



Red Hat Update Infrastructure 2.1

Installation Guide

Installation and Configuration of Red Hat Update Infrastructure

Red Hat Update Infrastructure 2.1 Installation Guide

Installation and Configuration of Red Hat Update Infrastructure

Red Hat Update Infrastructure Documentation Team

Legal Notice

Copyright © 2017 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). 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 Red Hat Update Infrastructure Installation Guide provides requirements and instructions for the installation and initial configuration of Red Hat Update Infrastructure for cloud providers.

Table of Contents

CHAPTER 1. INTRODUCTION TO RED HAT UPDATE INFRASTRUCTURE	3
1.1. SYSTEM OVERVIEW	3
CHAPTER 2. INSTALLATION REQUIREMENTS	6
2.1. PREREQUISITES	6
2.2. DOWNLOADING ENTITLEMENTS	7
2.3. PACKAGE INSTALLATION	10
CHAPTER 3. RED HAT UPDATE INFRASTRUCTURE INSTALLER	13
3.1. SETTING UP SSL	13
3.2. EDITING THE ANSWERS FILE	16
3.3. ADDING A CONTENT DELIVERY SERVER	21
3.4. UPDATING RED HAT UPDATE INFRASTRUCTURE	22
APPENDIX A. REVISION HISTORY	23
INDEX	28

CHAPTER 1. INTRODUCTION TO RED HAT UPDATE INFRASTRUCTURE

The Red Hat Update Infrastructure (RHUI) enables cloud providers to deploy Red Hat solutions into their cloud environments. Using Red Hat Update Infrastructure, cloud providers enable customers to update Red Hat technology in a customer's cloud-based deployment.

An X.509 certificate grants access to the Red Hat Enterprise Linux and Red Hat Update Infrastructure channels, including ISO images and RPM packages.



IMPORTANT

Both Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6 require appropriate GPG keys to work with Red Hat Update Infrastructure, and different packages supply these keys to the two operating systems. The packages required are:

- for Red Hat Enterprise Linux 5 — **redhat-release-5Server**
- for Red Hat Enterprise Linux 6 — **redhat-release-server**

Once installed and configured, Red Hat Update Infrastructure tools are used to create Red Hat Update Appliance (RHUA) and Content Delivery Server (CDS) instances. CDS instances are then managed and monitored by the Red Hat Update Appliance.

Using Red Hat Update Infrastructure, initial configuration, initialization, and synchronization of cloud-based Red Hat technology instances requires little user configuration or intervention. In some use cases, however, cloud-specific configuration is required. For example:

- Setting a storage volume mount point in the cloud to store installation or update packages synchronized from the Red Hat Customer Portal.
- Configuring network security for intra-cloud communications.
- Adding monitoring checks other than those offered by Red Hat.



NOTE

Because Red Hat Update Infrastructure updates packages, when the **yum list** command is run on a system using Red Hat Update Infrastructure, all package versions are returned. Despite this, Red Hat Update Infrastructure can only supply the latest available version of a package when clients are updated.

1.1. SYSTEM OVERVIEW

Red Hat Update Infrastructure comprises the following technologies:

- the Red Hat Update Appliance (RHUA). The Red Hat Update Appliance is a system instance that runs in the cloud by default. It
 - synchronizes packages from an external source (such as the Red Hat Customer Portal).
 - monitors status and provides both machine and human-readable update reports.
 - manages one or more Content Delivery Servers.

- the Content Delivery Server (CDS). A CDS serves packages to cloud-based clients via HTTPS.

1.1.1. Communication

1. The cloud provider accesses a central third-party content repository, such as Red Hat Customer Portal. Note: the Red Hat Update Appliance can connect to the content repository using a cloud provider's network proxy server.
2. The Red Hat Update Appliance synchronizes content to the CDS instances, and evenly distributes requests. Note: Each CDS serves as a load balancer. There is no need to install the load balancer either as a separate instance or as part of the Red Hat Update Appliance.
3. CDS instances distribute content via HTTPS to cloud-hosted Red Hat Enterprise Linux instances.

[Report a bug](#)

1.1.2. Certificates

Red Hat Update Infrastructure uses three different types of X.509 certificates:

Content certificate

The content certificate and its associated private key are given to the customer to allow access to Red Hat Customer Portal. This grants permission to the customer to download the Red Hat Update Infrastructure packages or ISO. Additionally, the Red Hat Update Appliance uses this certificate when authenticating with Red Hat Customer Portal to download updated packages into the Red Hat Update Infrastructure environment.

Content certificates are signed by the Red Hat Certificate Authority (CA). This is the only certificate in the Red Hat Update Infrastructure public key infrastructure (PKI) that is not signed by the cloud provider.

Entitlement certificate

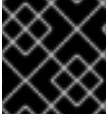
Clients use an entitlement certificate when connecting to CDS instances. The entitlement certificate contains entitlements for some or all of the products initially granted to the cloud provider in the content certificate. A client using an entitlement certificate can only get access to channels for which the certificate provides an entitlement.

The entitlement certificate must be signed by a Certificate Authority (CA). This allows you to generate entitlement certificates for use in your environment without having to request them from Red Hat. All requests to the Red Hat Update Infrastructure that test the entitlement certificate will check that it was signed by the CA. This prevents users from spoofing the Red Hat Update Infrastructure with self-signed certificates.

SSL Certificates

SSL is used for communicating with CDS instances. SSL requires that a new SSL certificate is generated for each instance. For example, in an environment with three CDS instances, three separate certificates will need to be generated. The common name (CN) of the certificate must match the hostname of the instance.

Red Hat does not restrict CA certificate choice. CA certificates can be: from a trusted source (for example VeriSign); subordinate certificates in a trust chain from an established certificate; or generated new using a tool such as openssl.

**IMPORTANT**

Always ensure your private key is well protected to avoid security breaches.

[Report a bug](#)

CHAPTER 2. INSTALLATION REQUIREMENTS

This chapter details the requirements that must be met before installing Red Hat Update Infrastructure on your environment.

2.1. PREREQUISITES

Cloud Provider Prerequisites

The following are prerequisites to becoming a certified Red Hat Cloud Provider. These must be fulfilled prior to installing and configuring Red Hat Update Infrastructure in a cloud environment.



NOTE

Red Hat Enterprise Linux 6 is required to successfully install and run Red Hat Update Infrastructure. The latest version of Red Hat Enterprise Linux 6 is supported for the Red Hat Update Appliance Server and Content Delivery Server. Red Hat Enterprise Linux versions 5, 6, and 7 are supported for the Red Hat Update Infrastructure client. For more information on installing Red Hat Enterprise Linux, refer to the *Red Hat Enterprise Linux Installation Guide*.

- Complete a Cloud Provider Agreement with Red Hat. Cloud providers must be certified by Red Hat in order to be able to resell Red Hat Enterprise Linux.
- Ensure you have an entitlement for every Red Hat Update Appliance instance in the cloud. This grants access to:
 - Red Hat Update Infrastructure (Red Hat Update Appliance and associated technologies).
 - 32-bit and 64-bit Red Hat Enterprise Linux images. This is required to perform instantiation.
 - Permission for the Red Hat Update Appliance to synchronize channel content from Red Hat Customer Portal.
- The ability to generate or obtain CA and SSL certificates. These are required for configuring SSL and signing client entitlement certificates.
- Employ a method of monitoring that includes some means of notification and the ability to run custom scripts and commands.

Hardware and Storage Requirements

Red Hat Update Infrastructure has the following hardware and storage requirements:

- The latest version of Red Hat Enterprise Linux
- 64-bit architecture.
- At least 2 GB of available memory
- At least 4 GB of available swap space

Ensure that you have allocated enough storage space for the RPM packages required by Red Hat Update Infrastructure.

All repositories are placed under `/var/lib/pulp`. Create this directory only if you need to create a new mount point for it; otherwise, it is automatically created during the installation process.

The `/var/lib/pulp` requires at least 40 GB of storage for each binary package repository and approximately double the allocated storage for each debug-info repository during Full Support Phase of a major Red Hat Enterprise Linux version. Note that, after the period, the estimated annual growth rates of these repositories are 10 GB per binary package repository and 20 GB per debug-info repository.

All repositories are synchronized with Content Delivery Server (CDS) nodes under `/var/lib/pulp-cds`.



NOTE

If you expect to be storing a large amount of data, consider using a separate storage volume for the installation.

Network and Firewall Requirements

Red Hat Update Infrastructure uses various network protocols for communication between Red Hat Update Appliance, CDS, and client instances. The following table outlines each of the protocols used:

Table 2.1. Protocols and Port requirements

Port	Protocol	Source	Destination	Notes
443	HTTPS	RHUA	Package Source	Third-party repository such as Red Hat Customer Portal
443	HTTPS	Client	CDS	Used by yum on the client to retrieve packages
5674	QPID	RHUA	CDS	Used for communication between the Red Hat Update Appliance and the CDS
5674	QPID	CDS	RHUA	Used for communication between the Red Hat Update Appliance and the CDS



IMPORTANT

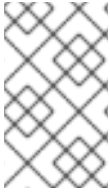
Every CDS instance must have access to ports 443 (HTTPS) and 5674 on the Red Hat Update Appliance in order to synchronize packages.

[Report a bug](#)

2.2. DOWNLOADING ENTITLEMENTS

Procedure 2.1. Downloading Entitlements from the customer portal

In order to use Red Hat Update Infrastructure, you need an entitlement for every Red Hat Update Appliance instance in the cloud. You can download the entitlement ISO from the Red Hat customer portal.



NOTE

Ensure you have activated your subscription before attempting to download entitlements from the customer portal. For help with activating your subscription, contact Red Hat Customer Service.

1. Go to the customer portal at <http://access.redhat.com> and click on the **Subscriptions** link.
2. Scroll down to the **Manage** section and click the **RHUI** link.
3. Click **Register a RHUI**.

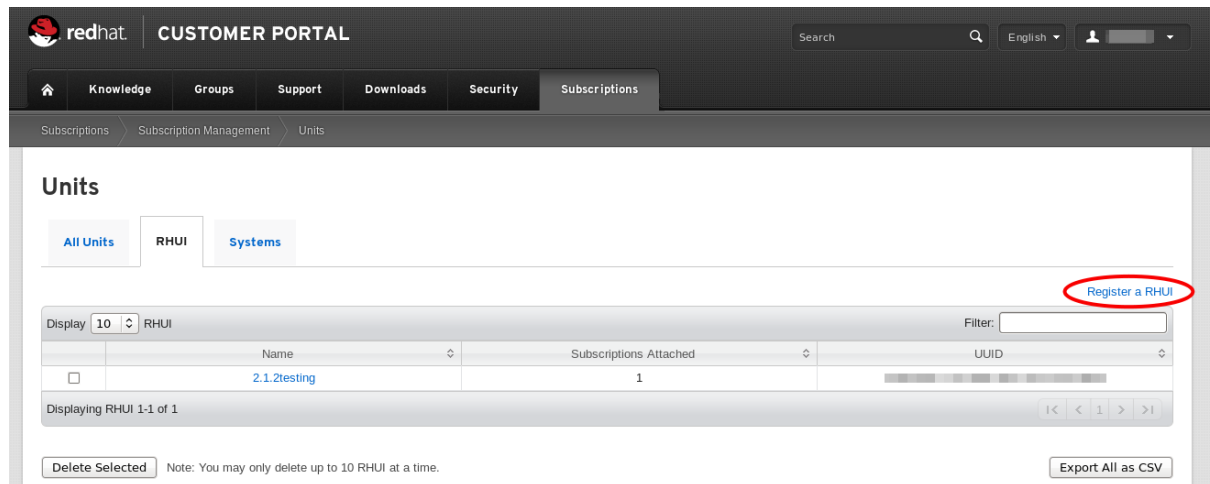


Figure 2.1. Create a New RHUI

4. On the **Register a New RHUI** page, enter the name of the Red Hat Update Appliance instance, select a version, and click **Register**.

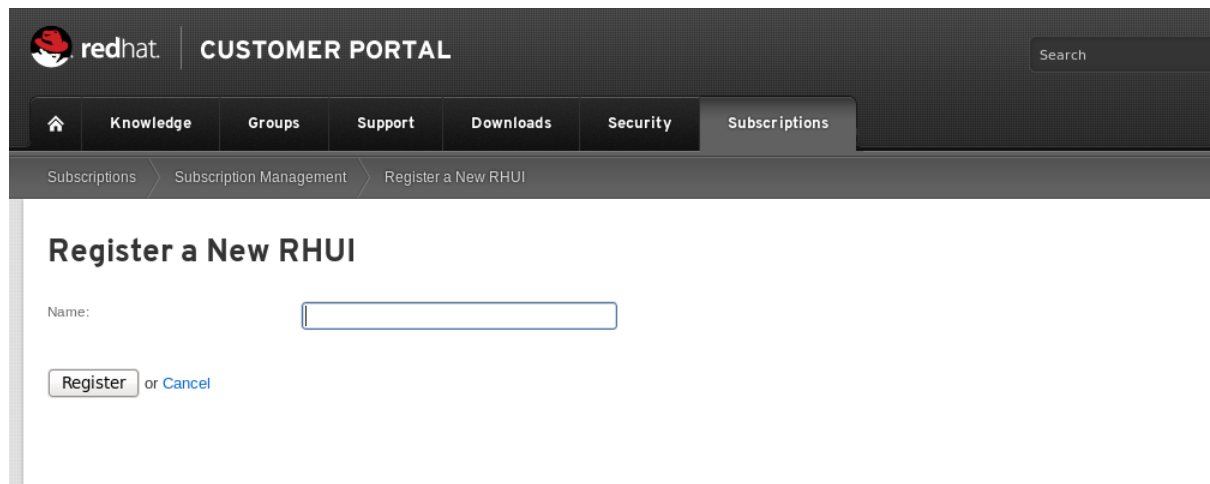


Figure 2.2. Register a New RHUI

5. Your new Red Hat Update Appliance instance will not yet have any subscriptions applied to it. Add a subscription by clicking **Attach a subscription** in the bottom right corner. A list of available subscriptions will be displayed. Select the check box next to the desired subscription and click **Attach Selected** to add it to the instance.

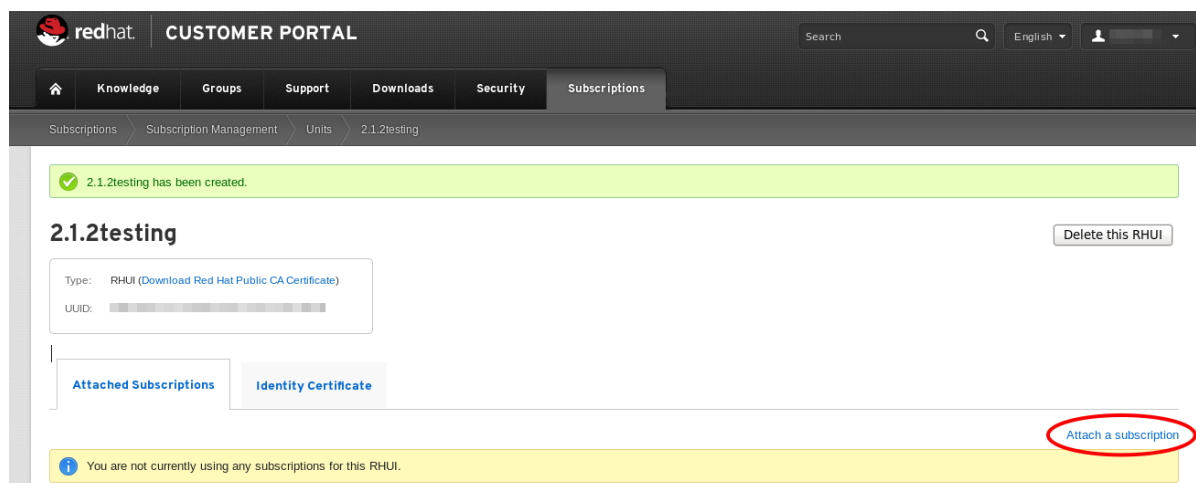


Figure 2.3. Adding Subscriptions

- Download the entitlement certificate by clicking **Download** in the **Entitlement Certificate** column of the subscriptions table. Save the entitlement certificate on your local machine and note down the location. You will need this information later when you install the Red Hat Update Infrastructure ISO.

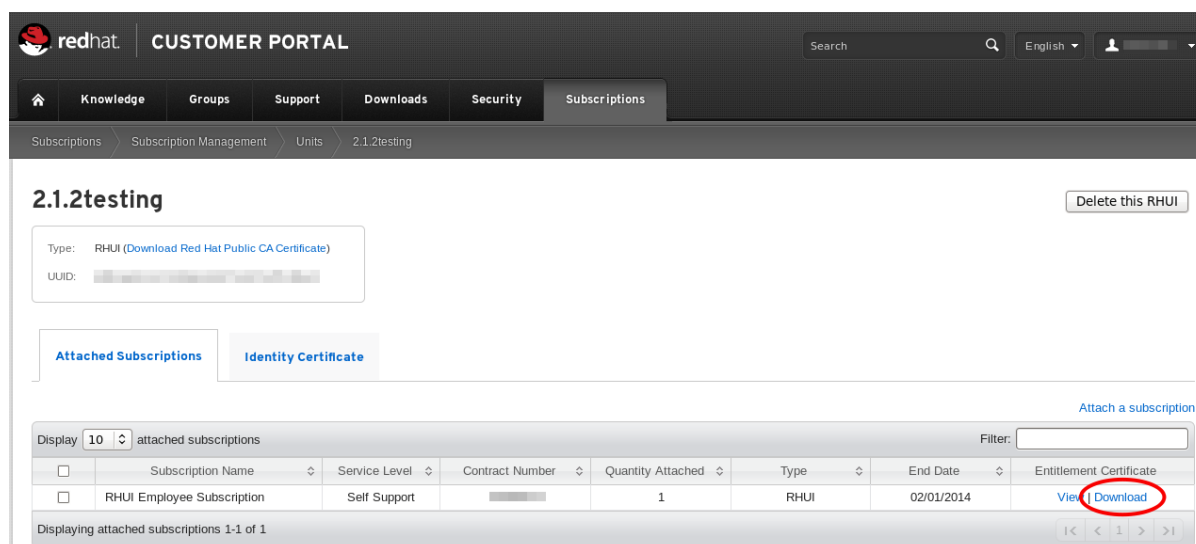


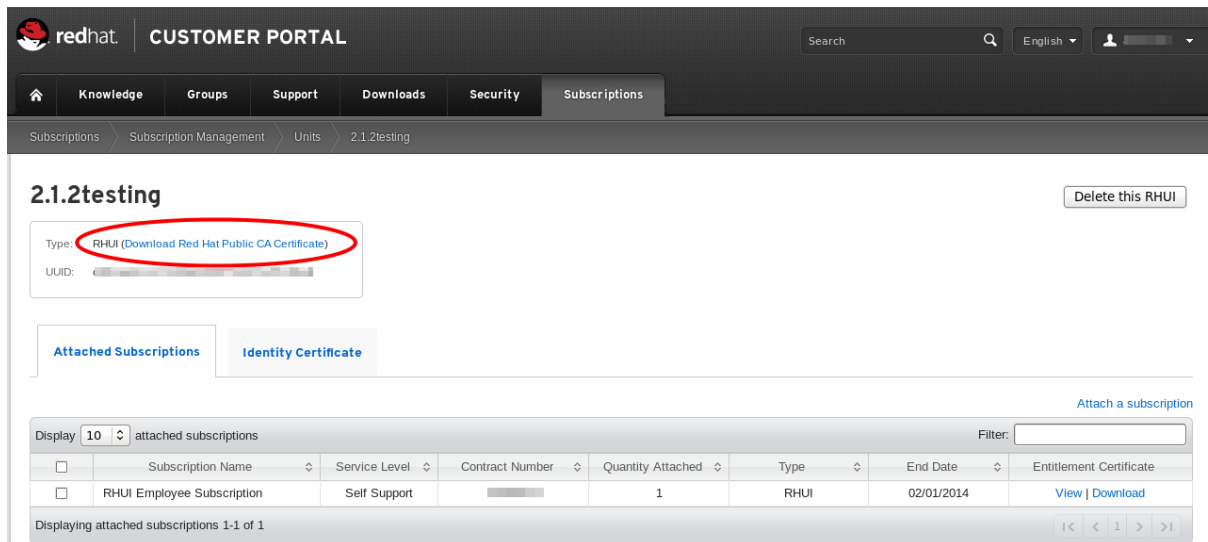
Figure 2.4. Download Entitlement Certificate



NOTE

The **Entitlement Certificate** downloaded here is used as a **Content Certificate** in the Red Hat Update Infrastructure package installation.

- Download Red Hat Public CA Certificate by clicking **Download Red Hat Public CA Certificate** in the upper left corner. Save the Red Hat Public CA Certificate on your local machine and note down the location. You will need this information later when you install the Red Hat Update Infrastructure ISO.



The screenshot shows the Red Hat Customer Portal interface. At the top, there is a navigation bar with 'redhat' logo and 'CUSTOMER PORTAL' text. Below it, there are tabs for 'Knowledge', 'Groups', 'Support', 'Downloads', 'Security', and 'Subscriptions'. The 'Subscriptions' tab is active, and the breadcrumb trail shows 'Subscriptions > Subscription Management > Units > 2.1.2testing'. The main content area displays the subscription details for '2.1.2testing', including a 'Type' field with the value 'RHUI (Download Red Hat Public CA Certificate)' circled in red. Below this, there are buttons for 'Attached Subscriptions' and 'Identity Certificate'. At the bottom, there is a table of attached subscriptions.

Subscription Name	Service Level	Contract Number	Quantity Attached	Type	End Date	Entitlement Certificate
RHUI Employee Subscription	Self Support		1	RHUI	02/01/2014	View Download

Figure 2.5. Download Red Hat Public CA Certificate

[Report a bug](#)

2.3. PACKAGE INSTALLATION

This section only outlines the package installation procedure for the Red Hat Update Appliance Server and the Content Delivery Server (CDS). Configuration is performed using the Red Hat Update Infrastructure Installer, as described in [Chapter 3, Red Hat Update Infrastructure Installer](#).

Red Hat Update Appliance Server and CDS instances require Red Hat Enterprise Linux installations with the base packages with all repositories disabled except for **rhel-6-server-rpms**. This requirement also means any third-party configurations or software that is not directly necessary for the direct operation of the server cannot be installed. This restriction includes hardening or other non-Red Hat security software.

The Red Hat Update Appliance Server and CDS instances must be installed on separate machines. You must have the Red Hat Update Infrastructure ISO and an appropriate content certificate, provided by Red Hat, in order to install Red Hat Update Infrastructure. Ensure the ISO is accessible from all machines and networks that will need to be connected to Red Hat Update Infrastructure. Instructions for downloading a content certificate are in [Section 2.2, “Downloading Entitlements”](#).



NOTE

Refer to README file for release notes and recent changes before starting Red Hat Update Infrastructure setup.

Procedure 2.2. Installing the Red Hat Update Infrastructure packages on the Red Hat Update Appliance Server

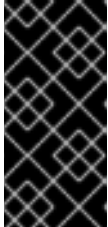
1. Download the ISO from [the Customer Portal](#).
2. Change the hostname of the Red Hat Update Appliance Server and all CDS instances to a resolvable fully qualified domain name (FQDN).

Change the hostname in your current session:

```
# hostname new_hostname
```

To make the hostname change persistent, edit `/etc/sysconfig/network` using your preferred text editor:

```
NETWORKING=yes
HOSTNAME=new_hostname
...
```



IMPORTANT

If the hostname is unset and its value is reported as `localhost.localdomain` or `localhost`, you will not be able to proceed. In this guide, the example hostname for Red Hat Update Appliance is `rhua.example.com`, and the example hostname for the first CDS instance is `cds01.example.com`.

3. Mount the ISO:

```
# mkdir -p /mnt/example
# mount -o loop <ISO> /mnt/example
```

4. Change directory to `/mnt/example`.

```
# cd /mnt/example
```

5. On the Red Hat Update Appliance Server, run `install_RHUA.sh` to install Red Hat Update Appliance packages.

```
# ./install_RHUA.sh
```

Procedure 2.3. Installing the Red Hat Update Infrastructure packages on the Content Delivery Server (CDS)

1. On the CDS instance, follow steps 1 to 4 in the previous procedure.
2. Run the following commands to register the system to Red Hat Subscription Manager and give the system a basic Red Hat Enterprise Linux entitlement.

- a. Register the system to Red Hat Subscription Manager:

```
# subscription-manager register
```

- b. Attach the system:

```
# subscription-manager attach --auto
```

- c. Disable all existing repositories:

```
# subscription-manager repos --disable=*
```

- d. Enable the Red Hat Enterprise Linux repository:

```
# subscription-manager repos --enable=rhel-6-server-rpms
```

- 3. Run **install_CDS.sh** to install CDS packages.

```
█ # ./install_CDS.sh
```

[Report a bug](#)

CHAPTER 3. RED HAT UPDATE INFRASTRUCTURE INSTALLER

The Red Hat Update Infrastructure Installer is used to configure Red Hat Update Infrastructure and get it started. This is achieved through an *answers file* which you complete with information describing the environment in which Red Hat Update Infrastructure will be installed. Red Hat Update Infrastructure Installer will then create the configuration RPMs it needs. This configures and starts all the necessary services.

The Red Hat Update Infrastructure Installer performs the following tasks:

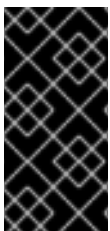
- Configures **httpd** on the Red Hat Update Appliance and any CDS instances with SSL certificates
- Installs a custom CA certificate that is used for authentication of users
- Configures the Red Hat Update Appliance
- Configures secure communication between the Red Hat Update Appliance and the CDS instances

Once Red Hat Update Infrastructure Installer has completed, use Red Hat Update Infrastructure Manager to interact with Red Hat Update Infrastructure.

This chapter explains how to perform an initial installation of Red Hat Update Infrastructure using Red Hat Update Infrastructure Installer. Ensure all the prerequisites described in [Chapter 2, *Installation Requirements*](#) have been met before attempting to install Red Hat Update Infrastructure.

3.1. SETTING UP SSL

In order to use Red Hat Update Infrastructure you will need to purchase a root SSL certificate and a private key, and be able generate SSL certificates of your own. This section outlines the basic skills you require to be able to perform these tasks.



IMPORTANT

It is recommended that you sign the SSL certificates and the client entitlement certificates with different certificate authorities (CAs). However, if you choose to use the same CA to sign both certificates, ensure the serial numbers for all server-side SSL certificates are below **0100** to avoid conflicts within Red Hat Update Infrastructure.

3.1.1. Configuring SSL Certificates Manually

Users must be able to generate SSL certificates for secure communication between CDS instances and clients. The following steps detail the process of acquiring and generating SSL certificates for use in Red Hat Update Infrastructure manually.

Procedure 3.1. Configuring Red Hat Update Appliance SSL Certificates

1. Acquire your company's root certificate and private key. Alternatively you can purchase one from a certificate authority (CA), or generate your own using tools such as **openssl** or **genkey**.

The CA key and certificate enables you to create SSL keys and certificates for the Red Hat Update Appliance and the CDS, as well as sign the entitlement certificates for the clients to access the CDS instances.

**NOTE**

In this section, *ca.key* and *ca.crt* are the example names for the CA key and certificate.

2. Create a file with the same name and in the same location as the CA certificate you have but using a `.sr1` extension. The file should contain the text `10` only. This can be performed using the following command:

```
# echo 10 > /home/example/certs/ca.sr1
```

3. Generate the Red Hat Update Appliance Server SSL key, using the following command:

```
# openssl genrsa -out ssl_RHUA.key 2048
```

4. Generate a certificate request using the `openssl` command:

```
# openssl req -new -key ssl_RHUA.key -out ssl_RHUA.csr
```

The tool will prompt you for further information, and then create an output file called `ssl_RHUA.csr`.

5. Use the CSR file to create a SSL certificate for the Red Hat Update Appliance instance with the following command:

```
# openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -in  
ssl_RHUA.csr -out ssl_RHUA.crt
```

In this example, `ssl_RHUA.csr` is the file created in the previous step, `ca.crt` is the certificate generated by the CA, `ca.key` is the CA certificate private key, and `ssl_RHUA.crt` is the name of the certificate file that will result from running this command.

Procedure 3.2. Configuring Content Delivery Server (CDS) SSL Certificates

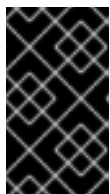
1. Generate the CDS SSL key, using the following command:

```
# openssl genrsa -out ssl_cds01.key 2048
```

2. Generate a certificate request using the `openssl` command:

```
# openssl req -new -key ssl_cds01.key -out ssl_cds01.csr
```

The tool will prompt you for further information, and then create an output file called `ssl_cds01.csr`.

**IMPORTANT**

When entering the hostname for `.csr` file, the hostname needs to be the same hostname clients will use to access the CDS. This is also the client hostname used in Procedure 3.3 Add a CDS Instance of the Administration guide.

- Use the CSR file to create SSL certificates for each CDS instance with the following command:

```
# openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -in
ssl_cds01.csr -out ssl_cds01.crt
```

**NOTE**

It is recommended that you name the output files correspondent with the hostname of the CDS instance for which the request was created. For example, if the hostname for the CDS is `cds01.example.com`, the output files could be named `ssl-cds01.key`, `ssl_cds01.csr`, and `ssl_cds01.crt`. This will help avoiding confusion when creating multiple CDS instances.

[Report a bug](#)

3.1.2. Configuring SSL Certificates Using the Automated Script

Users must be able to generate SSL certificates for secure communication between CDS instances and clients. The following steps detail the process of acquiring and generating SSL certificates for use in Red Hat Update Infrastructure using the automated script. Using the script reduces install time and reduces the chance of errors during the entry of the repetitive SSL information.

Procedure 3.3. Configuring SSL Certificates Using the Automated Script

- Generate the SSL certificates required for the Red Hat Update Infrastructure installation using the following command:

```
# /usr/share/rh-rhua/rhui_certs/create_rhui_ssl_certs.sh
RHUA_HOSTNAME CDS1_HOSTNAME
```

**NOTE**

If you do not wish to encrypt the keys use the `--noencrypt` option.

Additional hostnames can be added to the end of the command if SSL certificates are required for more than one CDS.

- You will be prompted for three separate passwords. These are for the root CA, the server CA and the client CA. Enter and confirm the passwords when prompted.

**IMPORTANT**

Use different passwords for each CA and record the passwords in a secure location.

[Report a bug](#)

3.2. EDITING THE ANSWERS FILE

In order to configure Red Hat Update Infrastructure, a series of configuration RPMs are required. These are created by Red Hat Update Infrastructure Installer using an *answers file*. Red Hat Update Infrastructure includes an example answers file at `/etc/rhui/answers.sample` to use as a basis for creating your own answers file. There is also an example answers file at [Example 3.1, “Example Answers File”](#).

Procedure 3.4. Editing the Answers File

1. Copy `/etc/rhui/answers.sample` to another location on your local machine:

```
# cp /etc/rhui/answers.sample /etc/rhui/myanswersfile
```

2. Open the local copy of the file in your preferred text editor. The answers file is divided into three sections: General, RHUA, and CDS Instances.

3. General

The General section contains all the general configuration options for Red Hat Update Infrastructure.

a. *version*

Red Hat Update Infrastructure Installer needs to generate configuration RPMs. These RPMs will be given the version number **2.1** by default. To make the RPMs use a different version number, enter it here:

```
[general]
version: 2.1
```

By default, this setting will apply to all the configuration RPMs that were created using this answers file. However, it can be overridden for specific sub-sections. For example, if in the General section version is set to **version: 2.1**, all the CDS RPMs will be version 2.1. Similarly, if you set Red Hat Update Appliance section version to **version: 2.5**, all the Red Hat Update Appliance RPMs will be version 2.5.

b. *dest_dir*

Enter the full path to the location where Red Hat Update Infrastructure Installer should create the configuration RPMs. Every RPM will be located in this directory after it runs and temporary files will be located in a sub-directory.

```
dest_dir: /tmp/rhui
```

4. Red Hat Update Appliance

The Red Hat Update Appliance section contains configuration options for the Red Hat Update Appliance (RHUA). There must be only one Red Hat Update Appliance section on the answers file.

a. *rpm_name*

Enter a name for the Red Hat Update Appliance configuration RPM. This name will have the version and architecture information added to it during the creation process, so there is no need to specify them here:

```
rpm_name: rh-rhua-config
```

b. **hostname**

Enter the fully qualified domain name (FQDN) of the Red Hat Update Appliance instance. This must not be an IP address, but a resolvable DNS name. Ensure that your SSL certificate has been created for this DNS name, as they must match exactly:

```
hostname: rhua.example.com
```

c. **ssl_cert and ssl_key**

Enter the full paths to the SSL certificate and its private key. These will be used to configure Apache on the Red Hat Update Appliance instance:

```
ssl_cert: /path/to/ssl_RHUA.crt
ssl_key: /path/to/ssl_RHUA.key
```

d. **ca_cert**

Enter the full path to the certificate authority (CA) certificate:

```
ca_cert: /path/to/ca.crt
```

e. **Optional Proxy Parameters**

It is possible to specify optional parameters to be used as a proxy server when the Red Hat Update Appliance attempts to access the internet (external to the cloud) and download packages from Red Hat.

```
proxy_server_host: proxy.example.com
proxy_server_port: 443
proxy_server_username: admin
proxy_server_password: password
```

For non-authenticating proxy servers, only **proxy_server_host** and **proxy_server_port** need to be defined.



IMPORTANT

When specifying the **proxy_server_host** parameter, ensure you do not have a trailing slash in the URL, as resolution of the address will fail. For example, use **proxy.example.com** not **proxy.example.com/** to avoid errors.

5. CDS Instances

The CDS section contains configuration options for each CDS instance. Create a new section under the CDS Instances heading for each CDS instance, giving each one a unique title with a **cds-** prefix, for example:

```
[cds-1]
-- parameters for a CDS --

[cds-2]
-- parameters for a different CDS --
```

a. ***rpm_name***

Enter a name for the CDS configuration RPM. This name will have the version and architecture information added to it during the creation process, so there is no need to specify them here:

```
rpm_name: rh-cds1-config
```

b. ***hostname***

Enter the fully qualified domain name (FQDN) of the CDS instance. This must not be an IP address, but a resolvable DNS name. Ensure that your SSL certificate has been created for this DNS name as they must match exactly:

```
hostname: cds01.example.com
```

c. ***ssl_cert* and *ssl_key***

Enter the full paths to the SSL certificate and its private key. These will be used to configure Apache on the CDS instance:

```
ssl_cert: /path/to/ssl_cds01.crt
ssl_key: /path/to/ssl_cds01.key
```

**NOTE**

To create a new CDS after Red Hat Update Infrastructure is deployed, refer to [Section 3.3, “Adding a Content Delivery Server”](#).

6. To execute the file and create the configuration RPMs, change to root user and run the **rhui-installer** command:

```
# rhui-installer /etc/rhui/myanswersfile
```

The configuration RPMs will be saved to the location you specified in [Step 3.b](#). There will be a configuration RPM for both the Red Hat Update Appliance and the CDS instances, using the names you gave for each.

7. Copy the Red Hat Update Appliance configuration RPM to the Red Hat Update Appliance and install it:

```
# yum install /tmp/rhui/rh-rhua-config-2.1-2.el6.noarch.rpm
```

8. Copy the CDS configuration RPM for each CDS instance (as defined by the hostname in the **[cds-1]** section) and install it:

```
# yum install /tmp/rhui/rh-cds1-config-2.1-2.el6.noarch.rpm
```

Example 3.1. Example Answers File

This example answers file is used to generate configuration RPMs.

```
#
# RHUI Installer Sample Answers File
```

```

#
# This sample answers file can be found at /etc/rhui/answers.sample.
#
# This file is meant to be used as a template for creating an answers
file for
use with
# the RHUI Installer. Once the appropriate values have been entered, the
RHUI
Installer
# will generate RPMs based on these values through the following call:
#
#   $ rhui-installer --answers <path to populated answers file>
#
# The results of running the above call will be found in the directory
specified in the
# dest_dir attribute under the [general] section.

# == General
=====

# The [general] section contains configuration options that apply to the
RHUI
installation
# as a whole.
[general]

# This will be used as the version for all RPMs that are created by this
answers file.
# Individual components may override this value with the "rpm_version"
attribute.
version: 2.1

# Local directory into which RHUI tools will place any temporary files
as well
as the
# built RPMs. If this directory exists prior to running RHUI tools, the
user
executing
# it must have write permissions.
dest_dir: /tmp/rhui

# == RHUA
=====

# The [rhua] section contains attributes describing a particular RHUA
instance.
[rhua]

# Name of the RHUA configuration RPM created by RHUI tools.
rpm_name: rh-rhua-config

# Fully qualified hostname of the RHUA instance.
hostname: rhua.example.com

```

```
# SSL certificate and private key to be installed on the RHUA. The CN of
this
certificate
# must match the hostname listed above.
ssl_cert:
ssl_key:

# CA certificate used to sign the RHUA's SSL certificate. This is needed
by the
CDS
# instances when connecting back to the RHUA to synchronize content to
verify
the
# RHUA certificate during the handshake.
ca_cert:

# If a proxy server is needed for the RHUA to connect to the internet,
this is
the hostname
# of that server. If this is not specified, no proxy server will be
used.
# proxy_server_host: proxy.example.com

# Port to access on the proxy server. This value has no effect if
proxy_server_host is
# not specified.
# proxy_server_port: 443

# Proxy server username. Omit if the proxy server does not require
authentication.
# proxy_server_username: admin

# Proxy server password.
# proxy_server_password: password

# == CDS Instances
=====

# There should be one [cds-*] section for each CDS to be used in the
RHUI
infrastructure.
# The name between the [ ] must begin with "cds", however the remainder
is
arbitrary and must
# only be unique with respect to other cds sections. There will be one
CDS
configuration RPM
# generated for each section found.

[cds-1]

# Name of the RPM that will be created for this CDS configuration.
rpm_name: rh-cds1-config
```



```
# Fully qualified name of this CDS instance.
hostname: cds01.example.com

# SSL certificate and private key to be used by this CDS instance. The
# CN of
# this
# certificate must match the hostname listed above.
ssl_cert:
ssl_key:

# [cds-2]
# rpm_name: rh-cds2-config
# hostname: cds02.example.com
# ssl_cert:
# ssl_key:
```

[Report a bug](#)

3.3. ADDING A CONTENT DELIVERY SERVER

To add a new CDS after Red Hat Update Infrastructure is deployed, perform the following steps.



NOTE

In this section, *cds02.example.com* is the example hostname for a new CDS.

Procedure 3.5. Generate SSL certificate for the new CDS

1. Generate the CDS SSL key, using the following command:

```
# openssl genrsa -out ssl_cds02.key 2048
```

2. Generate a certificate request using the **openssl** command:

```
# openssl req -new -key ssl_cds02.key -out ssl_cds02.csr
```

The tool will prompt you for further information, and then create an output file called **ssl_cds02.csr**.

3. Use the CSR file to create a SSL certificate for the new CDS instance with the following command:

```
# openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -in
ssl_cds02.csr -out ssl_cds02.crt
```

Procedure 3.6. Prepare the answers file and generate RPM for the new CDS

1. Change directory to the answers file created in [Procedure 3.4, “Editing the Answers File”](#)

```
# cd /etc/rhui/myanswersfile
```

2. Edit the `/etc/rhui/myanswersfile` answers file using your preferred text editor to include the correct details under `[cds-2]`.

```
[cds-2]
rpm_name: rh-cds2-config
hostname: cds02.example.com
ssl_cert: ssl_cds02.crt
ssl_key: ssl_cds02.key
```

3. To execute the file and create the configuration RPMs, change to root user and run the `rhui-installer` command:

```
# rhui-installer /etc/rhui/myanswersfile
```

4. Finally, install `/tmp/rhui/rh-cds2-config-2.1-2.el6.noarch.rpm` on `cds02.example.com`.

```
# yum install /tmp/rhui/rh-cds2-config-2.1-2.el6.noarch.rpm
```

[Report a bug](#)

3.4. UPDATING RED HAT UPDATE INFRASTRUCTURE

Red Hat Update Infrastructure can be configured to provide and use a repository that will update the Red Hat Update Infrastructure installation itself. The repository can be created using Red Hat Update Infrastructure Manager, which can then generate an entitlement certificate and client configuration RPM. The RPM is then installed on the Red Hat Update Appliance and each CDS instance, and future updates can be downloaded and installed using the `yum` command.

For further reading, see *Red Hat Update Infrastructure Administration Guide*:

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Update_Infrastructure/2.1/html/Administration_Guide/index.html

[Report a bug](#)

APPENDIX A. REVISION HISTORY

Revision 0-65	Tues Mar 13 2018	Les Williams
Changed "Production Phase 1" to "Full Support Phase" to line up with life cycle naming change		
Revision 0-64	Thu Mar 23 2017	Radek Bíba
BZ#1363952 Restored images. BZ#1427250 New location of the RHUI ISO.		
Revision 0-63	Tues Sep 1 2015	Megan Lewis
Preparing for Async Release BZ#1208142 Final correction based on feedback.		
Revision 0-62	Tues Aug 25 2015	Megan Lewis
BZ#1208142 Further corrections based on feedback.		
Revision 0-61	Wed Aug 19 2015	Megan Lewis
BZ#1208142 Corrections based on feedback.		
Revision 0-60	Mon Aug 3 2015	Megan Lewis
BZ#1208142 Corrected typo.		
Revision 0-59	Fri July 31 2015	Megan Lewis
BZ#1208142 Added information about what base packages to install for the RHUA / CDS servers. BZ#1208142 Added information about registering a CDS server with basic RHEL entitlement.		
Revision 0-58	Thu July 30 2015	Megan Lewis
BZ#1089651 Added note about --secure-protocol switches for wget.		
Revision 0-57	Thu Mar 26 2015	Megan Lewis
Updating screenshots.		
Revision 0-56	Thu Mar 26 2015	Megan Lewis
Preparing for March Asynchronous Release		
Revision 0-55	Wed Mar 25 2015	Megan Lewis
Added corrections for BZ#118747. BZ#1192168 Updated directions for registering a RHUI on the Customer Portal.		
Revision 0-54	Tues Dec 16 2014	Megan Lewis
Added bug links at the end of each section. BZ#118747 Added a section on automated configuration of SSL Certificates.		
Revision 0-53	Wed Dec 10 2014	Megan Lewis
Standardized the Preface to match new standards. Standardized the Abstract to match new standards. Standardized titles to match new standards. Applied brand changes.		
Revision 0-52	Thu Feb 20 2014	Dan Macpherson
Minor fix to wording of storage requirements		
Revision 0-51	Tue Jan 28 2014	Dan Macpherson
Clarified growth rates for storage requirements.		
Revision 0-50	Wed Jan 22 2014	Megan Lewis

Edits to #1055310 Changed storage requirements

Revision 0-49 #1055310 Changed storage requirements	Tue Jan 21 2014	Megan Lewis
Revision 0-48 Changing	Mon Dec 16 2013	Dan Macpherson
Revision 0-47 #951722 Fixed typos.	Mon Apr 22 2013	Julie Wu
Revision 0-46 #951722 updated hardware and storage requirements	Tue Apr 16 2013	Julie Wu
Revision 0-45 #927403 minor edits	Tue Mar 26 2013	Julie Wu
Revision 0-44 #921848 updated screen shots	Mon Mar 18 2013	Julie Wu
Revision 0-43 #908135 fixed all prompt to #	Thu Feb 07 2013	Julie Wu
Revision 0-42 Edited Procedure 2.3	Mon Oct 29 2012	Julie Wu
Revision 0-41 Whole book review	Fri Oct 26 2012	Julie Wu
Revision 0-40 Updated screenshots	Fri Oct 26 2012	Julie Wu
Revision 0-39 Edited note in introduction. #854875	Wed Oct 24 2012	Julie Wu
Revision 0-38 Added a note in introduction. #854875	Wed Sep 19 2012	Julie Wu
Revision 0-37 Edited checksum note in Procedure2.2 #850428	Tue Aug 28 2012	Julie Wu
Revision 0-36 Edited Procedure2.2 step1 link #850428 Edited Important note in Section2.1 #844224	Wed Aug 22 2012	Julie Wu
Revision 0-35 Edited Important note in Section2.1 #844224	Tue Aug 21 2012	Julie Wu
Revision 0-34 Edited Important note in Procedure3.2 step2 #842644 Fixed http://access.redhat.com and https://access.redhat.com/knowledge/docs/ Fixed RHUI abbreviation in Chap3	Tue Aug 21 2012	Julie Wu
Revision 0-33 Removed "Important" admonition regarding RPMs for Entitlement Certs from chapter 3 introduction para, as per James tech review.	Mon Aug 20 2012	Shikha Nansi
Revision 0-32	Thu Aug 16 2012	Julie Wu

Edited Procedure 3.4 #rhui-installer /etc/rhui/myanswersfile		
Revision 0-31	Tue Aug 14 2012	Julie Wu
Added an Important note in Procedure3.2		
Edited date format in Revision history		
Revision 0-30	Mon Aug 13 2012	Julie Wu
Moved the first two paragraphs in Procedure2.2 to Section2.3		
Revision 0-29	Tue Aug 07 2012	Julie Wu
Removed 1.1.2 certificate image #810854		
Fixed customer portal images		
Removed 'please' in Procedure3.3 Note		
In procedure3.2, changed 'ssl_CDS' to 'ssl_cds01' for example consistency		
Edited procedure3.1, and added a Note		
Removed numbering from Revision history		
Edited procedure3.5, and moved Note to step3		
Revision 0-28	Mon Aug 06 2012	Julie Wu
Changed RHN to Red Hat Customer Portal in 2.1		
Changed 2.1 Hardware and Storage Requirements: Red Hat Enterprise Linux 6.3		
Edited 2.3 Note: removed 'Please'		
Edited Procedure 2.2 Note		
Revision 0-27	Wed Jul 25 2012	Julie Wu
Fixed all Content Distribution Server to Content Delivery Server.		
Revision 0-26	Tue Jul 24 2012	Shikha Nansi
Split Rhui installer into Setting SSL, Answer Files, Adding new CDS		
Reworded Step 3 in section 3.2 as per QE feedback		
Revision 0-25	Tue Jul 24 2012	Julie Wu
new images for 2.2		
Revision 0-24	Mon Jul 23 2012	Julie Wu
QE review		
3.3 Procedure 3.4 split into 3.4 and 3.5.		
Revision 0-23	Fri Jul 20 2012	Julie Wu
Restore section 3.4.		
Remove Chapter 4 and 5.		
Revision 0-22	Thu Jul 19 2012	Julie Wu
Section 3.4 removed. Same paragraph appears in Chapter 4.		
Edited Notes in Procedure5.1		
Edited screen shots in Chapter 5		
Fixed links in Chapter 5		
Revision 0-21	Wed Jul 18 2012	Julie Wu
Updated 2.0 to 2.1 where applicable.		
Fixed author email address.		
Revision 0-20	Tue Jul 17 2012	Julie Wu

BZ840017 removed install_tools.sh from 2.3 Procedure2.2
2.3Package Installation split into two procedures(RHUA, CDS)
Edited Note in Procedure2.2
Edited 3.1 and 3.2 key and cert names for consistency
Changed Procedure2.2 step 1 ISO link.
BZ840016 added step 2 in Procedure2.2
Updated links in Procedure4.1

Revision 0-19	Sun Jul 15 2012	Shikha Nansi
Removed Disaster recovery from backup.		
Revision 0-18	Mon Jul 09 2012	Shikha Nansi
Added Backup Chapter BZ-813172		
Revision 0-17	Mon Jul 09 2012	Julie Wu
BZ838413 removed step 3 and 4 in 2.3 Edited 2.3 step 1 --ca-certificate 3.2 step 7 and 8 change rpm -Uvh to yum localinstall Edited Procedure2.2 in 2.3 Note added in 2.2 step 5 1.1.2 Take load balancer out of the text 3.2 step 4 c. rhua.crt and rhua.key changed to server.crt and server.key to be consistent in examples		
Revision 0-16	Tue Jul 5 2012	Julie Wu
BZ837713 Update customer portal/entitlement screen shots and instructions. Step 6 added. BZ835368 Procedure2.2 step2: change script order:intall_RHUA.sh,install_tools.sh. Note added in step2 Checksum note in Procedure2.2 step2 moved to step1		
Revision 0-15	Tue Jul 3 2012	Shikha Nansi
Split the Install guide into Install and Admin		
Revision 0-14	Tue Jun 26 2012	Julie Wu
BZ826142 A table of status codes is added in Ch 13. Monitoring		
Revision 0-13	Mon Jun 25 2012	Julie Wu
BZ802547 Note edited in Procedure7.4		
Revision 0-12	Mon Jun 25 2012	Julie Wu
BZ824613 screenshot updated		
Revision 0-11	Thu Jun 21 2012	Julie Wu
BZ831655 Note added in 1.1		
Revision 0-10	Tue Jun 19 2012	Julie Wu
BZ831119;BZ810854 Note added in 2.3		
Revision 0-9	Mon Jun 18 2012	Julie Wu
BZ829924;BZ829923		
Revision 0-8	Fri Jun 15 2012	Julie Wu
BZ829926		
Revision 0-7	Tue Jun 12 2012	Julie Wu

Replaced entities such as Red Hat Update Infrastructure, Red Hat, and Red Hat Enterprise Linux with their full words. Replaced all RHUI with Red Hat Update Infrastructure; Ex: RHUI Manager: Red Hat Update Infrastructure Manager. Replaced all RHUA with Red Hat Update Appliance

Revision 0-6	Wed Jun 06 2012	Julie Wu
Restore 4 images in the folder for ChapterII, section 2.2. (2) For ChapterII, section 2.2, step 2,3,4,5, put text in front of the image.		
Revision 0-5	Tue May 29 2012	Julie Wu
BZ808965		
Revision 0-4	Fri May 25 2012	Julie Wu
modify email address errors in Author_Group		
Revision 0-3	Fri May 25 2012	Julie Wu
#815656 Added a note on Checksum files for the latest ISO in Installation requirements section 2.3 step 2		
Revision 0-2	Fri May 25 2012	Julie Wu
#808966 Installation Requirements: Section 2.3, Step 5 removed		
Revision 0-1	Thu May 24 2012	Shikha Nansi
Initial creation of book by publican		

INDEX

C

Certificates

X.509, [Certificates](#)

I

installation

hardware, [Prerequisites](#)

SSL, [Configuring SSL Certificates Manually](#)

storage, [Prerequisites](#)

R

Red Hat Update Appliance

architecture, [System Overview](#)

Red Hat Update Infrastructure, [Introduction to Red Hat Update Infrastructure](#) (see Red Hat Update Infrastructure)

communications, [Communication](#)

requirements, [Installation Requirements](#)

Red Hat Update Infrastructure Installer

answers file, [Editing the Answers File](#)

configuration, [Editing the Answers File](#)

requirements, [Installation Requirements](#)

cloud provider, [Prerequisites](#)

firewall, [Prerequisites](#)

network, [Prerequisites](#)

U

Using the Red Hat Update Infrastructure Installer

overview, [Red Hat Update Infrastructure Installer](#)