOURCES** > **Workloads** > **Pet Sets** to display the current Pet Sets.
2. Click a Pet Set to view its details.

Pods

The Pods page provides information about the pods that are currently running or that have been running for the past 15 minutes. You can also access details about a specific pod as well as its log.

By default, pods run with unbounded CPU and memory limits. This means that any pod in the system will be able to consume as much CPU and memory on the node that executes the pod.

You may want to impose restrictions on the amount of resources a single pod in the system may consume for a variety of reasons.

View the Pods

1. Click **RESOURCES> Workloads** > **Pods**.

   The page displays the CPU and memory usage history of the namespace the pod belongs to, status, number of restarts during the lifecycle of the pod, the amount of time passed since the creation of the pod, the IP address of the pod, the CPU and memory usage of the pod itself in the last 15 minutes.

   - Click ≡ to display the log of the pod. See "View log" on the next page.
   - Click ⋮ **Actions** and select to delete the pod or to view and edit its YAML.
   - Click the pod itself to display its details. See "View a pod's details" below.

View a pod's details

1. Click **RESOURCES** > **Workloads** > **Pods**, and then click the relevant Pod.

   The page displays the CPU and memory usage history of the pod in the last 15 minutes, the pod details, and the network details. To display the log of the pod, see "View log" on the next page.

Also included is information about the pod containers such as the name, image, environment variables, commands, arguments, and more.

View log

1. Click **RESOURCES** > **Workloads** > **Pods**.
2. Click the relevant pod.
3. Click ≡ in the Pod page or **View logs** in the Pod Details page or click **View logs** in the Container area. The page displays the information for the pod.

   You can use the following tools:

   - Tт Toggles to change the size of the font used in the log.
   - A Toggles to change the colors of the log: white characters on black background or black characters on white background.
   -
     Logs from 10/31/16 7:23 AM to 10/31/16 7:37 AM The timestamp of the currently displayed log.
   - |< < > >| Use the relevant buttons to navigate between logs.

Services and discovery

Click **RESOURCES** > **Services** and discovery to display information about services and Ingress.

Services

The Services page provides information about services.

A service defines a set of pods and a means by which to access them, such as single stable IP address and corresponding DNS name (such as a web service or API server) that directs and load balances traffic to the set of pods that it covers.

View services

Click **RESOURCES** > **Services and Discovery** > **Services**.

The page displays the names of the services attached to the selected namespace, the labels assigned to the service, the IP of the related cluster, and the internal and external endpoints.

- Click ⋮ **Actions** and select **Delete** to delete the service.
- Click the relevant service to display its details. See "Services and discovery" on the previous page.

View a service's details

Click **RESOURCES** > **Services and Discovery** > **Services**, and then click the relevant Service.

The page displays details about the service and the connection as well as information about the related pods.

Ingress

An Ingress is a collection of rules that allow inbound connections to reach the cluster services.

It can be configured, for example, to give services externally reachable URLs, load balance traffic, terminate SSL, or offer name based virtual hosting. Users request ingress by POSTing the Ingress resource to the API server. An Ingress controller is responsible for fulfilling the Ingress, usually with a load balancer, though it may also configure your edge router or additional frontends to help handle the traffic in an HA manner.

View ingress

Click **RESOURCES** > **Services and discovery** > **Ingress**.

The page displays the names of the ingresses attached to the selected namespace, the labels assigned to the ingress, the IP of the related cluster, and the internal and external endpoints.

Click an ingress to view its details.

Persistent Volume Claims

The Persistent Volume Claims page displays information about the currently running persistent volumes.

A persistent volume claim is bound to a persistent volume. The claim is subsequently used inside a container volume specification. This provides volume technology abstraction for the suite deployment as suites request size and access type rather than a certain specific storage provider.

A volume is a directory, possibly with some data in it, which is accessible to the containers in a pod.

View the Persistent Volume Claims

Click **RESOURCES** > **Persistent Volume Claims**.

The page displays the name of the persistent volume, the volume it belongs to, the labels, and the timestamp of the creation of the persistent volume.

Each suite will have at least one persistent volume but may have more depending on the suite.

You can click the relevant volume to display its details.

View a persistent volume claim details

1. Click **RESOURCES** > **Persistent Volume Claims**, and then click the relevant Persistent Volume Claims. The page that opens displays detailed information about the persistent volume claim.

> **Tip:** To see the contents of **itom-vol**, go to the master node (the NFS server) and enter **cd /var/vols/itom/core**. It contains the **baseinfra-<version-number>** and the **suite-install** subdirectories.
>
> Enter **ls -R baseinfra-<version-number>**; this shows the **PrivateRegistry**.
>
> Enter **ls -R suite-install/**; this shows information about the containers that includes the configuration information to deploy the supported suites.

Configuration

Click **RESOURCES** > **Configuration** to display information about Secrets and Config Maps.

Secrets

The Secrets page provides information about secrets that are currently running.

A secret stores sensitive data, such as authentication tokens, which can be made available to containers upon request.

View the Secrets

Click **RESOURCES** > **Configuration** > **Secrets** .

The page displays the list of secrets and their age.

You can click the relevant secret to display its details. The page displays the details of the selected secret and its data.

Config Maps

The Config Maps page provides information about the config maps that are currently running.

The ConfigMap API resource holds key-value pairs of configuration data that can be consumed in pods or used to store configuration data for system components such as controllers. ConfigMap is similar to Secrets, but designed to more conveniently support working with strings that do not contain sensitive information.

View the Config Maps

Click **RESOURCES** > **Configuration** > **Config Maps**.

The page displays the names of the configuration map and its labels, and the amount of time passed since the configuration map was created.

- Click ⋮ and select **Delete** to delete the config map.
- Click the relevant config map to display its details. The page displays the selected config map details, and its related data.

Security

This section is intended for the ITOM Platform implementers and system administrators who need to implement their ITOM Platform environment in a secure manner.

This section includes the following information:

Secure Implementation and Deployment

This section provides information on implementing and deploying the ITOM Platform container-based platform in a secure manner.

Technical system landscape

The ITOM Platform is a container that integrates with other Suites. The ITOM Platform container-based platform is written in Java and JavaScript and Go.

For more information about typical deployment schemes and options, see ITOM Platform Architecture.

Security in the ITOM Platform configurations

The ITOM Platform configurations may be deployed in the following three implementations. See ITOM Platform Architecture.

- Single mode.
- Distributed mode 1 (one master node and multiple worker nodes).
- Distributed mode 2 (multiple master nodes and multiple worker nodes).

All of these implementations share the same basic out-of-the-box security configuration options.

1. In an out-of-the-box default installation, the Transport Layer Security/Secure Socket Layer (TLS/SSL) security is enabled between the browser and the ITOM Platform server by default.
2. In an out-of-the-box default installation, the ITOM Platform requires users to enter username and password credentials to gain access to the application.

External Authentication

With additional configuration, it is possible to supplement or replace the default authentication & authorization provider for the ITOM Platform by using a variety of industry-standard protocols and tools such as LDAP and Single Sign-On. See Configure LDAP.

Common Security Considerations

The ITOM Platform can only be deployed on supported operating systems. See Operating Systemin the *Support Matrix*.

It is recommended to follow vendor-provided best practices and security hardening guides for each of the third-party components used in support of your ITOM Platform deployment, which includes Docker, Kubernetes, Vault and Nginx, NFS. Below are some resources that can serve as a starting point for researching these recommended security considerations:

Docker Security Tips

https://www.docker.com/docker-security

Kubernetes Security Tips

http://kubernetes.io/docs/troubleshooting/

Vault Security Tips

https://www.hashicorp.com/security.html

Nginx Security Tips

http://nginx.org/en/security_advisories.html

NFS Security Tips

http://www.cert.org/historical/advisories/

The ITOM Platform Security Parameters

This section contains reference to some of the ITOM Platformparameters that are relevant to security.

Secure File Storage

The ITOM Platform allows users to upload files (suite installation binary) to the ITOM Platform Server. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojans.

As a result, it is strongly recommended to implement proper antivirus protection for the file storage.

Installation Security

This section provides information on aspects of installation security.

Operating Systems

Harden SSH on OS

On each node, the SSH server is configured with weak cipher and weak KexAlgorithms by default.

Set the values of **KexAlgorithms**, **Ciphers** and **MACs** in file: /etc/ssh/sshd_config as follows:

- **KexAlgorithms** ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256
- **Ciphers** aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
- **MACs** hmac-sha2-256

Database Security Recommendations

PostgreSQL

See http://www.openscg.com/postgresql-security-guidelines/ for information about PostgreSQL database security solutions.

Application Server Security Recommendations

Always change default passwords.

Always use the minimal possible permissions when installing and running the ITOM Platform.

Action	Permissions Needed for User
Installing/Running HPE ITOM Platform	You must install and run root permissions using the sudo command.

Network and Communication

This section provides information on network and communication security.

Secure Topology

The ITOM Platform is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

Several measures are recommended to securely deploy the ITOM Platform:

- Use of the TLS/SSL communication protocol

Replace the Certificate of Ingress Service with a Customized Certificate

Users can replace the certificate and private key of **Ingress Service** with a customized certificate and private key. Follow the steps below:

1. Generate a certificate and private key for the **host name**, of which host the **Ingress Service** is running on. And put it somewhere on the master node.
2. on master node, delete a secret with command:

   ```
   kubectl delete secret nginx-default-secret -n core
   ```

3. on master node, recreate the secret with a new certificate and private key

   ```
   echo "
   apiVersion: v1
   kind: Secret
   metadata:
   name: nginx-default-secret
   namespace: core
   data:
   ```

```
tls.crt: `base64 <certificate file name with absolute path> |tr -d \"\n\"`
tls.key: `base64 <private key file name with absolute path> |tr -d \"\n\"`
" | kubectl create -f -
```

4. on master node, delete and recreate the ingress service

```
kubectl delete -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
kubectl create -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
```

FAQ

Question

Are exceptions required to be added to the firewall policy?

Answer

Browsers access HPE ITOM Platform via HTTPS ports (TCP/5443). End users need to add it to the firewall exception policy.

User Management and Authentication

This section provides information related to user management and authentication.

Authentication Model

The ITOM Platform supports the following authentication methods:

- Username and password authentication

  In an out-of-the-box default installation, the ITOM Platform requires users to enter username and password credentials to gain access to the application.

- LDAP authentication

  You can integrate the ITOM Platform to an LDAP directory service to share contact information across your network.

Authorization

This section provides information related to user authorization in ITOM Platform.

Authorization Model

Access to the ITOM Platform resources is authorized based on the user’s following settings:

- User name
- Session & Inactivity timer timeouts

Authorization Configuration

For detailed information on authorization configuration, refer to the ITOM Platform Online Help Center in the ITOM Platform Portal top right corner.

FAQ

Question

Can the ITOM Platform inherit users’ information and authorization profiles from an external repository, such as LDAP?

Answer

No.

Data Integrity

The database server is used as a simple data store and is responsible for all persistent storage. While the database contains definitions describing business logic, no processing is actually performed in this tier, other than create, read, update, and delete (CRUD) operations in response to requests from the ITOM Platform. Referential integrity is enforced by the application, thereby protecting transactions. In addition, the database captures a complete audit log of all changes to data.

The data backup procedure is also an integral part of data integrity and while the ITOM Platform does not provide native backup capabilities, the following guidelines should be considered:

- Database backup is especially important before critical actions such as upgrades.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since database backup can be a resource intensive process, it is strongly recommended to avoid running backups during peak demand times.

Encryption

This section provides information on data encryption in the ITOM Platform platform.

TLS/SSL Data Transmission

The ITOM Platform was configured to use TLS/SSL to transmit data between the server and browsers.

Customers can change the default value of SSL CIPHER through the following steps:

1. On master node, change the **ssl-ciphers** value in file **$K8S_HOME/objectdefs/nginx-ingress.yaml**.
2. Recreate the ingress container with the commands below:

   kubectl delete -f **$K8S_HOME/objectdefs/nginx-ingress.yaml**

   kubectl create -f **$K8S_HOME/objectdefs/nginx-ingress.yaml**

For detailed information, please refer to the online help topic, Working with Secure Sockets Layer (SSL) in a Production Environment. See the ITOM Platform Online Help Center in the ITOM Platform top right corner.

Encryption of stored database fields

The ITOM Platform uses proprietary algorithms when encrypting data stored in the database and uses HPE Identity Manager (IDM) to manage user passwords.

Logs

This section provides information related to logs.

Log and Trace Model

Recommendations:

- Pay attention to the log level and do not leave tracing or debug parameters enabled unnecessarily.
- Pay attention to log rotation/switching.

For detailed information, please refer to the online help topic, Tracing and Logging in the ITOM Platform Online Help Center in the ITOM Platform top right corner.

Network and Communication Security

HPE recommends that you add the iptables rules listed below to the following below tables.

> **Important:** Apart from the listed ports on the specific hosts, all other ports should be blocked at the local host level.

Target server to configure the rules	Required ports	Service	Direction	Short description
NFS server	111	NFS	Nodes ->NFS Server	NFS server port access by all nodes
NFS server	2049	NFS	Nodes ->NFS Server	NFS server port access by all nodes
Master Node	2380	Etcd	Master<-> Master	Etcd service port for etcd cluster communication
Master Node	4001	Etcd	Nodes -> Master	Etcd service port for connection from client
All Nodes in Cluster	4194	Kubernetes	Localhost only	Cadvisor for local kubelet
All Nodes in Cluster	5000	Private Registry	Localhost only	Registry port for local host
Ingress Node	5443	MngPortal	All -> Ingress Node	The port exposed on ingress node. all clients could access this port
Master Node	8200	Vault	Nodes->Master	Vault port for client connection
Master Node	8443	kubernetes	Nodes->Master	API server port for client connection
All Nodes in Cluster	10250	Kubernetes	Nodes->Nodes	Kubernete port for internal communication
	10251	Kubernetes	Nodes-	Kubernete port for

Target server to configure the rules	Required ports	Service	Direction	Short description
			>Nodes	internal communication
	10252	Kubernetes	Nodes->Nodes	Kubernete port for internal communication
	10255	Kubernetes	Nodes->Nodes	Kubernete port for internal communication
NFS server	20048	NFS	Nodes ->NFS Server	NFS server port access by all nodes

> Example:
>
> The cluster is installed on 10.10.10.10, 10.10.10.11, 10.10.10.12. The Master Node on: 10.10.10.10
>
> To add an iptable rules to port 8443 on the master node do the following:

```
iptables -I INPUT 1 -p tcp -m tcp -s 0.0.0.0/0 --dport 8443 -j DROP

iptables -I INPUT 1 -p tcp -s 127.0.0.1 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.10 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.11 --dport 8443 -j ACCEPT

iptables -I INPUT 1 -p tcp -s 10.10.10.12 --dport 8443 -j ACCEPT
```

Administer the Operations Bridge Suite

You can perform the following tasks to administer the Operations Bridge Suite in a container deployment:

"Replace the suite trial license" on page 37

"Configure scaling" on page 38

"Configure LDAP authentication" on page 39

"Access Command Line Interfaces" on page 43

"Access the JMX Console" on page 45

Replace the suite trial license

If you do not provide a perpetual license prior to the suite installation, the built-in 60-day trial license (InstantOn) is used.

If later you purchase a perpetual license after the installation, you can replace the trial license with the perpetual license. To do this, follow these steps:

1. Launch the ITOM Platform from a supported web browser:

   https://*<external_access_host>*:5443

   <external_access_host> is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

2. Log in as the admin user.
3. Click **ADMINISTRATION > License**.
4. Click **Install Licenses**.
5. Click **Choose File** to browse to the license file on your local drive, then click **Next**.

   The license details are displayed.

6. Select all listed licenses and click **Install Licenses**.
7. *Optional*. When the installation is complete, click **View Licenses** to view the installed licenses.

Configure scaling

You can improve your system availability and reliability by scaling your suite resources as required. You can scale single nodes, as well as multiple nodes.

By managing your resources, you can scale your system out or in. For example, by increasing a deployment's number of pod replicas, the deployment's load is automatically distributed across all pods.

How to scale a BVD deployment horizontally

1. Launch the ITOM Platform from a supported web browser:

   https://*<external_access_host>*:5443

   <external_access_host> is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

2. Log in as the admin user.
3. Go to **Resources**, and click **All namespaces**. In the drop-down list, select the namespace for the Operations Bridge Suite that was assigned during the installation (for example `opsbridge`).
4. Go to **Workloads** > **Deployments**. You can either scale out the receiver load (`bvd-receiver-deployment`), or the web server load (`bvd-www-deployment`).
5. For the deployment you want to scale out, click ⋮ **Actions** and select **View/edit YAML**. The Edit a Replica Set window opens.
6. Edit the line `spec replicas : 1`. Increase the number of pod replicas as required.
7. Click **Update**.
8. Wait until the deployment is updated. This might take a few minutes.
9. *Optional*. You can verify that the deployment has been updated correctly:

   a. Refresh the Deployments page. For the deployment you selected, the number of pods should have increased (for example `2/2` instead of `1/1`).

   b. Go to **Workloads** > **Replica Sets**, and verify that the number of the deployment's pod replicas increased as specified. The age displays for how long the pods have been running.

Configure LDAP authentication

With the default single sign-on authentication strategy for the Operations Bridge Suite, users are authenticated to all installed capabilities with the same credentials. User names and passwords are stored and verified by a central server so that a user needs only one account to access all capabilities.

A suite-specific Identity Management (IDM) server is used for the authentication. The IDM server is monitored by a single center policy server, and consists of a user repository, a policy store, and a web server agent installed over each of the capability's web servers communicating with the policy server. The IDM server controls users' access to various organizational resources, protecting confidential personal and business information from unauthorized users.

For optimal security, HPE recommends to either configure a TLS connection between the suite and the IDM server, or have the suite server and the IDM servers on the same secure internal network segment. Authentication is performed by the IDM server, and authorization is handled by the capabilities.

Additionally, you can configure LDAP authentication for BVD. Automatic user creation from LDAP servers simplifies the user management process for administrators as authentication is performed through the LDAP server.

You can use an external LDAP server to store user information (user names and passwords) for authentication purposes, instead of using the internal IDM service. You can manually create BVD users and LDAP users, and use LDAP servers to automatically create LDAP users in BVD.

> **Note:** LDAP should be configured *after* the installation of the Operations Bridge Suite.

How to configure LDAP

1. Launch the ITOM Platform from a supported web browser:

   https://*<external_access_host>*:5443

   <external_access_host> is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

2. Log in as the admin user.

3. Go to **ADMINISTRATION**> **LDAP**. In the Organization List, click **Provider**.

4. Click **ADD CONFIGURATION** to enter a valid LDAP configuration. For details on what to enter for each LDAP setting, see "LDAP settings" below.
5. Click **SAVE**.
6. Log on to your capabilities via LDAP:

   OMi: `https://<external_access_host>/omi`

   BVD: `https://<external_access_host>/bvd`

   `<external_access_host>` is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

LDAP settings

The LDAP settings contain parameters for the LDAP server configuration, LDAP attributes, and user login information.

Setting	Description
LDAP Server Information	
Name	Name of the LDAP configuration. This name cannot be changed when you reconfigure the settings.
Hostname	Fully-qualified domain name of the LDAP server. **Example**: `192.0.2.24`
Port	Port of the LDAP server. LDAP servers typically use port 389 or secure port 636.
Connection Security	Select **Connection Security: SSL** if an LDAPS URL is specified.
Base DN	The Distinguished Name (DN) of the LDAP entity from which you want to start your user search. **Example**: `CN=Users,DC=omi,DC=example,DC=com`
User ID (Full DN)	The Distinguished Name (DN) of a user with search privileges on the LDAP directory server. **Example**: `CN=Administrator,CN=Users,DC=example,DC=com`
Password	Password of the specified user ID.

User Authentication	
User Search Base	Parameters to indicate which attributes are to be included in the user search. **Example**: `CN=Users`
User Name	Name of the user with search privileges on the LDAP directory server. **Example**: `sAMAccountName`
User Search Filter	LDAP pattern to use when searching for a user account. **Example**: `(sAMAccountName={0})` The user search filter must include the pattern `{0}`, which is replaced with the user name entered on login. IDM does not support LDAP multiple search filter components like `(&(sAMAccountName={{username}})(objectclass=user))`.
Follow Referral	Select to follow LDAP referrals to another server that offers the requested information.
Search Subtree	Select to search the subtree below the base DN (including the base DN level).
User Attributes	
Common Name	Common name to be included in the user search. **Example**: `cn`
User Email	Property that contains the user's email address (specific to the selected LDAP vendor, for example MS Active Directory). **Example**: `mail`
Manager Identifier	Any attribute (for example DN or CN) of the user who is the user's manager. **Example**: `manager`
Manager Identifier Value	The value of the identifier. For example, if you specified the DN in the Manager Identifier field, enter `dn`.
User Avatar	Attribute for the user avatar image. You must specify an LDAP record property name that exists on the LDAP server. **Example**: `cn`
User Group	
Group Membership	List of comma-separated LDAP attributes to find groups in a user profile.

	> **Example**: `member,uniqueMember`
Group Name	LDAP name used to identify objects of the type group. > **Example**: `cn`
Group Search Filter	LDAP pattern to use when searching for a group account. > **Example**: `(objectclass=group)`

Access Command Line Interfaces

OMi and OBR provide several command line interfaces that are useful for automation and troubleshooting. To access the CLIs from within the Operations Bridge Suite container environment, the basic workflow is as follows:

1. Find the container that contains the CLI.

   ```
   [root@master]# kubectl get pods --all-namespaces | grep <omi|obr-server>
   ```

2. Start the shell.

   ```
   [root@master]# kubectl exec -ti <pod_id> bash -c <omi|obr-server> -n
   <namespace>
   ```

   For example: `kubectl exec -ti omi-2246081285-8u1e0 bash -c omi -n opsbridge1`

3. Execute the CLI.

For examples specific to OMi and OBR, see "Example: Access OMi command line interfaces" below and "Example: Access OBR command line interfaces: " below.

Example: Access OMi command line interfaces

1. Find the container that contains the CLI.

   ```
   [root@master]# kubectl get pods -n opsbridge1 -o name | grep omi
   pod/<container_id>
   ```

2. Start the shell.

   ```
   [root@master]# kubectl exec -ti <container_id> -n opsbridge1 -c omi bash
   omi:/ #
   ```

3. Execute the CLI, in this example, `opr-node`:

   ```
   omi:/ # /opt/HP/BSM/opr/bin/opr-node -username admin -list_nodes –all
   ```

Example: Access OBR command line interfaces:

1. Find the container that contains the CLI:

   ```
   [root@master]# kubectl get pods -n opsbridge1 -o name | grep obr-server
   pod/<container_id>
   ```

2. Start the shell.

   ```
   [root@master]# kubectl exec -ti <container_id> -n opsbridge1 -c obr-server bash
   obr-server:/ #
   ```

3. Execute the CLI, in this example, `abcMonitor`:

   ```
   obr-server:/ # abcMonitor -streamdef
   ```

Access the JMX Console

OMi and the RTSM provide JMX consoles that provide additional information and advanced configuration possibilities.
To access the JMX consoles from your container deployment, open the following URL from a supported web browser:

```
https://<external_access_host>/jmx-console
```

`<external_access_host>` is the fully qualified domain name of the host which you specified as `EXTERNAL_ACCESS_HOST` in the `install.properties` file during the ITOM Platform installation. Usually, this is the master node's FQDN.

Integration

You can integrate the capabilities of the Operations Bridge Suite to fully leverage the suite's benefits. See the following sections for information about OMi, BVD, PE, or OBR integrations.

OMi integrations

Integrating Operations Bridge Manager (OMi) with other software products is a great way to extend your IT management capability. You can integrate OMi with every component of the Operations Bridge Suite Premium:

Integration	Documentation
OMi - BVD	BVD Administration Guide
OMi - PE	See "Integrate Performance Engine with OMi" on page 48.
OMi - OBR	OBR Integration Guide
OMi - OA	See "Integrate Operations Agent with OMi" on page 49.

Most major integrations between OMi and other HPE products are described in *the OMi Integrations Guide*.

For a complete list of available product integrations, see the Integrations Catalog on HPE Software Support.

BVD integrations

Business Value Dashboard (BVD) can be integrated out-of-the-box with OMi and Operations Connector (OpsCx). You can also create your own integrations for any data source by writing an adapter for BVD. For more information, see the *BVD Administration Guide*.

PE integrations

Performance Engine (PE) can be integrated with OMi. You must configure the OMi infrastructure settings to set up the integration. For details, see "Integrate Performance Engine with OMi" on page 48.

OBR integrations

Operations Bridge Reporter can be integrated with OMi, and with other HPE products. For a complete list of available product integrations, see the Integrations Catalog on HPE Software Support.

The OBR - OMi integration is documented in the *OBR Integration Guide*.

Integrate Performance Engine with OMi

After installing Performance Engine, you must configure the infrastructure settings to integrate Performance Engine with OMi.

1. In OMi, go to **Administration** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Select the **Applications** context.
3. Select the **Performance Engine** from the drop-down list.
4. In the Performance Engine Node Infrastructure Setting, click ✎ **Edit**.

   You can use this parameter to configure the Performance Engine Node details from which OMi Performance Dashboard must request data. The value is required in the format `http://<external_access_host>:<port>`.

   The default port is `31387`.
5. Click **Save**. Alternatively, click **Restore Default** > **Save**, to reset the default values.
6. In the Performance Engine Node password, click ✎ **Edit** and specify the password that you set during the Performance Engine configuration.
7. Click **Save**.

Integrate Operations Agent with OMi

If Operations Agent is installed on one of the master or worker nodes, additional steps are required to integrate Operations Agent with OMi .

> **Caution:** If the agent is installed on an external node instead, these steps are **not** required.

Configure the agent to use a different port than the one used by default, and configure OMi to use this non-default port:

1. Make sure that your system has a virtual external hostname (for example `kubecluster.example.com`) which is different than the physical node name (for example `dock.example.com`).
   To do this, add an entry to the DNS server for the virtual hostname of the suite installation. This hostname must be resolvable for all agents that are installed on one of the Kubernetes nodes.
2. Configure the Agent to use a different server port (for example 384):

   ```
   ovconfchg -ns bbc.cb -set SERVER_PORT 384
   ```

3. Configure Operations Agent to use the virtual external hostname (`kubecluster.example.com`) as the management server name:

   ```
   opcactivate.sh -s <virtual_external_hostname>
   ```

4. Configure OMi to connect to the master node with the specified port (for example 384):

   ```
   ovconfchg -ns bbc.cb.ports -set PORTS dock.example.com:384
   ```

Troubleshooting

This section provides information that can help you troubleshoot problems you may encounter when installing and using the ITOM Platform and the Operations Bridge Suite.

- "Manual verification commands" below
- "Log files" on page 52
- "Common problems and limitations" on page 52

Manual verification commands

The following commands can be used to troubleshoot the ITOM Platform and the Operations Bridge Suite container deployment, for example to list namespaces and services.

Command	Description
`./kube-status.sh`	Displays the status of the K8S cluster.
`./kube-stop.sh`	Stops the K8S cluster.
`./kube-restart.sh`	Restarts the K8S cluster.
`./kube-start.sh`	Starts the K8S cluster.
`kubectl`	The command to interact with Kubernetes (K8S). **Tip:** To shorten the `kubectl`command, run the following command: `ln -s /usr/bin/kubectl /usr/bin/kl` This enables you to type `kl` instead of `kubectl`.
`kubectl cluster-info`	Summarizes information about some of the services that are running on the cluster, including Kubernetes master, KubeDNS for service discovery, and the endpoints of the KubeRegistry (if you are running a registry).
`kubectl get nodes`	Lists all nodes in the cluster.
`kubectl describe nodes`	Provides more specific information about the node, such as labels, events, capacity, CPU, memory, the maximum number of pods that the node can

Command	Description
`./kube-status.sh`	Displays the status of the K8S cluster.
`./kube-stop.sh`	Stops the K8S cluster.
`./kube-restart.sh`	Restarts the K8S cluster.
`<node_IP>`	support, system information on the node, external IP address, the pods that are running, the list of namespaces, and resources.
`kubectl get pods`	Lists all pods in the default namespace (used to separate the ITOM Platform services from the deployed suites).
`kubectl get pods -n=<namespace>`	Lists all the pods that are running on the specified namespace. For example, run `kubectl get pods -n=opsbridge1` to get a list of the pods running in the namespace `opsbridge1`.
`kubectl get pods --all-namespaces`	Lists all the pods that are currently running in the cluster.
`kubectl describe pod <pod_name> --namespace=< namespace>`	Displays details about a specified pod in a specified namespace, such as the image it is running, the port it is exposing, and the command (/hyperkube) that is running inside the container itself with their options, volumes, and more.
`kubectl exec <pod_name> -c <container> -n <namespace>`	Executes a command in the specified container. If no container is specified, the first container in the pod is selected. **Example**: `kubectl exec omi-1949254658-p3ipj -c omi -n opsbridge1 bash -ti` Executes a bash shell in the OMi container with the pod name `omi-1949254658-p3ipj` and the namespace `opsbridge1`. By executing a bash shell in the OMi container, you can call CLIs from inside the container. For more information, see the *Operations Bridge Suite Administration Guide*.
`kubectl get services --all-namespaces`	Displays all the services running in the cluster.
`kubectl logs <pod_name> --namespace=< namespace>`	Displays the log output for the specified pod.

Log files

To troubleshoot your issue, you can review the following log files.

Installation

`/opt/kubernetes/install-<date><time>.log`

NFS share

- `/var/vols/itom/opsbridge/`*`<namespace>`*`/omi/opt/HP/BSM/log/topaz_all.log`
- `/var/vols/itom/opsbridge/`*`<namespace>`*`/omi/opt/HP/BSM/log/jboss7_boot.log`
- `/var/vols/itom/opsbridge/`*`<namespace>`*`/omi/opt/HP/BSM/log/supervisor/nanny_all.log`
- `/var/vols/itom/opsbridge/opsbridge-opsbridge/pe/logs`

Login

`/var/vols/itom/opsbridge/`*`<namespace>`*`/omi/opt/HP/BSM/log/jboss/login.log`

OBR

- `/var/vols/itom/opsbridge/`*`<namespace>`*`/obr/obr-server/adminServer/logs` (Administration UI)
- `/var/vols/itom/opsbridge/`*`<namespace>`*`/obr/obr-server/Flink/log` (Flink)
- `/var/vols/itom/opsbridge/`*`<namespace>`*`/obr/obr-server/log` (OBR platform)
- `/var/vols/itom/opsbridge/`*`<namespace>`*`/obr/obr-server/data` (OBR data)
- `/var/vols/itom/opsbridge/<namespace>/obr/obr-server/config` (OBR configuration)

Common problems and limitations

You may encounter the following problems and limitations when installing or administering the ITOM Platform and the Operations Bridge Suite.

ITOM Platform is not accessible

Description

After the installation of the ITOM Platform, the ITOM Platform cannot be accessed at https://*<external_access_host>*:5443.

Possible solutions

- Make sure you entered the correct URL and port.
- Make sure you can access the host: `ping <external_access_host>`
- Check your browser's proxy settings.
- Check the installation logs in `/opt/kubernetes/install-<timestamp>.log`.
- Empty the NFS folder and then reinstall the ITOM Platform.
- See also "ITOM Platform is not accessible: nginx controller is Pending" below, "Troubleshooting" on page 50 and "Login to ITOM Platform is not possible: IDM service is not ready yet" on the next page.

ITOM Platform is not accessible: nginx controller is Pending

Description

After the installation of the ITOM Platform, the ITOM Platform cannot be accessed at https://*<external_access_host>*:5443.
When running `kubectl get pods --all-namespaces`, the nginx ingress controller status is Pending.

Cause and solution

The map hash bucket size might be too small. Check if that is the case by running the following commands:

```
kubectl describe nginx-ingress-controller-u69gg
```

```
kubectl logs nginx-ingress-controller-u69gg
```

If an error is displayed similar to `nginx: [emerg] could not build map_hash`, increase the `map_hash_bucket_size` as follows:

1. Access the file `/opt/kubernetes/objectdefs/nginx-ingress.yaml`
2. Locate the specified `map_hash_bucket_size` (32 by default) and increase it, for example to 128
3. Run the following commands to recreate the `nginx-ingress.yaml` file:

   ```
   kubectl delete –f /opt/kubernetes/objectdefs/nginx-ingress.yaml
   ```

   ```
   kubectl create –f /opt/kubernetes/objectdefs/nginx-ingress.yaml
   ```

4. *Optional*. If you get a warning about failed scheduling, the scheduling constraints could not be fulfilled. Execute the following command to fix this:

   ```
   kubectl label nodes role=loadbalancer –all
   ```

   The nginx pod container should then be started automatically.

5. After the OMi configuration, you must repeat steps 2 and 3 for the OMi nginx controller located at `/var/vols/itom/core/suite-install/opsbridge/output/suite-ingress-controller-configmap.yaml`

ITOM Platform is not accessible: Gateway time out

Description

After the installation of the ITOM Platform, the ITOM Platform cannot be accessed at https://<*external_access_host*>:5443. The Docker daemon cannot be started, and displays the error message `Gateway time out` when logging into IDM.

Cause and solution

Kubernetes might not be running. Run the following commands to start Kubernetes:

```
cd $K8S_HOME/bin
```

```
./kube-start.sh
```

Login to ITOM Platform is not possible: IDM service is not ready yet

Description

After the installation of the ITOM Platform, the ITOM Platform cannot be accessed at https://<*external_access_host*>:5443. The login failure error `The IDM service is not ready yet` is displayed, and the pods `autopass-lm`, `idm`, and `suite-installer` all have the status `CrashLoopBackOff`.

Solution

1. Run the following command:

   ```
   kubectl delete -f autopass-lm.yaml; kubectl delete -f autopass-pg.yaml; kubectl delete -f idm.yaml; kubectl delete -f idm-pg.yaml; kubectl delete -f suite.yaml
   ```

2. Delete the subfolders located in the NFS subdirectories `<NFS_HOME>/baseinfra-1.0/autopass_db`, `<NFS_HOME>/baseinfra-1.0/idm_db`, and `<NFS_HOME>/baseinfra-1.0/suite_db`.

3. Run the following command:

```
kubectl create -f idm-pg.yaml; kubectl create -f idm.yaml; kubectl create -f
autopass-pg.yaml; kubectl create -f autopass-lm.yaml; kubectl create -f
suite.yaml
```

"502 Bad Gateway" error when attempting to launch OMi

Description

After the installation of the Operations Bridge Suite, a 502 Bad Gateway error is displayed when trying to access OMi.

Cause and solution

The 502 error is displayed because OMi is not yet up and running. Depending on the host machine, it might take up to one hour for OMi to start after the initial configuration.

No server connection: invalid character "{" in host name

Description

A connection to the server could not be established. The log displays that the invalid character "{" is used in the host name.

Cause and solution

The firewall might still be enabled on the NFS server. Make sure that the firewall is disabled.

Pod is in ImagePullBackOff or ErrImagePull status: Image not found

Description

After the installation of the ITOM Platform, one of the pods has the status `ImagePullBackOff` or `ErrImagePull`. When running the command `kubectl describe pod <pod_name> -n <namespace>`, the following error message is displayed:

```
Image <image_name> not found
```

Cause and solution

Make sure the images are pushed into the private docker registry. To confirm, run the following command:

```
docker pull <image_name>
```

Pod is in ImagePullBackOff or ErrImagePull status: Error while pulling image

Description

After the installation of the ITOM Platform, one of the pods has the status `ImagePullBackOff` or `ErrImagePull`. When running the command `kubectl describe pod <pod_name> -n <namespace>`, the following error message is displayed:

```
Error while pulling image: Get http://localhost:5000/v1/repositories/xxx: dial tcp
[::1]:5000: getsockopt: connection refused
```

Cause and solution

To resolve this issue, delete the Docker registry and the registry proxy pods, and then restart them.

Worker node installation fails with a Flannel related error

Description

Setting up one or multiple worker nodes fails during the ITOM Platform installation due to an error related to Flannel.

Cause and solution

To troubleshoot and resolve this issue, do the following:

- Double check if the FQDN is resolved to the correct IP address on the master node.
- On the master node, run `kube-restart.sh`
- Reinstall the worker node from the ITOM Platform.

"503 nginx error" when attempting to run the Suite Installer

Description

After the installation of the ITOM Platform, a 503 Nginx error is displayed when trying to access the Suite Installer.

Cause and solution

This error might be displayed because the time on the master and worker nodes is different. To resolve this issue, synchronize the time on your nodes by using, for example, NTP or VMWare tools.

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 Administration Guide (Operations Bridge Suite 2017.04)

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!