



OpenShift Enterprise

2

2.2 Release Notes

Release Notes for OpenShift Enterprise

Red Hat OpenShift Documentation
Team

OpenShift Enterprise 2 2.2 Release Notes

Release Notes for OpenShift Enterprise

Red Hat OpenShift Documentation Team

Legal Notice

Copyright © 2017 Red Hat.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

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

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

The OpenShift Enterprise 2.2 Release Notes summarize all new features, major corrections from the previous version, and any known bugs upon general availability. Instructions are also included to help OpenShift Enterprise administrators to install and configure asynchronous updates to existing installations.

Table of Contents

Chapter 1. Introduction to OpenShift Enterprise	2
1.1. Installing OpenShift Enterprise 2.2	2
1.2. Upgrading to OpenShift Enterprise 2.2	2
Chapter 2. New Features	3
2.1. What's New in OpenShift Enterprise 2.2	3
2.2. Notable Technical Changes	4
Chapter 3. Bug Fixes	6
Chapter 4. Known Issues	11
Chapter 5. Asynchronous Errata Updates	12
Chapter 6. Product Support and Documentation	24
Appendix A. Revision History	25

Chapter 1. Introduction to OpenShift Enterprise

OpenShift Enterprise by Red Hat is a Platform as a Service (PaaS) that provides developers and IT organizations with an auto-scaling, cloud application platform for deploying new applications on secure, scalable resources with minimal configuration and management overhead. OpenShift Enterprise supports a wide selection of programming languages and frameworks, such as Java, Ruby, and PHP. Integrated developer tools, such as Eclipse integration, JBoss Developer Studio, and Jenkins, support the application life cycle.

Built on Red Hat Enterprise Linux, OpenShift Enterprise provides a secure and scalable multi-tenant operating system for today's enterprise-class applications while providing integrated application runtimes and libraries.

OpenShift Enterprise brings the OpenShift PaaS platform to customer data centers, enabling organizations to implement a private PaaS that meets security, privacy, compliance, and governance requirements.

1.1. Installing OpenShift Enterprise 2.2

See the current version of the [OpenShift Enterprise Deployment Guide](#) for instructions on how to deploy OpenShift Enterprise for the first time.

1.2. Upgrading to OpenShift Enterprise 2.2

If you have a previous version of an OpenShift Enterprise instance currently installed and would like to upgrade to OpenShift Enterprise 2.2, see the current edition of the [OpenShift Enterprise Deployment Guide](#).

Chapter 2. New Features

2.1. What's New in OpenShift Enterprise 2.2

OpenShift Enterprise 2.2 introduces the following new features:

New Cartridge Support

OpenShift Enterprise now supports the Ruby 2.0 cartridge through the use of the Software Collections Library (SCL). The JBoss Fuse, JBoss A-MQ, and Fuse Builder premium xPaaS cartridges, introduced in OpenShift Enterprise 2.1.7, are available with add-on subscriptions in OpenShift Enterprise 2.2 as well.

Highly-available Deployments Using `oo-install`

The `oo-install` installation utility can now be used to install a highly-available OpenShift Enterprise deployment by defining services across multiple hosts configured for redundancy. By default without the `-a` option, the installation utility scales and installs ActiveMQ and MongoDB services along with the broker hosts that are defined. If the `-a` option is used, you can define these services on separate hosts as well. See the [OpenShift Enterprise Deployment Guide](#) for more information.

Routing Daemon for Use with an External Routing Layer

A supported routing daemon can be used as a listener with an external routing layer to dynamically control traffic to gears and allow OpenShift Enterprise applications to achieve high availability. The initial version of the routing daemon can be configured to use an `nginx` or `Nginx Plus®` routing back end. See the [OpenShift Enterprise Deployment Guide](#) for more information on the routing daemon as well as new information on selecting an external routing solution.

Gear Placement Plug-in and Example Algorithms

A supported gear placement plug-in, which allows administrators to control the placement of gears as they are created, is now shipped with OpenShift Enterprise. The plug-in also provides a number of example gear placement algorithms for use with the plug-in. See the [OpenShift Enterprise Deployment Guide](#) for instructions on installing the plug-in and implementing your own custom algorithm.

Gear Size Restriction for Cartridges

Administrators can now associate cartridges with specific gear sizes to restrict the size of deployed applications using the `VALID_GEAR_SIZES_FOR_CARTRIDGE` broker configuration setting. This allows developers to deploy certain applications on appropriate infrastructures. For example, administrators can set a gear size to a corresponding cartridge for applications that requires a faster CPU or more RAM to run at a higher proficiency. See the [OpenShift Enterprise Administration Guide](#) for more information.

Additional DNS Plug-ins

Administrators can now use one of several available DNS plug-ins that make dynamic, real-time updates to a DNS domain to publish OpenShift Enterprise applications. The Fog DNS plug-in uses cloud DNS services and can currently be configured for use with Rackspace® Cloud DNS, and the DYN® DNS plug-in uses the DYN® Managed DNS service. In addition to BIND, the `nsupdate` DNS plug-in supports integration with other compatible DNS services, such as Infoblox®. See the [OpenShift Enterprise Deployment Guide](#) for instructions on configuring these DNS plug-ins.

Region Selection Using Management Console and Client Tools

Region selection by developers was previously only possible using a REST API call. If allowed by administrators, developers can now use the Management Console or the client tools to select an available region for their applications. See the [OpenShift Enterprise User Guide](#) for more information on regions.

Mutual SSL Authentication

Administrators can now configure their deployment to use mutual SSL authentication, commonly referred to as x509 or two-way authentication. After the broker has been configured, developers must also configure their client tools appropriately. This feature allows for a developer (the SSL client) to authenticate to an application (the SSL server) and vice versa. Each side has a verification certificate, which is shared upon connection. This feature ensures an additional level of security in your deployment, because without the approved authentication certificate a developer is unable to connect to the SSL server. See the [OpenShift Enterprise Deployment Guide](#) for administrator instructions and the [OpenShift Enterprise User Guide](#) for developer instructions.

Integration with Identity Management

OpenShift Enterprise can integrate with Identity Management (IdM) on Red Hat Enterprise Linux to take advantage of its various features. IdM provides a simple, centralized solution to securely manage user authentication. Integration with IdM is ideal because its authorization and authentication framework easily supports protocols such as Kerberos, LDAP, DNS, NTP, and x509 authentication. See the [OpenShift Enterprise Deployment Guide](#) for instructions on integrating Active Directory authentication with Identity Management in your OpenShift Enterprise deployment.

Gear Firewall Tool

The new `oo-gear-firewall` command creates firewall rules and SELinux policy to contain services running on gears to their own internal gear IPs. This prevents access to unprotected network resources running in another developer's gear. This command is invoked by default during new installations of OpenShift Enterprise 2.2 to restrict access to services running on different gears. Administrators should run the following on node hosts in existing deployments after upgrading to 2.2:

```
# oo-gear-firewall -i enable -s enable
```

See the man page for the `oo-gear-firewall` command for more details.

IPv6 Tolerance

Red Hat now supports OpenShift Enterprise deployments using a mixed IPv4 and IPv6 topology. See the [OpenShift Enterprise Deployment Guide](#) for requirements and known issues when using this type of deployment.

Supported Puppet Module

A supported Puppet module is now available for deploying OpenShift Enterprise. See the new [OpenShift Enterprise Puppet Deployment Guide](#) for details and installation instructions.

2.2. Notable Technical Changes

OpenShift Enterprise 2.2 includes the following notable technical changes:

New OpenShift Enterprise 2.2 Channels

Distinct channels have been created for OpenShift Enterprise 2.2 for both RHN Classic and Red Hat Subscription Management. See the *OpenShift Enterprise Deployment Guide* ^[1] for an updated list of channel names and for more information on available repositories.

Default Front-end Server Proxy Plug-in

Starting with OpenShift Enterprise 2.2, the **apache-mod-rewrite** front-end server proxy plug-in is deprecated. New deployments of OpenShift Enterprise 2.2 now use the **apache-vhost** plug-in as the default.



Important

Any new nodes added to your deployment after an upgrade to 2.2 will use the **apache-vhost** plug-in by default. The **apache-mod-rewrite** plug-in is incompatible with the **apache-vhost** plug-in, and the front-end server configuration on all nodes across a deployment must be consistent. See the [OpenShift Enterprise Deployment Guide](#) for more information on upgrading from 2.1 to 2.2.

If your OpenShift Enterprise 2.1 deployment was configured to use the **apache-mod-rewrite** plug-in before starting the 2.2 upgrade, you can optionally allow the **ose-upgrade** tool to migrate your node hosts to the **apache-vhost** plug-in while upgrading to 2.2. The default behavior of the **ose-upgrade** tool, however, is to leave the **apache-mod-rewrite** plug-in in place, if installed. See the [OpenShift Enterprise Deployment Guide](#) for more information.

Rsyslog7 Packages

OpenShift Enterprise (OSE) 2.1 was originally released on Red Hat Enterprise Linux (RHEL) 6.5. In order for the **mmopenshift** plug-in to work, the *rsyslog7* package from RHEL 7 was shipped in the OSE 2.1 channel. Later, RHEL 6.6 shipped its own *rsyslog7* package that was incompatible with the one from OSE. This created many edge cases for RPM conflicts and confusing configurations.

This release updates the **rsyslog7-mmopenshift** package for compatibility with RHEL 6.6. The **openshift.sh** installation script and the **ose-upgrade** tool used for upgrading from 2.1 to 2.2 have been updated to handle the configuration changes as well. The *rsyslog7* package from RHEL 6.6 conflicts with the base *rsyslog* package. A manual upgrade can be done with the following steps:

```
# cp -f /etc/rsyslog7.d/* /etc/rsyslog.d/

# yum shell --disableplugin=priorities -y <<YUM
# erase rsyslog rsyslog7-7.4.7 rsyslog7-mmopenshift-7.4.7
# install rsyslog7 rsyslog7-mmopenshift
# transaction run
# YUM

# sed -i 's/rsyslog7.d/rsyslog.d/' /etc/rsyslog.conf
# service rsyslog start
```

[1] See https://access.redhat.com/documentation/en-US/OpenShift_Enterprise/2/html-single/Deployment_Guide/index.html#sect-Configuring_Broker_Host_Entitlements for broker host entitlements. See https://access.redhat.com/documentation/en-US/OpenShift_Enterprise/2/html-single/Deployment_Guide/index.html#sect-Configuring_Node_Host_Entitlements for node host entitlements.

Chapter 3. Bug Fixes

OpenShift Enterprise 2.2 fixes the following bugs:

[BZ#1093192](#)

The `/etc/openshift-enterprise-release` file was not consistently updated when a host updated to a newer asynchronous release (for example, release 2.1.7). This was due to the `openshift-enterprise-release` RPM package, which provides the file, only being consistently updated for use during minor release upgrades (for example, upgrading from release 2.0 to 2.1). This issue led to confusion when trying to later determine the installed asynchronous release of an OpenShift Enterprise deployment. This bug fix updates the file to "OpenShift Enterprise 2.2.0" and future asynchronous releases will ensure that this file is updated accordingly.

[BZ#1154471](#)

OpenShift Enterprise (OSE) 2.1 was originally released on Red Hat Enterprise Linux (RHEL) 6.5. In order for the `mmopenshift` plugin to work, the `rsyslog7` package from RHEL 7 was shipped in the OSE 2.1 channel. Later, RHEL 6.6 shipped its own `rsyslog7` package that was incompatible with the one from OSE. This created many edge cases for RPM conflicts and confusing configurations. This bug fix updates the `rsyslog7-mmopenshift` package for compatibility with RHEL 6.6. The `openshift.sh` installation script and the `ose-upgrade` tool used for upgrading from 2.1 to 2.2 have been updated to handle the configuration changes as well. The `rsyslog7` package from RHEL 6.6 conflicts with the base `rsyslog` package. A manual upgrade can be done with the following steps:

```
# cp -f /etc/rsyslog7.d/* /etc/rsyslog.d/

# yum shell --disableplugin=priorities -y <<YUM
# erase rsyslog rsyslog7-7.4.7 rsyslog7-mmopenshift-7.4.7
# install rsyslog7 rsyslog7-mmopenshift
# transaction run
# YUM

# sed -i 's/rsyslog7.d/rsyslog.d/' /etc/rsyslog.conf
# service rsyslog start
```

[BZ#1121195](#)

When the `EXTERNAL_ETH_DEV` parameter in the `/etc/openshift/node.conf` file was set to a device that did not have a globally scoped IPv4 address, such as "lo", the `oo-iptables-port-proxy` command failed with unhelpful output. As a result, after an application creation failed because of this issue, it was difficult to determine the root cause when investigating logs on a node host. This bug fix adds logic to the `oo-iptables-port-proxy` command to produce better logs when a device does not have a globally scoped IPv4 address, and the logs when investigating this type of issue are now more clear.

BZ#[1153893](#)

Previously, attempting to use the client tools with OpenShift Enterprise (OSE) environments that had SSLv3 disabled resulted in connection errors. This was due to an issue with the `rubygem-httpclient` and `ruby193-rubygem-httpclient` packages prior to version 2.4, which were what shipped in OSE channels. This bug fix updates the `rubygem-httpclient` package in the OSE Client Tools channel and the `ruby193-rubygem-httpclient` package in the OSE Broker Infrastructure channel both to version 2.4. As a result, the client tools now connect successfully with OSE environments that have SSLv3 disabled.

BZ#[1100102](#)

The `oo-diagnostics` tool did not verify the source of the package dependencies for the `python-3.3` cartridge as it did for the `python-2.7` cartridge. As a result, it was possible for these packages to be missed during the tool's RPM test if they were installed from an unsupported source. This bug fix adds the relevant packages to the tool's RPM test and the `python-3.3` cartridge dependencies are now properly verified.

BZ#[1123850](#)

For applications using a PostgreSQL cartridge, any configuration changes made to the `~/postgresql/data/postgresql.conf` file were overwritten when the cartridge was restarted. However, some applications require certain values for the `datestyle` and `locale` settings in this file in order to run correctly. This bug fix adds the `OPENSIFT_POSTGRESQL_DATESTYLE` and `OPENSIFT_POSTGRESQL_LOCALE` environment variables for the PostgreSQL cartridges, and users can now set these values persistently.

BZ#[1131167](#)

Previously, when attempting to quit while using the `oo-install` installation utility, the installation process instead continued. This bug fix updates the utility to ensure quitting while configuring the deployment successfully returns to the main menu and quitting from the main menu exits the utility completely. Configuration values are still saved in the `~/openshift/oo-install-cfg.yml` file.

BZ#[1131190](#)

When stopping an application that used a JBoss EWS cartridge, cartridge log files did not show any information related to the stop action. This issue was due to the cartridge sending a `SIGKILL` to the processes instead of a `SIGTERM`. This bug fix updates the JBoss EWS cartridge control logic, and cartridge logs for these applications now show information related to the stop action.

BZ#[1144940](#)

When adding an invalid SSL certificate to an existing application alias, the Management Console did not show any information regarding the validity of the certificate file or key or the success of the operation. The client tools, however, did show this information for the same operation. This bug fix updates the Management Console to show the same error messages as the client tools when adding invalid SSL certificates to existing aliases.

BZ#[1145810](#)

The HAProxy cartridge did not consider a "401 unauthenticated" status code valid for health checks. As a result, when a scaled application required HTTP Basic Authentication, the HAProxy health checks failed and marked the server as down, resulting in a 503 internal server error response from the application. This bug fix updates the HAProxy cartridge to add 401 to the default expected status codes for health checks, and applications requiring HTTP Basic Authentication can now work in scaled mode. This bug fix also provides the ability for administrators and users to change the expected status code list and the health check URI values using the `OPENSIFT_HAPROXY_HTTPCHK_EXPECT_RSTATUS` and `OPENSIFT_HAPROXY_HTTPCHK_URI` environment variables.

BZ#[1151244](#)

On a node host, placing any files in the `/var/lib/openshift/.cartridge_repository` directory that were not cartridge directories and restarting the MCollective service caused MCollective to fail. A warning message was reported in logs, and the process continued without error, however no messages were serviced or sent. This bug fix updates this logic to allow for any files in the `.cartridge_repository` directory, and MCollective now operates correctly in this scenario.

BZ#[1152698](#)

Previously, the PostgreSQL cartridges were missing dates and time stamps in their logs. This bug fix updates these cartridges, and their logs now include dates and timestamps.

BZ#[1152699](#)

After using the Management Console to add a SSL certificate with a separate certificate chain file to an application alias, some browsers reported the site as untrusted. This was due to a bug in the Management Console's logic to strip certificate content when appending a chain file. This bug fix updates this logic, and SSL certificates added using this method now validate correctly.

BZ#[1153663](#)

OpenShift Enterprise node web proxies previously had SSLv3 enabled, making them susceptible to POODLE-style attacks. This bug fix updates the node web proxies to remove SSLv3 support, and as a result they are no longer susceptible to these issues.

BZ#[1153750](#)

The `oo-iptables-port-proxy` command had a typo in its usage output. This bug fix updates the usage `"showproxies"` to instead show the correct usage `"showproxy"`.

BZ#[1152700](#)

Previously, incomplete deployments that had never been activated caused the broker to no longer update the deployments list for the application. This created a situation where the user would be unable to rollback a failed deployment if the last successful deployment was after an incomplete one. This bug fix updates node logic to skip incomplete deployments when reporting to the broker, and as a result users can successfully rollback deployments in this scenario.

BZ#[1140289](#)

Previously, background requests made to the broker from the Management Console were performed under a hard-coded timeout of 10 seconds. As a result, it was possible to hit this timeout under certain conditions, for example due to users having a high number of domains and gears or network latency. This bug fix adds the `BACKGROUND_REQUEST_TIMEOUT` parameter to the `/etc/openshift/broker.conf` file on broker hosts, and this timeout is now a configurable value (in seconds).

BZ#[1144057](#)

If a gear size is already in use, for example by being an allowed size for a user domain, an administrator later removing that size from the `VALID_GEAR_SIZES` list in the `/etc/openshift/broker.conf` file can cause validation problems during subsequent operations. For example, an error would occur while attempting to add a new gear size to an existing user domain where the removed size was still allowed. This bug fix updates the `oo-admin-chk` tool to check for inconsistencies in allowed gear sizes between domains in MongoDB records and the valid gear sizes in the broker configuration. This bug fix also adds the `--gear-size` option to the `oo-admin-repair` tool which fixes such inconsistencies by removing all invalid gear sizes from the allowed sizes list of all domains.

BZ#[1145877](#)

The Management Console did not display vendor names when multiple cartridges had the same name, while the client tools did make this distinction. This bug fix updates the Management Console to show the vendor of a cartridge when more than one cartridge has the same name.

As a result, it now easier to distinguish between cartridges in the Management Console in these scenarios.

BZ#[1146224](#)

This release updates the version of HAProxy provided by the haproxy15side package to 1.5.4.

BZ#[1148192](#)

Previously, there was a race condition when using the apache-vhost front-end server plug-in. If the "oo-httpd-singular graceful" command was run to incorporate one gear vhost update while another gear was creating its vhost configuration, the configuration was left in a bad state and the httpd service would not restart. As a result, the vhost configuration would cease being updated and newly-added gears would be unreachable via the vhost front-end server. If the httpd service was stopped, it would fail to start until the configuration was fixed. This bug fix extends a lock around the call to the oo-httpd-singular command, and as a result the race condition no longer occurs.

BZ#[1156200](#)

The oo-admin-ctl-iptables-port-proxy command uses the "iptables -L" command in several places, which by default attempts to reverse-resolve the IPs listed to host names. Since most of the IPs on a node are internal and have no host name associated, all configured name servers may be consulted once for each rule in the tables. If all nameservers are appropriately configured, "service openshift-iptables-port-proxy restart" tends to take a few seconds. If any name servers are unreachable or slow in responding, resolving several thousand internal IPs was reported to take over an hour. This bug fix adds the -n flag to the iptables command used by oo-admin-ctl-iptables-port-proxy command so that it does not attempt to reverse-resolve IPs, which was unnecessary to begin with. As a result, the "service openshift-iptables-port-proxy restart" command completes in sub-second timing under either condition.

Chapter 4. Known Issues

This chapter highlights known issues in the OpenShift Enterprise 2.2 release.

[BZ 1394328](#)

If needed, administrators can choose to configure the JBoss EWS cartridge *tomcat7* binary provided by the EWS 3 product to work around known security issues with the JBoss EWS-2 *tomcat7* binary. To enable the use of the EWS 3 *tomcat7* binary, use the following command to update *tomcat7* on each node:

```
# yum update tomcat7 --enablerepo jws-3-for-rhel-6-server-rpms
```

This change will affect all JBoss EWS cartridges on the node. Running JBoss EWS cartridges will not see any changes until they are restarted. All new JBoss EWS cartridges will use the updated *tomcat7* binary.

If using JBoss EWS 3 binaries with the EWS 2 cartridge, ensure that you are using the Java 1.7 binaries, or you will see issues with the cartridge. EWS 3 is only certified to run with Java 1.7.

[BZ 1097928](#)

When using RHN Classic, the `oo-admin-yum-validator --oo-version 2.2 --fix-all` command does not automatically subscribe a system to the OpenShift Enterprise 2.2 channels, but instead reports the manual steps required. This command is also automatically run during the `ose-upgrade begin` step when upgrading to OpenShift Enterprise 2.2, therefore upgrades using RHN Classic also require manual intervention. After the channels are manually subscribed, running either command again sets the proper `yum` priorities and continues as expected.

[BZ 1084035](#)

When scaling up a scalable application with a large minimum number of gears, newly created gears are deleted automatically before the scale up is finished, until the number of gears is the same as before the scale up.

[BZ 871569](#)

While Red Hat supports OpenShift Enterprise deployments using a mixed IPv4 and IPv6 topology starting in the 2.2 release, full IPv6 connectivity is not supported, and OpenShift Enterprise has not been tested as such. Some components that may be affected are listed in the bug report. See the [OpenShift Enterprise Deployment Guide](#) for requirements and known issues regarding IPv6 tolerance.

[BZ 1029173](#)

If you delete the Jenkins builder gear (from JBoss Developer Studio) and try to rebuild an application, the build fails because the build can not be found. This seems to be caused because Jenkins keeps a list of builders, and upon builder deletion (using REST calls), Jenkins does not get cleaned up.

[BZ 1029174](#)

Jenkins Server fails to build a re-created application that uses the same name as a previously deleted application. To work around this issue, delete the Jenkins job before creating an application using the same name as a deleted application.

Chapter 5. Asynchronous Errata Updates

Security, bug fix, and enhancement updates for OpenShift Enterprise 2.2 are released as asynchronous errata through the Red Hat Network. All OpenShift Enterprise 2 errata is available on the Red Hat Customer Portal at <https://rhn.redhat.com/errata/rhel6-rhose2-errata.html>. See <https://access.redhat.com/support/policy/updates/openshift> for more information about asynchronous errata.

Red Hat Customer Portal users can enable errata notifications in the account settings for Red Hat Subscription Management (RHSM) or Red Hat Network (RHN) Classic. When errata notifications are enabled, users are notified via email whenever new errata relevant to their registered systems are released.



Note

Red Hat Customer Portal user accounts must have systems registered and consuming OpenShift Enterprise entitlements for OpenShift Enterprise errata notification emails to generate.

Additional Update Instructions per Release

The latest [OpenShift Enterprise Deployment Guide](#) provides general instructions on how to apply asynchronous errata updates within a minor release. Some errata have additional instructions specific to that release that must be performed to fully apply the update to a host. The general instructions provided in the [OpenShift Enterprise Deployment Guide](#) reference [Table 5.1, “Additional Update Instructions per Release”](#) in this section, which details the releases that require additional steps.

Running the **yum update** command on a host installs packages for all pending updates at once. If you are applying multiple asynchronous errata updates at once, any additional update instructions for all releases being installed must be performed. However, the steps can be aggregated in this situation when commands would be unnecessarily repeated. When evaluating which additional steps must be performed for multiple pending asynchronous errata updates, consider the following general workflow:

1. Run the **yum update** command on each host.
2. Restart relevant services.
3. Import, activate, and migrate the latest cartridge manifests on the broker host, if relevant.
4. Run the **oo-admin-upgrade** command on the broker host to upgrade existing gears, if relevant.

[Table 5.1, “Additional Update Instructions per Release”](#) details whether certain parts of the above workflow are relevant to the errata updates you are applying.

Example 5.1. Applying Multiple Asynchronous Errata Updates at Once

For example, if you are updating an OpenShift Enterprise release 2.2.0 deployment to release 2.2.2, see [Table 5.1, “Additional Update Instructions per Release”](#) and read through the additional instructions for releases 2.2.1 and 2.2.2. The instructions listed for these two releases can be aggregated into the following steps:

1. After running the **yum update** command on each host, run the following on each node host:

```
# service ruby193-mcollective restart
```

2. Restart the routing daemon, if installed:


```
# service openshift-routing-daemon restart
```

3. Run the following on the broker host:

```
# service openshift-broker restart
# service openshift-console restart
# oo-admin-ctl-cartridge -c import-node --activate --obsolete
# oo-admin-ctl-cartridge -c migrate
# oo-admin-upgrade archive
# oo-admin-upgrade upgrade-node --version=2.2.2
```

Note that the `oo-admin-upgrade upgrade-node` command is only run once, using the version for the latest release being applied.

Table 5.1. Additional Update Instructions per Release

Release	Advisory	Additional Instructions
2.2.1	RHBA-2014:1903	<p>After running the <code>yum update</code> command on each host and ensuring all packages have been updated, restart the <code>ruby193-mcollective</code> service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other <code>oo-admin-upgrade</code> command usage and use <code>2.2.1</code> as the target <code>--version</code>.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.1</pre>

Release	Advisory	Additional Instructions
2.2.2	RHBA-2014:1979	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service and, if installed, the Management Console service:</p> <pre># service openshift-broker restart # service openshift-console restart</pre> <p>Restart the routing daemon, if installed:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.2 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.2</pre>
	RHBA-2014:1978	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the routing daemon, if installed:</p> <pre># service openshift-routing-daemon restart</pre>

Release	Advisory	Additional Instructions
2.2.3	RHBA-2015:0019	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective and openshift-watchman services on each node host:</p> <pre># service ruby193-mcollective restart # service openshift-watchman restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.3 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.3</pre>

Release	Advisory	Additional Instructions
2.2.4	RHBA-2015:0220	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service:</p> <pre># service openshift-broker restart</pre> <p>Restart the routing daemon, if installed:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.4 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.4</pre>

Release	Advisory	Additional Instructions
2.2.5	RHBA-2015:0779	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective and openshift-watchman services on each node host:</p> <pre># service ruby193-mcollective restart # service openshift-watchman restart</pre> <p>On the broker host, restart the broker service:</p> <pre># service openshift-broker restart</pre> <p>Restart the routing daemon, if installed:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.5 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.5</pre>

Release	Advisory	Additional Instructions
2.2.6	RHBA-2015:1463	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the broker service and, if installed, the Management Console service on the broker host:</p> <pre># service openshift-broker restart # service openshift-console restart</pre> <p>Restart the routing daemon, if installed and integrated with F5 BIG-IP LTM®:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.6 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.6</pre> <p>Restart rsyslog7 on each node host, if installed:</p> <pre># service rsyslog restart</pre>

Release	Advisory	Additional Instructions
2.2.7	RHSA-2015:1844	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service:</p> <pre># service openshift-broker restart</pre> <p>Restart the routing daemon, if installed and integrated with F5 BIG-IP LTM®:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.7 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.7</pre> <p>Users must restart their gears for the changes in this release to take effect.</p>

Release	Advisory	Additional Instructions
2.2.8	RHSA-2015:2666	<p>After running the yum update command on each host and ensuring all packages have been updated, restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service:</p> <pre># service openshift-broker restart</pre> <p>Restart the routing daemon, if installed and integrated with F5 BIG-IP LTM®:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.8 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.8</pre> <p>Users must restart their gears for the changes in this release to take effect.</p>

Release	Advisory	Additional Instructions
2.2.9	RHSA-2016:0489	<p>After running the yum update command on each host and ensuring all packages have been updated, restart ActiveMQ on any broker or messaging host running the service:</p> <pre># service activemq restart</pre> <p>Restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service and, if installed, the Management Console service:</p> <pre># service openshift-broker restart # service openshift-console restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.9 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.9</pre> <p>Users must restart their gears for the changes in this release to take effect.</p>

Release	Advisory	Additional Instructions
2.2.10	RHSA-2016:1773	<p>After running the yum update command on each host and ensuring all packages have been updated, restart ActiveMQ on any broker or messaging host running the service:</p> <pre># service activemq restart</pre> <p>Restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service and, if installed, the Management Console service:</p> <pre># service openshift-broker restart # service openshift-console restart</pre> <p>Restart the routing daemon, if installed and integrated with F5 BIG-IP LTM®:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.10 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.10</pre> <p>Users must restart their gears for the changes in this release to take effect.</p>

Release	Advisory	Additional Instructions
2.2.11	RHBA-2017:0017	<p>After running the yum update command on each host and ensuring all packages have been updated, restart ActiveMQ on any broker or messaging host running the service:</p> <pre># service activemq restart</pre> <p>Restart the ruby193-mcollective service on each node host:</p> <pre># service ruby193-mcollective restart</pre> <p>On the broker host, restart the broker service and, if installed, the Management Console service:</p> <pre># service openshift-broker restart # service openshift-console restart</pre> <p>Restart the routing daemon, if installed and integrated with F5 BIG-IP LTM®:</p> <pre># service openshift-routing-daemon restart</pre> <p>On the broker host, import and activate the latest cartridge manifests, then migrate old cartridge versions to the latest active versions. Note that this may also activate cartridges that you have previously deactivated, so you may need to again deactivate any cartridges that you want to remain deactivated.</p> <pre># oo-admin-ctl-cartridge -c import-profile - -activate --obsolete # oo-admin-ctl-cartridge -c migrate</pre> <p>On the broker host, archive previous upgrade data and upgrade all nodes. Alternatively, to only upgrade a single node or gear, see the OpenShift Enterprise Deployment Guide for other oo-admin-upgrade command usage and use 2.2.11 as the target --version.</p> <pre># oo-admin-upgrade archive # oo-admin-upgrade upgrade-node -- version=2.2.11</pre> <p>Users must restart their gears for the changes in this release to take effect.</p>

Chapter 6. Product Support and Documentation

Product Support

Product support is available at <http://www.redhat.com/support>.

Product Documentation

Product documentation for OpenShift Enterprise is available at https://access.redhat.com/knowledge/docs/OpenShift_Enterprise/.

Appendix A. Revision History

Revision 1.0-15	Thu Jun 15 2017	Ashley Hardin
Updated Chapter 4, Known Issues to note JBoss EWS 3 is only certified to run with Java 1.7.		
Revision 1.0-14	Wed Jan 4 2017	Ashley Hardin
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2017-0017 .		
Revision 1.0-13	Wed Nov 23 2016	Ashley Hardin
Updated Chapter 4, Known Issues to add BZ 1394396 and its workaround.		
Revision 1.0-12	Wed Aug 24 2016	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHSA-2016:1773 .		
Revision 1.0-11	Tue Mar 22 2016	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHSA-2016:0489 .		
Revision 1.0-10	Thu Dec 17 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHSA-2015:2666 .		
Revision 1.0-9	Wed Sep 30 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHSA-2015:1844 .		
Revision 1.0-8	Wed Jul 22 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2015:1463 .		
Revision 1.0-7	Mon Apr 6 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2015:0779 .		
Revision 1.0-6	Thu Feb 12 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2015:0220 .		
Revision 1.0-5	Thu Jan 8 2015	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2015:0019 .		
Revision 1.0-4	Wed Dec 10 2014	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2014:1979 and RHBA-2014:1978 .		
Revision 1.0-3	Tue Nov 25 2014	Alex Dellapenta
Updated Chapter 5, Asynchronous Errata Updates with instructions for RHBA-2014:1903 .		
Revision 1.0-2	Mon Nov 10 2014	Alex Dellapenta
Updated Section 2.1, "What's New in OpenShift Enterprise 2.2" to include "Supported Puppet Module".		
Revision 1.0-1	Thu Nov 6 2014	Alex Dellapenta
Fixed minor publication issue.		
Revision 1.0-0	Tue Nov 4 2014	Alex Dellapenta
OpenShift Enterprise 2.2 release.		

