



# **Red Hat Update Infrastructure 2.0**

## **Installation Guide**

Installation and configuration of Red Hat Update Infrastructure

Edition 2



# Red Hat Update Infrastructure 2.0 Installation Guide

---

Installation and configuration of Red Hat Update Infrastructure  
Edition 2

Lana Brindley  
Red Hat, Inc. Engineering Content Services  
lbrindle@redhat.com

Jason Dobies  
Red Hat, Inc. Engineering  
jdobies@redhat.com

John Ha  
Red Hat, Inc. Engineering Content Services  
jha@redhat.com

Wes Hayutin  
Red Hat, Inc. Engineering  
whayutin@redhat.com

Michael McCune  
Red Hat, Inc. Engineering  
mmccune@redhat.com

James Slagle  
Red Hat, Inc. Engineering  
jslagle@redhat.com

## Legal Notice

Copyright © 2011 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

This book covers installation and configuration of Red Hat Update Infrastructure for cloud providers.

---

## Table of Contents

<b>PREFACE</b> .....	<b>2</b>
<b>PART I. INTRODUCTION</b> .....	<b>3</b>
<b>CHAPTER 1. INTRODUCTION</b> .....	<b>4</b>
1.1. ARCHITECTURE .....	4
<b>PART II. INSTALLATION</b> .....	<b>6</b>
<b>CHAPTER 2. INSTALLATION REQUIREMENTS</b> .....	<b>7</b>
2.1. INSTALLATION PREREQUISITES .....	7
2.2. ENTITLEMENTS .....	8
2.3. PACKAGE INSTALLATION .....	10
<b>CHAPTER 3. RHUI INSTALLER</b> .....	<b>13</b>
3.1. SETTING UP SSL .....	13
3.2. ANSWERS FILE .....	16
3.3. UPDATING RED HAT UPDATE INFRASTRUCTURE .....	21
<b>PART III. OPERATION</b> .....	<b>22</b>
<b>CHAPTER 4. RHUI MANAGER</b> .....	<b>23</b>
4.1. RHUI MANAGER FIRST LAUNCH .....	23
4.2. USING RHUI MANAGER .....	25
4.3. USING RHUI MANAGER FROM THE SHELL PROMPT .....	28
<b>CHAPTER 5. REPOSITORIES</b> .....	<b>32</b>
5.1. CUSTOM REPOSITORIES .....	41
<b>CHAPTER 6. CONTENT DISTRIBUTION SERVER (CDS) INSTANCES</b> .....	<b>44</b>
<b>CHAPTER 7. CLIENT ENTITLEMENTS</b> .....	<b>48</b>
<b>CHAPTER 8. MANAGING ENTITLEMENT CERTIFICATES</b> .....	<b>54</b>
<b>CHAPTER 9. IDENTITY CERTIFICATES</b> .....	<b>58</b>
<b>CHAPTER 10. STATUS AND SCHEDULING</b> .....	<b>60</b>
<b>CHAPTER 11. USERS</b> .....	<b>67</b>
<b>CHAPTER 12. MONITORING</b> .....	<b>68</b>
<b>CHAPTER 13. UPDATING RED HAT UPDATE INFRASTRUCTURE</b> .....	<b>70</b>
<b>APPENDIX A. REVISION HISTORY</b> .....	<b>73</b>
<b>INDEX</b> .....	<b>79</b>

## PREFACE

Welcome to the *Red Hat Update Infrastructure Installation Guide*. This guide is designed to provide users the tested, supported methods of deploying Red Hat update solutions in their cloud environments.

The intended audience for this manual are organizations who have been certified to deploy Red Hat technology (such as Red Hat Enterprise Linux) as a part of their cloud solution. Topics in this manual range from detailing technical and license requirements to installation and configuration of the Red Hat Update Appliance (RHUA), and associated update infrastructure technology, such as the content delivery server (CDS) and firewall configuration.

# PART I. INTRODUCTION

## CHAPTER 1. INTRODUCTION

Red Hat Update Infrastructure is a collection of technologies that offers cloud providers the ability to easily deploy Red Hat solutions into their environments. Cloud solution providers can use Red Hat Update Infrastructure to give their customers the ability to update Red Hat technology in the cloud.

Red Hat Update Infrastructure streamlines the deployment of Red Hat technologies into a cloud environment. Initial configuration, initialization, and synchronization of available instances in the cloud are done with very little user configuration or intervention. However, cloud-specific configuration is sometimes required, such as in these use cases:

- Setting a storage volume mountpoint in the cloud to store installation or update packages that have been synchronized from Red Hat Network (RHN)
- Configuring network security to safeguard communications within the cloud
- Adding supplemental monitoring checks that are outside those offered by Red Hat

Cloud providers are given an X.509 content certificate that grants access to the Red Hat Enterprise Linux and Red Hat Update Infrastructure content stream, including ISO images and RPM packages. Once installed and configured, the Red Hat Update Infrastructure tools can be used to create Red Hat Update Appliance (RHUA) and content distribution server (CDS) instances. CDS instances are then managed and monitored by the RHUA.



### IMPORTANT

Always ensure that you include the package that installs the GPG keys when installing client configuration RPMs. For Red Hat Enterprise Linux 6, the package required is `redhat-release-server`.

## 1.1. ARCHITECTURE

Red Hat Update Infrastructure encompasses the following technologies:

- Red Hat Update Appliance (RHUA) is a system instance that runs in the cloud by default and performs the following tasks:
  - Synchronizing packages from the external source (such as RHN)
  - Providing monitoring status updates for both machine and human readability
- The content delivery server (CDS) serves packages over HTTPS to clients in the cloud. One RHUA can manage multiple CDS instances.
- The client provides customer Red Hat Enterprise Linux instances in the cloud, which connect to a CDS for package updates.
- The load balancer schedules requests to all CDS instances using a round-robin method. The load balancer can run either on the RHUA or on a separate instance.

### 1.1.1. Communications

1. The cloud provider accesses a central third-party content repository, such as RHN. A provider can choose to configure the RHUA to connect using their network proxy server to access the content repository.



2. The RHUA synchronizes content to the CDS instances, and evenly distributes requests.
3. The CDS instances distribute content via HTTPS to a Red Hat Enterprise Linux client instance.

## 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 RHN. This grants permission to the customer to download the Red Hat Update Infrastructure packages or ISO. Additionally, the RHUA uses this certificate when authenticating with RHN 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 the load balancer and 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.

### Server Certificates

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

Red Hat does not impose requirements on which CA certificate you choose to use. You can acquire one from a trusted source (such as VeriSign, for example), use a subordinate certificate in a trust chain from their established CA certificate, or generate a new one manually using a tool such as openssl.



### IMPORTANT

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

## PART II. INSTALLATION

This section describes the requirements for Red Hat Update Infrastructure, and how to install it. It also describes how to generate each certificate you will require.

## CHAPTER 2. INSTALLATION REQUIREMENTS

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

### 2.1. INSTALLATION 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.

- 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 RHUA instance in the cloud. This grants access to:
  - Red Hat Update Infrastructure (RHUA and associated technologies).
  - 32-bit and 64-bit Red Hat Enterprise Linux images. This is required to perform instantiation.
  - Permission for the RHUA to synchronize channel content from RHN.
- 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

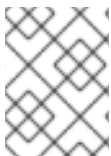
Red Hat Update Infrastructure has the following hardware and storage requirements:

- Red Hat Enterprise Linux 6.1 or higher. Red Hat Update Infrastructure will not run on Red Hat Enterprise Linux 5 or below.
- 64-bit architecture. Red Hat Update Infrastructure will not run on 32-bit architecture.
- At least 2GB of available memory
- At least 4GB 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 file directly only if you need to create a new mount point for it, otherwise, it will be created automatically during the installation process. You will require at least 30GB of storage for each software channel in `/var/lib/pulp`

All repositories are synchronized with content distribution 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 RHUA, 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 RHN
443	HTTPS	CDS	RHUA	Allows the CDS to download content from the RHUA
443	HTTPS	Client	CDS	Used by <b>yum</b> on the client to retrieve packages
5674	QPID	RHUA	CDS	Used for communication between the RHUA and the CDS
5674	QPID	CDS	RHUA	Used for communication between the RHUA and the CDS

**NOTE**

Every CDS instance must have 443 (HTTPS) as well as 5674 access to the RHUA in order to be able to synchronize packages.

**2.2. ENTITLEMENTS****Procedure 2.1. Downloading Entitlements from the customer portal**

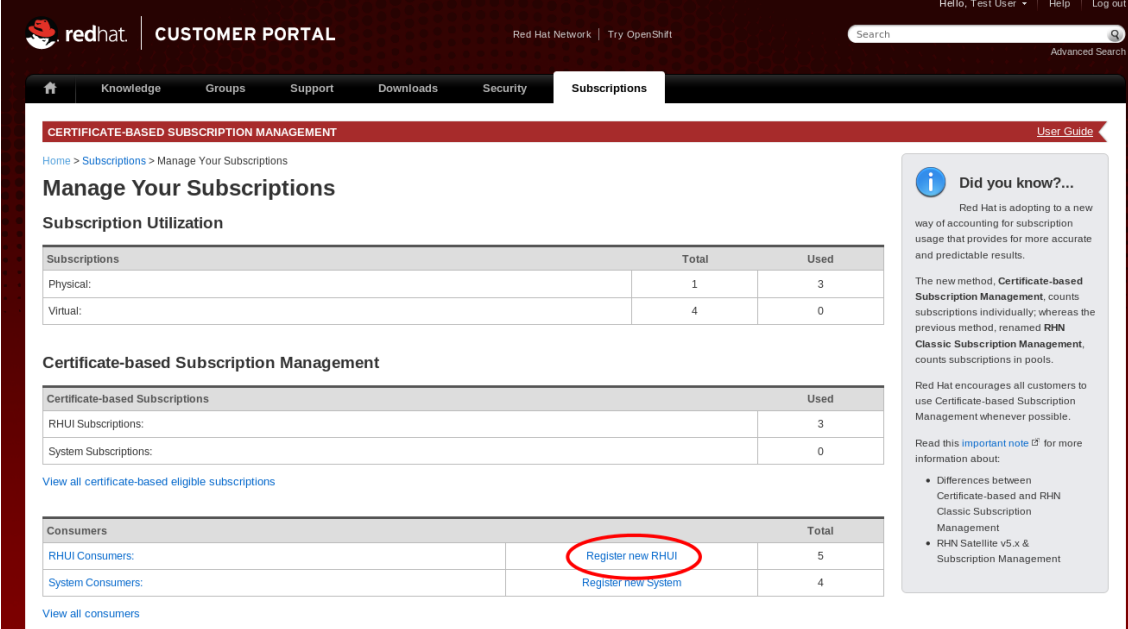
In order to use Red Hat Update Infrastructure, you need an entitlement for every RHUA instance in the cloud. You can download the entitlement ISO from the Red Hat customer portal.

**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 [access.redhat.com](https://access.redhat.com)

2.



The screenshot shows the Red Hat Customer Portal interface. The 'Subscriptions' tab is selected in the navigation menu. The page title is 'Manage Your Subscriptions'. Under the 'Certificate-based Subscription Management' heading, there are two tables:

Subscriptions	Total	Used
Physical:	1	3
Virtual:	4	0

Certificate-based Subscriptions	Used
RHUI Subscriptions:	3
System Subscriptions:	0

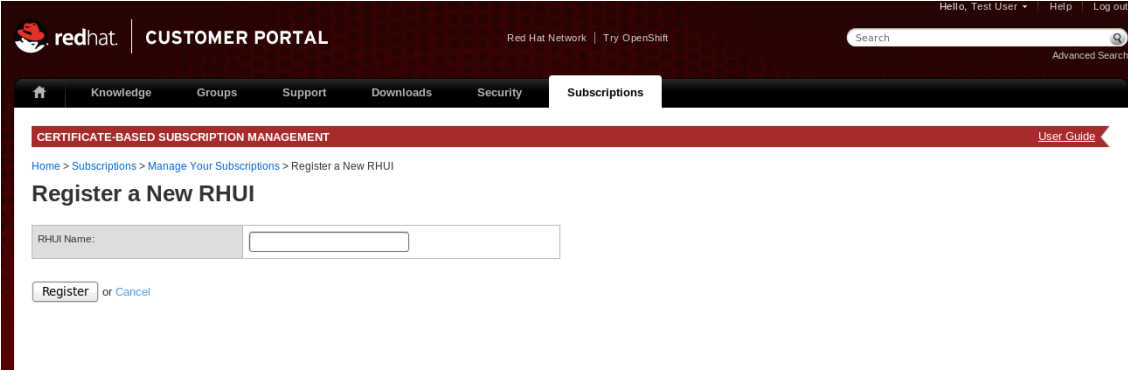
Consumers	Total
RHUI Consumers:	5
System Consumers:	4

The 'Register new RHUI' link in the RHUI Consumers row is circled in red. A 'Did you know?' sidebar on the right provides information about the new Certificate-based Subscription Management method.

**Figure 2.1. Manage Your Subscriptions**

Hover on the **Subscriptions** tab. Select **Overview** under the **Certificate-based management** heading. Select **Register new RHUI** from the **Consumers** table.

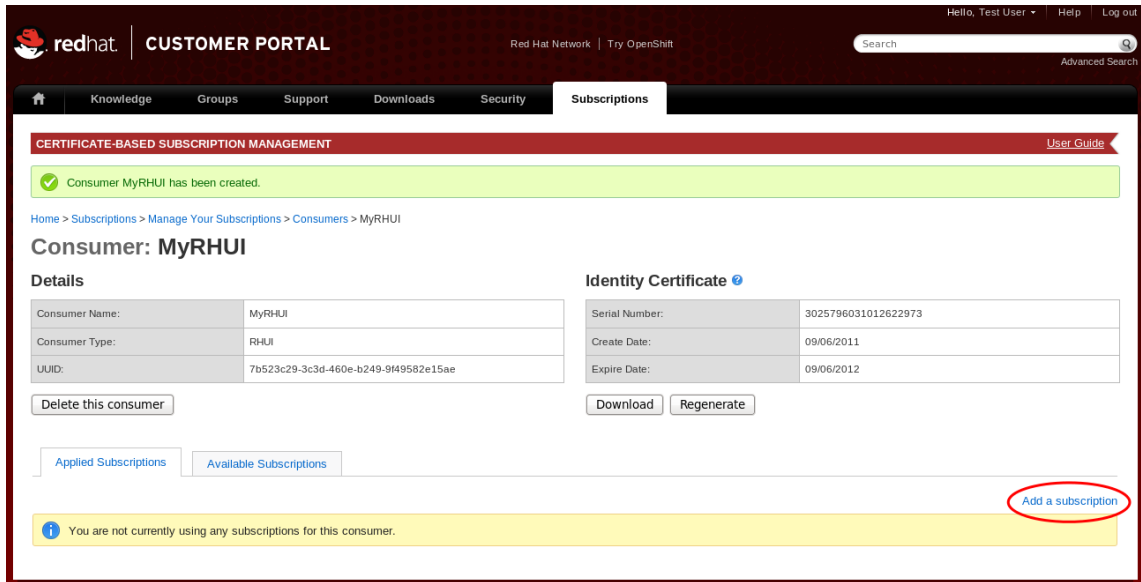
3.



The screenshot shows the 'Register a New RHUI' page. The 'RHUI Name' input field is visible, and the 'Register' button is highlighted.

**Figure 2.2. Register a New RHUI**

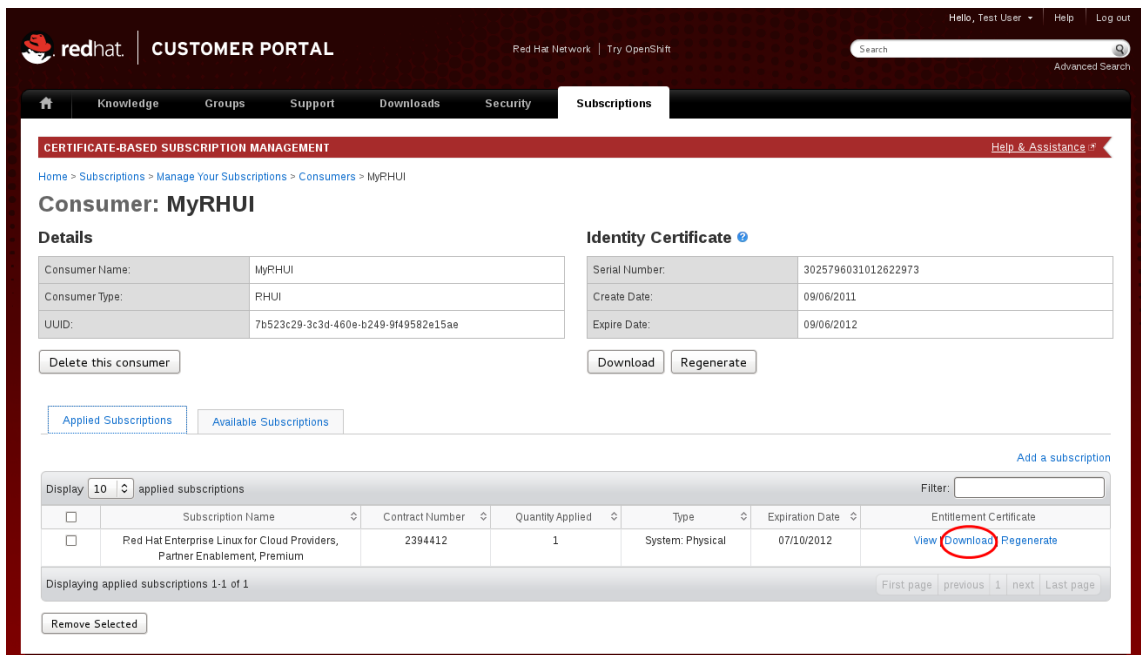
On the **Register a New RHUI** page, enter the name of the RHUA instance.



4.

Figure 2.3. Adding Subscriptions

Your new RHUA instance will not yet have any subscriptions applied to it. Add a subscription by clicking **Add 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 **Add Selected** to add it to the instance.



5.

Figure 2.4. Download Entitlement Certificate

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.

## 2.3. PACKAGE INSTALLATION

### Procedure 2.2. Installing the Red Hat Update Infrastructure packages

This section outlines the package installation procedure only. Configuration is performed using the

RHUI Installer, as described in [Chapter 3, RHUI Installer](#).

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, “Entitlements”](#).

Ensure all instances have access to the relevant Red Hat Enterprise Linux base channel, in order to be able to download the full list of package dependencies.

1. Download the ISO by running the `wget` command.

```
$ wget --no-check-certificate --certificate=<Content Certificate>\
https://cdn.redhat.com/content/dist/rhel/rhui/server/6/6Server/x86_64/rhui/2.0/iso/RHEL-6.1-RHUI-2.0-LATEST-Server-x86_64-DVD.iso
```

2. Mount the ISO and run the following installation scripts to set up each piece of Red Hat Update Infrastructure infrastructure, as follows:

- o The `install_tools.sh` script is used to install the Red Hat Update Infrastructure tools packages on the RHUA:

```
# install_tools.sh
```

- o The `install_RHUA.sh` script is used to install Red Hat Update Appliance packages on the RHUA node:

```
# install_RHUA.sh
```

- o The `install_CDS.sh` script is used to install the content delivery server packages on the CDS:

```
# install_CDS.sh
```

3. On the RHUA server, edit the `/etc/pulp/pulp.conf` configuration file using your preferred text editor to include the correct hostname of the RHUA server. The hostname will be listed as *localhost* by default:

```
[server]
server_name: localhost
...
...
[messaging]
url:          tcp://localhost:5672
```

Also on the RHUA server, edit the `/etc/pulp/admin/admin.conf` configuration file using your preferred text editor to include the correct hostname of the RHUA server. The hostname will be listed as *localhost* by default:

```
[server]
host = localhost.localdomain
...
...
```

```
[cds]
baseurl = https://localhost/pulp/repos
keyurl = http://localhost/pulp/gpg
ksurl = http://localhost/pulp/ks
```

4. Also on the RHUA server, edit the `/etc/rhui/rhui-tools.conf` configuration file using your preferred text editor, and add the fully qualified domain name (FQDN) to be used to connect to the RHUA:

```
[rhua]
hostname: rhua.example.com
```



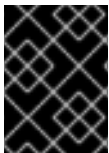
## CHAPTER 3. RHUI INSTALLER

RHUI 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 RHUI will be installed. RHUI Installer will then create the configuration RPMs it needs. This configures and starts all the necessary services.

The RHUI Installer performs the following tasks:

- Configures `ht tpd` on the RHUA and any CDS instances with SSL certificates
- Installs a custom CA certificate that is used for authentication of users
- Configures the RHUA
- Configures secure communication between the RHUA and the CDS instances

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



### IMPORTANT

You need one configuration RPM for each entitlement certificate, but you can reuse the same client configuration RPM for all clients that share the same entitlements.

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



### NOTE

You must be using Red Hat Enterprise Linux 6 in order to successfully install and run Red Hat Update Infrastructure. For more information on installing Red Hat Enterprise Linux, refer to the *Red Hat Enterprise Linux Installation Guide*

## 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), in order to help mitigate any security risk should one of the certificates become compromised. 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.

### Procedure 3.1. Configuring SSL Certificates

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:

1. Acquire a root certificate and private key. You can purchase one from a certificate authority (CA), or you can generate your own using a tool like **genkey**, which can be found in the **crypto-utils** package in Red Hat Enterprise Linux.

This certificate and key enables you to create SSL keys and certificates for the RHUA and the CDS, as well as sign the entitlement certificates for the clients to access the CDS instances.

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 server SSL key, using the following command:

```
$ openssl genrsa -out server.key 2048
```

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

```
$ openssl req -new -key server.key -out server.csr
```

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



#### NOTE

It is recommended that you name the output **.csr** file to correspond with the hostname of the CDS instance for which the request was created. For example, if the hostname for the CDS is **cds1.example.com**, the output file could be named **cds1-example-com.csr**. This will help avoid confusion when creating multiple CDS instances.

5. Once the CSR request file is created, create SSL certificates for each CDS instance with the following command:

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

In this example, **server.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 **server.crt** is the name of the certificate file that will result from running this command.

### Procedure 3.2. Generating a Qpid SSL Certificate

Red Hat Update Infrastructure uses a qpid message broker for internal communications. These communication processes are secured by SSL, which is set up using a script called **nss-db-gen**. When the script is run, it will prompt you for some information.

1. Run the **nss-db-gen** script by switching to the root user and issuing the command:

```
# /usr/bin/nss-db-gen  
Working in: /tmp/tmp24055
```

2. Specify a directory for the new database and certificates to be stored, or press enter to accept the default value of `/tmp/rhua/qpid`:

```
Please specify a directory into which the created NSS database  
and associated certificates will be installed.
```

```
Enter a directory [/tmp/rhua/qpid]:  
/tmp/rhua/qpid
```

3. Enter a password to be used by qpid to secure the database:

```
Enter NSS database password:  
Password file created.
```

4. The script will create the database and generate the necessary keys and certificates:

```
Database created.  
Creating CA certificate:  
Generating key. This may take a few moments...  
CA created  
Creating BROKER certificate:  
Generating key. This may take a few moments...  
Broker certificate created.  
Creating CLIENT certificate:  
Generating key. This may take a few moments...  
Client certificate created.
```

5. Enter the NSS database password again. This is so that the database created in the last step can be accessed:

```
Enter Password or Pin for "NSS Certificate DB":
```

6. Enter a password to be used for the pkcs12 file, and re-enter it to confirm:

```
Enter password for PKCS12 file:  
Re-enter password:  
pk12util: PKCS12 EXPORT SUCCESSFUL
```

7. Enter the pkcs12 password again. This is so that the certificate created in the last step can be accessed. The script will export the key and certificate, and finish:

```
Enter Import Password:
MAC verified OK
Client key & certificate exported

Artifacts copied to: /tmp/rhua/qpid.
```

## 3.2. ANSWERS FILE

In order to configure Red Hat Update Infrastructure, a series of configuration RPMs are required. These are created by RHUI 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 3.3. 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*

RHUI Installer needs to generate configuration RPMs. These RPMs will be given the version number `2.0` by default. To make the RPMs use a different version number, enter it here:

```
[general]
version: 2.0
```

This setting will apply to all configuration RPMs created using this answers file. It can be overridden in any of the sub-sections for just that subsection. For example, if *version: 2.0* is set in the General section, and *version: 2.5* is set in the RHUA section, all the CDS RPMs will be version 2.0, and all the RHUA RPMs will be version 2.5.

##### b. *dest\_dir*

Enter the full path to the location where RHUI 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. RHUA

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

##### a. *rpm\_name*

Enter a name for the RHUA 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 of the RHUA 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 RHUA instance:

```
ssl_cert: rhua.crt
ssl_key: rhua.key
```

**d. *ca\_cert***

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

```
ca_cert: ca.crt
```

**e. *Optional Proxy Parameters***

It is possible to specify optional parameters to be used as a proxy server when the RHUA 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 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: cds1.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: cds1.crt  
ssl_key: cds1.key
```

6. To execute the file and create the configuration RPMs, 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 RHUA and the CDS instances, using the names you gave for each.

7. Copy the RHUA configuration RPM to the RHUA and install it:

```
$ rpm -Uvh /tmp/rhui/rh-rhua-config-2.0-2.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:

```
$ rpm -Uvh /tmp/rhui/rh-cds1-config-2.0-2.el6.noarch.rpm
```

### Example 3.1. Example Answers File

This example shows the example answers file. This 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: 2.0

# 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: cds1.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: cds2.example.com
# ssl_cert:
# ssl_key:
```

### 3.3. 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 RHUI Manager, which can then generate an entitlement certificate and client configuration RPM. The RPM is then installed on the RHUA and each CDS instance, and future updates can be downloaded and installed using the `yum` command.

This procedure is detailed in [Chapter 13, \*Updating Red Hat Update Infrastructure\*](#)

## PART III. OPERATION

The RHUI Manager is an interactive shell that allows you to configure a running RHUI installation. The RHUI Manager can be used to:

- Upload Red Hat content certificates.
- Import Red Hat repositories. Select one or more products within a content certificate to import and manage.
- Create custom repositories and upload their own content. These repositories can be protected by entitlement certificates.
- Manage content delivery servers (CDS), including registration, unregistration, and selecting repositories to deploy to each CDS instance.
- Create entitlement certificates, using either Red Hat provided repositories or any custom repositories.
- Create client configuration RPMs.

This section describes how to use the RHUI Manager to perform tasks related to the operation and use of Red Hat Update Infrastructure.

## CHAPTER 4. RHUI MANAGER

RHUI Manager is used to interact with Red Hat Update Infrastructure. It allows you to manage CDS instances, repositories, certificates, and users.

### 4.1. RHUI MANAGER FIRST LAUNCH

Start RHUI Manager by running the `rhui-manager` command from the command prompt. Depending on your local setup, this operation might need to be performed as the root user in order to obtain the necessary permissions:

```
# rhui-manager
```

When RHUI Manager is run for the first time, it will prompt for some extra information before it will start:

1. The entitlement-signing CA certificate and its private key.
2. A password for the entitlement-signing CA certificate, if it requires one. RHUI Manager will generate an identity certificate using the entitlement signing CA certificate. If the CA private key requires a password, then you will need to enter that information.

You will also be asked to enter the number of days that the identity certificate is valid for. The system will default to 3650 days (ten years). Once an identity certificate has expired, it will need to be regenerated. This procedure is detailed in [Chapter 9, Identity Certificates](#).

3. Log in using the default name *admin*, and the default password *admin*:

```
--> rhui-manager
Previous authentication credentials could not be found. Logging into
the RHUI.

If this is the first time using the RHUI, it is recommended to
change
the user's password in the User Management section of RHUI Tools.

RHUI Username: admin
RHUI Password:
```

The Home screen will be displayed after the password has been entered.

This login is used for the initial connection to the RHUA. After the first login, a certificate is stored at `~/ .rhui` that identifies the user with the RHUA for all future calls and prevents you from having to log in each time. RHUI Manager will store authentication credentials for one week. Once authentication details have expired, all communications will fail until they have been refreshed. If you are using Red Hat Update Infrastructure when the credentials expire, you will be prompted to renew them the next time they are required for an operation. Otherwise, you will be asked to log in again next time you start RHUI Manager.



#### IMPORTANT

Ensure you change the default password for the RHUA before you begin using the system. For details on how to do this, see [Chapter 11, Users](#),

- You will require a Red Hat content certificate and private key in order to access repositories with RHUI Manager. Each product requires its own content certificate, which is provided by Red Hat. Once you have run RHUI Manager for the first time, upload a new content certificate for each product you require by following the directions in [Procedure 8.3, “Upload Content Certificate”](#).

Content certificates are installed to `/etc/pki/rhui`. This means that you will require write permission to `/etc/pki/rhui` to be able to install a new content certificate.

#### Example 4.1. Running RHUI Manager for the first time

This example shows the information that RHUI Manager requests when being run for the first time. This information must be provided before RHUI Manager can operate.

```
# rhui-manager
An entitlement signing CA certificate is required to use RHUI Tools
but was not found.

Full path to the new signing CA certificate:
/root/rhui_certs/ca.crt

Full path to the new signing CA certificate private key:
/root/rhui_certs/ca.key

Generating entitlement certificate serial number database file
/etc/pki/rhui/entitlement-ca.srl
A RHUI identity certificate is required to use RHUI Tools but was not
found.
A new identity certificate will be generated now using the CA
certificate
found at /etc/pki/rhui/entitlement-ca.crt.

Enter the number of days the RHUI identity certificate will be valid.
If the identity certificate ever expires, it will need to be
regenerated using rhui-manager [Default: 3650]:
.....+++
.....+++
Previous authentication credentials could not be found. Logging into
the RHUI.

If this is the first time using the RHUI, it is recommended to change
the user's password in the User Management section of RHUI Tools.

RHUI Username: admin
RHUI Password:

-----
-----
                                -= Red Hat Update Infrastructure Management

Tool =-

-- Home --

    r manage repositories
```

```

c manage content delivery servers (CDS)
s synchronization status and scheduling
e create entitlement certificates and client configuration RPMs
n manage Red Hat entitlement certificates
i manage identity certificate
u manage users

```

```

logout
  removes stored authentication credentials and exits
<
  move to the previous screen
^, home
  move to the home screen
/, clear
  clears the screen
?, help
  display help
q, quit, exit
  exit

```

```

Connected: rhua.example.com
-----
-----
rhui (home) =>

```

## 4.2. USING RHUI MANAGER

RHUI Manager operates using an interactive shell. This section describes how to interact with RHUI Manager, including common concepts and commands.

### Starting RHUI Manager

- Start RHUI Manager by running the `rhui-manager` command from the command prompt:

```
$ rhui-manager
```

- If RHUI Manager has not already stored a password for you, it will ask you to login. Once you have successfully authenticated, RHUI Manager will display a prompt, ready to accept commands:

```
rhui (home) =>
```

- When a menu is displayed, RHUI Manager will display the name of the server it is connected to at the bottom, immediately above the prompt. At the prompt, the text in the parentheses ( ) indicates which screen you are currently viewing. In this example, RHUI Manager is connected to `rhua.example.com`, and the current screen is the Home screen:

```

Connected: rhua.example.com
-----
rhui (home) =>

```

## Logging out of RHUI Manager

- The `logout` command is accessible at any time. Logging out will remove any stored authentication credentials that were saved when first logging in to RHUI Manager. Next time RHUI Manager is run, the user will be prompted to log in again.
- To log out of RHUI Manager, type `logout` at the prompt. You will be returned to the command line:

```
rhui (home) => logout
[user@example]$
```

## Exiting RHUI Manager

- To exit RHUI Manager, type `q`, `quit`, or `exit` at the prompt. You will be returned to the command line:

```
rhui (home) => quit
[user@example]$
```

- RHUI Manager can also be exited by typing `Ctrl+C` from within the interface.

## Navigating around RHUI Manager

There are several commands that can be used at any time to navigate around RHUI Manager:

- `<` to move to the previously viewed screen
- `home` or `^` to return to the home screen
- `clear` or `/` to clear the screen
- `help` or `?` to display the help screen

The help screen is divided into screen and shell commands. Screen commands are used at the RHUI Manager prompt, and shell commands are used at the shell prompt. For more information about using RHUI Manager from the shell prompt, see [Section 4.3, “Using RHUI Manager from the Shell Prompt”](#)

## RHUI Manager Screens

RHUI Manager uses *screens* to provide access to functions. Each screen has its own menu of related commands

### Home

The Home screen is the first screen displayed after logging in. It provides access to the other screens.

### Repository Management

The Repository Management screen is used to list, add, and delete repositories. You can also create and upload packages to custom repositories.

### CDS Management

The CDS Management screen is used to list, add, and delete content distribution server (CDS) instances.

From this screen, you can also access the CDS Repository Management screen, which allows you to view and change information for individual CDS instances. While in this screen, the prompt will indicate the hostname of the CDS being edited:

```
rhui (cds1.example.com) =>
```

### Synchronization Status

The Synchronization Status and Scheduling screen is used to display and change the synchronization schedules for CDS instances and repositories, and view past synchronizations. You can also trigger individual synchronizations.

### Client Entitlement Management

The Client Entitlement Management screen is used to create new entitlement certificates and client configuration RPMs.

### Entitlements Manager

The Entitlements Manager screen is used to list entitled products in the current content certificate and upload new certificates.

### User Manager

The User screen is used to change the user password.

### Example 4.2. The Home Screen

This example shows the Home screen on a typical RHUI Manager setup. Return to this screen at any time by typing `home` or `^` at the prompt:

```
-----
-----
      -= Red Hat Update Infrastructure Management Tool -=

-= Home -=

r  manage repositories
c  manage content delivery servers (CDS)
s  synchronization status and scheduling
e  create entitlement certificates and client configuration RPMs
n  manage Red Hat entitlement certificates
u  manage users

<  move to the previous screen
^, home
   move to the home screen
/, clear
   clears the screen
?, help
   display help
q, quit, exit
```

```
exit
```

```
Connected: rhua.example.com
```

```
-----  
-----  
rhui (home) =>
```

### 4.3. USING RHUI MANAGER FROM THE SHELL PROMPT

RHUI Manager is designed to be run using the interactive shell, however some functions can also be run from a standard shell prompt.

View all options and commands by using the `--help` command:

```
$ rhui-manager --help
Usage: rhui-manager [options] [command]

OPTIONS
  -h/--help  show this help message and exit
  --debug    enables debug logging
  --config   absolute path to the configuration file; defaults to
/etc/rhui/rhui.conf
  --server   location of the RHUA server (overrides the config file)
  --username if specified, previously saved authentication credentials
are ignored and this username is used to login
  --password used in conjunction with --username

COMMANDS
  cert      : Red Hat content certificate management
  packages  : package manipulation on repositories
  repo      : repository listing and manipulation
  status    : RHUI status and health information
```



#### NOTE

Commands in this list that begin with a `--` can be used both in the interactive shell and at the shell prompt. All other commands can only be used at the shell prompt.

#### Flags

##### `--debug`

Enables more verbose logging. The log file can be found at `~/ .rhui/rhui.log`

##### `--config /path/examplefilename.conf`

This command instructs RHUI Manager (both the interactive shell and the shell prompt) to use the specified configuration file, instead of the default file located at `/etc/rhui/rhui-tools.conf`

##### `--server rhua.example.com`

This command instructs RHUI Manager (both the interactive shell and the shell prompt) to connect to the specified server instead of the server specified in the configuration file. Authentication



credentials are stored on a per server basis, so this flag can be used to allow a single RHUI Manager installation to manage multiple RHUI installations.

**--username *username* --password *password***

This command instructs RHUI Manager to use the specified credentials to log into the Red Hat Update Appliance (RHUA). When using these commands, the authentication certificate will *not* be stored. This allows scripts to execute shell prompt commands on the RHUI without needing to manage authentication certificates as well.

## Content Certificate Management

The `cert` command is used to manipulate Red Hat content certificates.

**rhui-manager cert info**

Display information about the current content certificate.

**rhui-manager cert upload**

Use this command to upload a new content certificate. Specify the full path to the new certificate with the `--cert` flag, and the full path to the new key with the `--key` flag. RHUI Manager and all repositories will be updated automatically when using this command.

```
$ rhui-manager cert upload --cert /home/example/content-cert.crt --key
/home/example/content-key.pem
```

## Repository Management

The `repo` command is used to manipulate repositories on the RHUI.

**rhui-manager repo list**

Displays a list of repositories currently in the RHUI:

```
$ rhui-manager repo list
ID                               :: Repository Name

Red Hat Repositories
-----
rhui-srpms-1.2-5Server-x86_64    :: Red Hat Update Infrastructure 1.2
(SRPMS)
(5Server-x86_64)
rhui-srpms-1.2-5Server-i386     :: Red Hat Update Infrastructure 1.2
(SRPMS)
(5Server-i386)
rhui-1.2-5Server-x86_64         :: Red Hat Update Infrastructure 1.2
(RPMs)
(5Server-x86_64)
rhui-1.2-5Server-i386          :: Red Hat Update Infrastructure 1.2
(RPMs)
(5Server-i386)
```

**Custom Repositories**

-----

```
repo_1 :: Custom Repository 1
```

**rhui-manager repo info**

Displays information about a specified repository. Specify the name of the repository with the `--repo_id` flag. The repository ID is shown in the output of the `rhui-manager repo list` command.

```
$ rhui-manager repo info --repo_id rhui-1.2-5Server-x86_64
Name: Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
Type: Red Hat
Relative Path: content/dist/rhel/rhui/server/5Server/x86_64/rhui/1.2/os
Package Count: 13
Last Sync: 04-16-2011 21:58
Next Sync: 04-16-2011 23:44
```

**Package Management**

The `packages` command is used to manipulate packages on repositories.

**rhui-manager packages list**

Displays a list of all packages in a repository. Specify the name of the repository with the `--repo_id` flag. The repository ID is shown in the output of the `rhui-manager repo list` command:

```
$ rhui-manager packages list --repo_id rhui-1.2-5Server-x86_64
PyYAML-3.08-4.el5.x86_64.rpm
grinder-0.0.57-1.el5.noarch.rpm
httpd-2.2.3-43.el5_5.3.x86_64.rpm
libyaml-0.1.2-3.el5.x86_64.rpm
m2crypto-0.16-6.1.el5_5.1.x86_64.rpm
mod_python-3.3.1-12.el5.x86_64.rpm
python-hashlib-20081119-5.el5.x86_64.rpm
python-pycurl-7.15.5.1-4.el5.x86_64.rpm
rh-cds-0.27-1.el5_5.noarch.rpm
rh-rhua-0.91-1.el5_5.noarch.rpm
rh-rhua-0.95-1.el5_5.noarch.rpm
rh-rhui-tools-0.76-1.el5_5.noarch.rpm
rpm-build-4.4.2.3-20.el5_5.1.x86_64.rpm
```

**rhui-manager packages upload**

Use this command to upload a new package to a custom repository. Specify the repository to upload the packages to with the `--repo_id` flag, and the full path to an `.rpm` file or directory containing `.rpm` files with the `--packages` flag. The repository ID is shown in the output of the `rhui-manager repo list` command.

```
$ rhui-manager packages upload --repo_id rhui-1.2-5Server-x86_64 --
packages /home/example/filename.rpm
```

## Status

The `status` command is used to check the status of the RHUI.

### `rhui-manager status`

Displays a short summary of whether or not CDS instances are running.

```
$ rhui-manager status
US East Region CDS ..... [ UP ]
```

Use the `--code` flag to display a code that reflect the state of the RHUI (where an output of `0` means the RHUI is running, and any other output means one or more CDS instances have failed).

```
$ rhui-manager status --code
0
```

## CHAPTER 5. REPOSITORIES

The Repository Management screen is used to list, add, and delete repositories. You can also create and upload packages to custom repositories.

You will require a Red Hat content certificate and private key in order to access repositories with RHUI Manager. Each product requires its own content certificate, which is provided by Red Hat. Once you have run RHUI Manager for the first time, upload a new content certificate for each product you require by following the directions in [Procedure 8.3, “Upload Content Certificate”](#).

If you attempt to work with repositories without having a valid content certificate, you will see the following error message:

```
No Red Hat content certificates have been loaded. Upload
a content certificate to provide entitled products for import.
```

To access the Repository Management screen, go to the Home screen and type `r` at the prompt:

```
rhui (home) => r

-= Repository Management =-

l  list repositories currently managed by the RHUI
i  display detailed information on a repository
a  add a new Red Hat content repository
c  create a new custom repository
d  delete a repository from the RHUI
u  upload content to a custom repository
p  list packages in a repository

                               Connected: rhua.example.com
-----
rhui (repo) =>
```

### Procedure 5.1. List Repositories

- From the Repository Management screen, type `l` at the prompt to list the repositories currently being managed by the RHUI:

```
-----
-----
rhui (repo) => l

Custom Repositories
  Custom Repository 1

Red Hat Repositories
  Red Hat Update Infrastructure 1.2 (RPMS) (5Server-i386)
  Red Hat Update Infrastructure 1.2 (RPMS) (5Server-x86_64)
  Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
  Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-x86_64)
```

```
-----
-----
```

## Procedure 5.2. Display Repository Information

1. From the Repository Management screen, type `i` at the prompt to display information about a particular repository:

```
-----
-----
rhui (repo) => i
```

2. A list of all repositories currently being managed by the RHUI will be displayed. Select which repositories to view by typing the number of the repository at the prompt:

```
Select one or more repositories:
```

```
Custom Repositories
- 1 : Custom Repository 1

Red Hat Repositories
- 2 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
- 3 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
- 4 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
- 5 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-
x86_64)

Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?'
for more commands: 1
```

Typing the number of a repository will place a checkmark next to the name of that repository:

```
Select one or more repositories:
```

```
Custom Repositories
x 1 : Custom Repository 1

Red Hat Repositories
- 2 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
- 3 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
- 4 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
- 5 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-
x86_64)

Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?'
for more commands: 2
```

```
Select one or more repositories:
```

```
Custom Repositories
x 1 : Custom Repository 1
```

```

Red Hat Repositories
x  2 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
-  3 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
-  4 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
-  5 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-
x86_64)

Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?'
for more commands:

```

Continue until all repositories you wish to view have been checked, and then type **c** at the prompt to display the details:

```

Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?'
for more commands: c

Name:                Custom Repository 1
Type:                Custom
Relative Path:       custom/i386
Entitlement Path:    /custom/$basearch
Package Count:      0

Name:                Red Hat Update Infrastructure 1.2 (RPMs)
(5Server-i386)
Type:                Red Hat
Relative Path:       content/dist/rhel/rhui/server/5Server/i386/rhui/1.2/os
Package Count:      13
Last Sync:           05-11-2011 16:01
Next Sync:           05-13-2011 16:01

-----
-----
rhui (repo) =>

```

### Procedure 5.3. Add a Red Hat Repository

1. Before adding a new Red Hat repository, you will need to have the specific repositories loaded for your entitled products. For example, if your content certificate grants access to the product **Red Hat Enterprise Linux Server (RPMs)**, you will need to have both 32-bit and 64-bit repositories loaded. This occurs automatically when RHUI Manager contacts RHN.
2. From the Repository Management screen, type **a** at the prompt to add a new Red Hat repository:

```
rhui (repo) => a
```

3. There are three ways to add new Red Hat repositories:
  - o *All in Certificate*: Adds all available repositories for all entitled products in the certificate. You will be required to confirm the list of repositories before they are added.

- o *By Product*: Adds all available repositories for chosen products. As each repository is added, it will be displayed.
- o *By Repository*: This option shows a list of all available repositories for all entitled products. Select each individual repository to be added.

```
rhui (repo) => a

Loading latest entitled products from Red Hat...
... listings loaded
Determining undeployed products...
... product list calculated

Import Repositories:
  1 - All in Certificate
  2 - By Product
  3 - By Repository
Enter value (1-3) or 'b' to abort:
```

- o **All in Certificate method**

From the Add a Red Hat Repository screen, select the 'all in certificate' method by typing **1** at the prompt:

```
Enter value (1-3) or 'b' to abort: 1

All repositories for all entitled products will be imported in
this process. This may result in multiple repositories being
imported,
such as if a product is supported on multiple architectures.

The following products will be deployed:
  Red Hat Enterprise Linux Server 6 Releases (RPMs)
    Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-
x86_64)
    Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-
i386)
  Red Hat Enterprise Linux Server 6 Releases (SRPMS)
    Red Hat Enterprise Linux Server 6 Releases (SRPMS) (6Server-
x86_64)
    Red Hat Enterprise Linux Server 6 Releases (SRPMS) (6Server-
i386)
  Red Hat Enterprise Linux Server 6 Updates (RPMs)
    Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-
x86_64)
    Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-
i386)
  Red Hat Enterprise Linux Server 6 Updates (SRPMS)
    Red Hat Enterprise Linux Server 6 Updates (SRPMS) (6Server-
i386)
    Red Hat Enterprise Linux Server 6 Updates (SRPMS) (6Server-
x86_64)
Proceed? (y/n)
```

Confirm the list of repositories by typing **y** at the prompt:

**NOTE**

Content will not be downloaded to the newly imported repositories immediately. It will download when the next synchronization occurs.

- o **By Product**

From the Add a Red Hat Repository screen, select the 'by product' method by typing **2** at the prompt:

```
Import Repositories:
  1 - All in Certificate
  2 - By Product
  3 - By Repository
Enter value from (1-3) or 'b' to abort: 2
```

A list of products with repositories available to be added will be displayed. Select the products to be deployed to the RHUI by typing the number of each product at the prompt. Typing the number of a product will place a checkmark next to the name of that product. Continue until all products you want to deploy have been checked, and then type **c** at the prompt to confirm:

```
All repositories for selected products will be imported in this
process.
```

```
Select the products to be deployed to the RHUI (only undeployed
products are
displayed):
```

```
- 1 : Red Hat Enterprise Linux Server (RPMs)
- 2 : Red Hat Enterprise Linux Server (SRPMS)
- 3 : Red Hat Enterprise Linux Server (STS)
- 4 : Red Hat Enterprise Linux Server 6 Optional Releases
(RPMs)
- 5 : Red Hat Enterprise Linux Server 6 Optional Releases
(SRPMS)
- 6 : Red Hat Enterprise Linux Server 6 Optional Updates
(RPMs)
- 7 : Red Hat Enterprise Linux Server 6 Optional Updates
(SRPMS)
- 8 : Red Hat Enterprise Linux Server 6 Releases (RPMs)
- 9 : Red Hat Enterprise Linux Server 6 Releases (SRPMS)
- 10: Red Hat Enterprise Linux Server 6 Updates (RPMs)
- 11: Red Hat Enterprise Linux Server 6 Updates (SRPMS)
- 12: Red Hat Update Infrastructure 1.2 (SRPMS)
```

```
Enter value from (1-12) to toggle selection, 'c' to confirm
selections, or '?'
for more commands:
```

**NOTE**

Content will not be downloaded to the newly imported repositories immediately. It will download when the next synchronization occurs.



- **By Repository**

From the Add a Red Hat Repository screen, select the 'by repository' method by typing **3** at the prompt:

```

Enter value (1-3) or 'b' to abort: 3

Select the product repositories to be deployed to the RHUI (only
undeplied
products are displayed):
  Red Hat Enterprise Linux Server 6 Optional Updates (SRPMS)
    - 1 : Red Hat Enterprise Linux Server 6 Optional Updates
      (SRPMS)
      (6Server-i386)
    - 2 : Red Hat Enterprise Linux Server 6 Optional Updates
      (SRPMS)
      (6Server-x86_64)

  Red Hat Enterprise Linux Server 6 Updates (RPMs)
    - 3 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
      (6Server-x86_64)
    - 4 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
      (6Server-i386)

Enter value (1-4) to toggle selection, 'c' to confirm selections,
or '?' for
more commands: 1

... [output truncated] ...

Enter value (1-4) to toggle selection, 'c' to confirm selections,
or '?' for
more commands: c

The following product repositories will be deployed:
  Red Hat Enterprise Linux Server 6 Optional Updates (SRPMS)
  Red Hat Enterprise Linux Server 6 Optional Updates (SRPMS)
  (6Server-i386)
Proceed? (y/n)

```

A list of the repositories to be deployed will be displayed. Type **y** at the prompt to confirm the selection and deploy the products:



#### NOTE

Content will not be downloaded to the newly imported repositories immediately. It will download when the next synchronization occurs.

### Procedure 5.4. Delete a Red Hat Repository

1. Deleting a Red Hat repository using RHUI Manager will remove the repository from both the RHUA and any CDS instance it is deployed on.

From the Repository Management screen, type **d** at the prompt to delete a Red Hat repository:

```
rhui (repo) => d
```

2. A list of all repositories currently being managed by the RHUI will be displayed. Select which repositories to delete by typing the number of the repository at the prompt. Typing the number of a repository will place a checkmark next to the name of that repository. Continue until all repositories you wish to delete have been checked, and then type **c** at the prompt to confirm:

```
Select one or more repositories:
```

```
Custom Repositories
```

```
- 1 : Custom Repository 1
```

```
Red Hat Repositories
```

```
- 2 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
(6Server-i386)
- 3 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
(6Server-x86_64)
- 4 : Red Hat Enterprise Linux Server 6 Updates (SRPMS)
(6Server-i386)
- 5 : Red Hat Enterprise Linux Server 6 Updates (SRPMS)
(6Server-x86_64)
- 6 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
- 7 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
- 8 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
- 9 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-
x86_64)
```

```
Enter value (1-9) to toggle selection, 'c' to confirm selections, or
'?'
```

```
for more commands: 2-4
```

```
Select one or more repositories:
```

```
Custom Repositories
```

```
- 1 : Custom Repository 1
```

```
Red Hat Repositories
```

```
x 2 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
(6Server-i386)
x 3 : Red Hat Enterprise Linux Server 6 Updates (RPMs)
(6Server-x86_64)
x 4 : Red Hat Enterprise Linux Server 6 Updates (SRPMS)
(6Server-i386)
- 5 : Red Hat Enterprise Linux Server 6 Updates (SRPMS)
(6Server-x86_64)
- 6 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
- 7 : Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
- 8 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
- 9 : Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-
x86_64)
```

```
Enter value (1-9) to toggle selection, 'c' to confirm selections, or
'?'
```

```
for more commands: c
```

3. A list of the repositories to be deleted will be displayed. Type **y** at the prompt to confirm the selection and delete the repositories:

```
The following repositories will be deleted:
Red Hat Repositories
  Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-i386)
  Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-
x86_64)
  Red Hat Enterprise Linux Server 6 Updates (SRPMS) (6Server-i386)

Proceed? (y/n) y
```

**NOTE**

Repositories can not be deleted immediately. They will be deleted when the next CDS synchronization occurs.

**Procedure 5.5. List Packages in a Repository****NOTE**

When listing repositories within RHUI Manager, only repositories that contain less than 100 packages will have their contents displayed. Results with more than 100 packages will display a package count only. To see a complete list, regardless of how many packages are contained within a repository, use the `rhui-manager packages list` command at the shell prompt instead. See [Section 4.3, “Using RHUI Manager from the Shell Prompt”](#) for more information about managing RHUI from the shell prompt.

1. From the Repository Management screen, type **p** at the prompt to list the packages in a particular repository:

```
rhui (repo) => p

Choose a repository:
 1 - Custom Repository 1
 2 - Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-
i386)
 3 - Red Hat Enterprise Linux Server 6 Updates (RPMs) (6Server-
x86_64)
 4 - Red Hat Enterprise Linux Server 6 Updates (SRPMS) (6Server-
i386)
 5 - Red Hat Enterprise Linux Server 6 Updates (SRPMS) (6Server-
x86_64)
 6 - Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
 7 - Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
 8 - Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
 9 - Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-x86_64)

Enter value (1-9) or 'b' to abort:
```

2. Select the number of the repository you wish to view. RHUI Manager will ask if you want to filter the results. Leave the line blank to see the results without a filter:



```
Enter value (1-9) or 'b' to abort: 8
```

```
Enter the first few characters (case insensitive) of an RPM to
filter the
results
(blank line for no filter):
```

```
Only filtered results that contain less than 100 packages will have
their
contents displayed. Results with more than 100 packages will display
a package count only.
```

```
Packages:
```

```
PyYAML-3.08-4.el5.src.rpm
grinder-0.0.57-1.el5.src.rpm
httpd-2.2.3-43.el5_5.3.src.rpm
libyaml-0.1.2-3.el5.src.rpm
m2crypto-0.16-6.1.el5_5.1.src.rpm
mod_python-3.3.1-12.el5.src.rpm
python-hashlib-20081119-5.el5.src.rpm
python-pycurl-7.15.5.1-4.el5.src.rpm
rh-cds-0.27-1.el5_5.src.rpm
rh-rhua-0.91-1.el5_5.src.rpm
rh-rhua-0.95-1.el5_5.src.rpm
rh-rhui-tools-0.76-1.el5_5.src.rpm
rpm-4.4.2.3-20.el5_5.1.src.rpm
```

```
-----
-----
rhui (repo) =>
```

3. Alternatively, type the first few letters of the RPM name you are looking for to filter the results:

```
Enter the first few characters (case insensitive) of an RPM to
filter the
results
(blank line for no filter):
py
```

```
Only filtered results that contain less than 100 packages will have
their
contents displayed. Results with more than 100 packages will display
a package count only.
```

```
Packages:
```

```
PyYAML-3.08-4.el5.src.rpm
python-hashlib-20081119-5.el5.src.rpm
python-pycurl-7.15.5.1-4.el5.src.rpm
```

```
-----
-----
rhui (repo) =>
```

## 5.1. CUSTOM REPOSITORIES

### Procedure 5.6. Create a Custom Repository

1. From the Repository Management screen, type **p** at the prompt to list the packages in a particular repository:

```
rhui (repo) => c
```

2. Enter a unique ID for the repository. Only alphanumeric characters, **\_** (underscore), and **-** (hyphen) are permitted. You cannot use spaces in the unique ID. For example: **repo1**, **repo\_1**, and **repo-1** are all valid entries.

```
Unique ID for the custom repository (alphanumerics, _, and - only):
repo_1
```

3. Enter a display name for the repository. This name is used to identify the repository within RHUI Manager:

```
Display name for the custom repository [repo_1]:
Custom Repository 1
```

4. Specify the path that will host the repository. The path must be unique across all repos hosted by the RHUI. For example: if you specify the path at this step as **foo/bar/baz** then the repository will be located at **https://<server>/pulp/repos/foo/bar/baz**:

```
Path at which the repository will be served [repo_1]:
/custom/i386
```

5. Select the checksum type to be used for the repository metadata:

```
Algorithm to use when calculating the checksum values for repository
metadata:
  1 - sha256
  2 - sha1
Enter value (1-2) or 'b' to abort: 1
```

6. Choose whether or not to protect the new repository. If you answer **no** to this question, any client will be able to access the repository. If you answer **yes** then only clients with an appropriate entitlement certificate will be able to access the repository:

```
Should the repository require an entitlement certificate to access?
(y/n)
y
```

7. If you choose to protect the new repository, RHUI Manager will ask for the entitlement path. It will also make a suggestion for the entitlement path, based on the repository's relative path.

Client entitlement certificates contain the download URLs that they are allowed to access. RHUI analyzes the contents of the certificate to determine if the repository requested matches any of the permitted URLs, which determines whether or not it will allow the client to authenticate. For example: if an entitlement certificate grants access to **/foo/bar/baz**, and

the request is made to a repository located at `https://server/pulp/repos/foo/bar/baz/os/repodata` RHUI will approve the request and grant the authentication, because the path begins with one of the entitled download URLs. The URL only needs to begin with the correct information, it does not need to match exactly.

Entitlements can also contain variables, as long as `yum` knows the value for the variable. The two most common variables to use are `$basearch` and `$releasever`, which are populated with details of the client making the request. For example: if an entitlement certificate grants access to `/foo/$basearch/bar`, and the request is made to a repository located at `https://server/pulp/repos/foo/i386/bar` RHUI will approve the request and grant the authentication, because the path matches when the variable is populated.

RHUI Manager will suggest a path to use, based on the variables you used when you used when you gave it a path for the repository. Leave the field blank to accept the suggested path. In this example, the path was given as `/custom/i386`, so RHUI Manager has suggested that the `/i386` parameter be replaced with `$basearch` instead.

```
Based on the repository's relative path, the suggested entitlement
path is:
```

```
  /custom/$basearch
```

```
The following repositories have the same entitlement path as
suggested:
```

```
  Custom Repository 2
```

```
Path that should be used when granting an entitlement for this
repository. This
may use yum variable substitutions (e.g. $basearch) to group this
together with
other repositories that share the entitlement [/custom/$basearch]:
```

8. The details of the new repository will be displayed. Type `y` at the prompt to confirm the information and create the repository:

```
The following repository will be created:
```

```
  ID:          repo_1
  Name:        Custom Repository 1
  Path:        /custom/i386
  Entitlement: /custom/$basearch
Proceed? (y/n) y
```

```
Successfully created repository Custom Repository 1
```

```
-----
-----
```

```
rhui (repo) =>
```

### Procedure 5.7. Upload Packages to a Custom Repository

1. It is possible to upload multiple packages at a time, and to upload to more than one repository at a time. Packages are uploaded to the RHUA immediately, but will not be available on the CDS instance until the next time the CDS is synchronized.

From the Repository Management screen, type **u** at the prompt to upload new packages to a particular repository:

```
rhui (repo) => u
```

- A list of all available custom repositories will be displayed. Packages cannot be uploaded to Red Hat repositories. Select which repositories to add the packages to by typing the number of the repository at the prompt. Typing the number of a repository will place a checkmark next to the name of that repository. Continue until all repositories you wish to add to have been checked, and then type **c** at the prompt to confirm:

```
Select the repositories to upload the package into:
- 1 : Custom Repository 1

Enter value (1-1) to toggle selection, 'c' to confirm selections, or
'?'
for more commands: 1

Select the repositories to upload the package into:
x 1 : Custom Repository 1

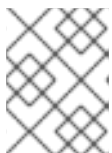
Enter value (1-1) to toggle selection, 'c' to confirm selections, or
'?'
for more commands: c
```

- Specify the location of the RPMs to be uploaded. This can be a single `.rpm` file, or it can be a directory containing several `.rpm` files. If you specify a directory, all `.rpm` files in that directory will be uploaded:

```
Enter the location of the packages to upload. If the location is an
RPM,
the file will be uploaded. If the location is a directory, all RPMs
in that
directory will be uploaded:
/home/example/data/rpms
```

- The details of the new packages to be uploaded will be displayed. Type **y** at the prompt to confirm the information and upload the packages:

```
The following RPMs will be uploaded:
emoticons-0.1-2.x86_64.rpm
feedless-1.0-1.noarch.rpm
origin-1.0-1.noarch.rpm
parent-1.0-1.noarch.rpm
patb-0.1-2.x86_64.rpm
Proceed? (y/n) y
```



#### NOTE

The packages will be uploaded to the RHUA immediately, but will not be available on the CDS until the CDS has performed a synchronization.

## CHAPTER 6. CONTENT DISTRIBUTION SERVER (CDS) INSTANCES

The CDS Management screen is used to list, add, and delete content distribution server (CDS) instances. From this screen, you can also access the CDS Repository Management screen, which allows you to view and change information for individual CDS instances.

To access the CDS Management screen, go to the Home screen and type `c` at the prompt:

```
rhui (home) => c
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= Content Delivery Server (CDS) Management =-

  l  list all CDS instances registered to the RHUI
  a  register (add) a new CDS instance
  d  unregister (delete) a CDS instance from the RHUI

                                   Connected: rhua.example.com
-----
-----
rhui (cds) =>
```

### Procedure 6.1. List CDS instances

- From the CDS Management screen, type `l` at the prompt to list the CDS instances currently being managed by the RHUI:

```
rhui (cds) => l

-= RHUI Content Delivery Servers =-

  US East Region CDS
  US West Region CDS

-----
-----
rhui (cds) =>
```

### Procedure 6.2. Add a CDS Instance

- From the CDS Management screen, type `a` at the prompt to add a new CDS instance:

```
rhui (cds) => a
```



2.

**IMPORTANT**

Ensure that the CDS you are adding is configured and running. If the CDS is not running before you try to register it, the registration will fail.

Enter the hostname of the CDS to added. This must match the hostname configured on the CDS itself. You cannot use the IP address. If the hostname does not match exactly, the operation will fail.

```
Prior to registering a CDS, the CDS must be configured and running.
```

```
Hostname of the CDS to register:
cds.us-east.example.com
```

3. Enter a display name for the CDS. This name is used to identify the CDS within RHUI Manager. Alternatively, leave the field blank to use the hostname as the display name:

```
Display name for the CDS [cds.us-east.example.com]:
US East Region CDS
```

4. The details of the new CDS will be displayed. Type **y** at the prompt to confirm the information and create the CDS:

```
The following CDS instance will be registered:
```

```
  Hostname: cds.us-east.example.com
```

```
  Name:      US East Region CDS
```

```
Proceed? (y/n) y
```

```
Successfully registered US East Region CDS
```

```
-----
```

```
rhui (cds) =>
```

**NOTE**

If adding the CDS fails, check that the CDS daemon **pulp-cds** is running and that the firewall rules permit access between the RHUA and the CDS.

**Procedure 6.3. Delete a CDS Instance****WARNING**

When a CDS is deleted, all of the repositories and data will be lost. It is important that RHUI Manager can access the CDS to ensure that content is no longer being hosted from the CDS instance before it is deleted.

1. From the CDS Management screen, type `d` at the prompt to delete a CDS instance:

```
rhui (cds) => d
```

2. A list of all CDS instances currently being managed by the RHUI will be displayed. Select which CDS instances to delete by typing the number of the CDS at the prompt. Typing the number of a CDS will place a checkmark next to the name of that CDS. Continue until all CDS instances you wish to delete have been checked, and then type `c` at the prompt to confirm:

```
Select the CDS instances to be removed from the RHUI:
- 1 : US East Region CDS
Enter value from (1-1) to toggle selection, 'c' to confirm
selections, or '?'
for more commands: 1
```

```
Select the CDS instances to be removed from the RHUI:
x 1 : US East Region CDS
Enter value from (1-1) to toggle selection, 'c' to confirm
selections, or '?'
for more commands: c
```

3. A list of the CDS instances to be deleted will be displayed. Type `y` at the prompt to confirm the selection and delete the CDS instances:

```
The following CDS instances will be unregistered:
  US East Region CDS
Proceed? (y/n) y

Unregistering US East Region CDS...

-----
-----
rhui (cds) =>
```

4. RHUI Manager contacts the CDS to ensure it is properly cleaned up when it is deleted. RHUI Manager is unable to delete a CDS instance that it cannot communicate with. However, there are some cases where you might need to remove an unresponsive CDS instance.



### IMPORTANT

CDS instances exchange a secret with the RHUA so that only the RHUA is able to communicate with it. This secret is removed as part of the cleanup operation when a CDS is deleted normally. When a CDS instance is forcibly removed without being properly cleaned up, this secret is not deleted. You will not be able to register the CDS again until that secret has been removed. You can do this manually by deleting the `/var/lib/pulp-cds/.gofer/secret` file.

When you attempt to perform a delete operation on a CDS instance that is not running, RHUI Manager will notify you that it is unable to delete the CDS, and ask if you want to forcibly remove the CDS. Type `y` to forcibly remove the unresponsive CDS:

**WARNING**

Be very careful with this command. If you delete a CDS instance that is not running, RHUI Manager cannot confirm that the CDS instance is not hosting repositories that have previously been deployed.

```

-----
-----
rhui (cds) => d

Select the CDS instances to be removed from the RHUI:
  - 1 : CDS 1
Enter value (1-1) to toggle selection, 'c' to confirm selections, or
'?' for
more commands: 1

Select the CDS instances to be removed from the RHUI:
  x 1 : CDS 1
Enter value (1-1) to toggle selection, 'c' to confirm selections, or
'?' for
more commands: c

All previously deployed repositories will be deleted when a CDS is
unregistered.

The following CDS instances will be unregistered:
  CDS 1
Proceed? (y/n) y

Unregistering CDS 1...

The following CDS instances could not be contacted to be
unregistered.
They may still be removed from the RHUI database, however the RHUI
is unable
confirm that they have stopped hosting repositories.
  CDS 1

Forcibly remove these CDS instances? (y/n)y

Forcibly unregistering CDS 1...

```

## CHAPTER 7. CLIENT ENTITLEMENTS

The Create Certificates and Configuration RPMs screen is used to create new entitlement certificates and configuration RPMs.

When Red Hat issues the original entitlement certificate, it will grant access to the repositories you requested. When you create client entitlement certificates, you will need to decide how to sub-divide your clients, and create a separate certificate for each one. Each certificate can then be used to create individual RPMs for installation on the appropriate guest images. For example, you might create separate certificates for clients that require access to Red Hat Enterprise Linux 5 and those that require access to Red Hat Enterprise Linux 5 and JBoss channels.

To access the Create Certificates and Configuration RPMs screen, go to the Home screen and type `e` at the prompt:

```
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= Client Entitlement Management -=

    e   generate an entitlement certificate
    c   create a client configuration RPM from an entitlement certificate

                                                    Connected:
rhua.example.com
-----
-----
rhui (client) =>
```

### Procedure 7.1. Generate an Entitlement Certificate

1. From the Create Certificates and Configuration RPMs screen, type `e` at the prompt to generate a new Red Hat entitlement certificate:

```
rhui (client) => e
```

2. A list of all available repositories will be displayed. This includes all custom repositories, and all products that have been granted entitlements in the content certificate that Red Hat granted. Select which repositories to include in the entitlement certificate by typing the number of the repository at the prompt. Typing the number of a repository will place a checkmark next to the name of that repository. Continue until all repositories you wish to add have been checked, and then type `c` at the prompt to confirm.

Repositories that are shown with an asterisk (\*) indicates that they are deployed in the RHUI.

```
Select one or more repositories to include in the entitlement
certificate:
(an * next to a Red Hat repository indicates it is deployed in the
RHUI)
```

```
Custom Repositories
- 1 : /protected/$basearch/os
```

Repo 1  
Repo 2

#### Red Hat Repositories

- 2 : Red Hat Enterprise Linux Server (RPMs)
- 3 : Red Hat Enterprise Linux Server (SRPMS)
- 4 : Red Hat Enterprise Linux Server (STS)
- 5 : Red Hat Enterprise Linux Server 6 Optional Releases (RPMs)
- 6 : Red Hat Enterprise Linux Server 6 Optional Releases (SRPMS)
- 7 : Red Hat Enterprise Linux Server 6 Optional Updates (RPMs)
- 8 : Red Hat Enterprise Linux Server 6 Optional Updates (SRPMS)
- 9 : Red Hat Enterprise Linux Server 6 Releases (RPMs)
- 10: Red Hat Enterprise Linux Server 6 Releases (SRPMS)
- 11: Red Hat Enterprise Linux Server 6 Updates (RPMs)
- 12: Red Hat Enterprise Linux Server 6 Updates (SRPMS)
- 13: Red Hat Update Infrastructure 1.2 (RPMs) \*
- 14: Red Hat Update Infrastructure 1.2 (SRPMS) \*

Enter value from (1-14) to toggle selection, 'c' to confirm selections, or '?'  
for more commands: 1

Select one or more repositories to include in the entitlement certificate:  
(an \* next to a Red Hat repository indicates it is deployed in the RHUI)

#### Custom Repositories

- x 1 : /protected/\$basearch/os  
Repo 1  
Repo 2

#### Red Hat Repositories

- 2 : Red Hat Enterprise Linux Server (RPMs)
- 3 : Red Hat Enterprise Linux Server (SRPMS)
- 4 : Red Hat Enterprise Linux Server (STS)
- 5 : Red Hat Enterprise Linux Server 6 Optional Releases (RPMs)
- 6 : Red Hat Enterprise Linux Server 6 Optional Releases (SRPMS)
- 7 : Red Hat Enterprise Linux Server 6 Optional Updates (RPMs)
- 8 : Red Hat Enterprise Linux Server 6 Optional Updates (SRPMS)
- 9 : Red Hat Enterprise Linux Server 6 Releases (RPMs)
- 10: Red Hat Enterprise Linux Server 6 Releases (SRPMS)
- 11: Red Hat Enterprise Linux Server 6 Updates (RPMs)
- 12: Red Hat Enterprise Linux Server 6 Updates (SRPMS)
- 13: Red Hat Update Infrastructure 1.2 (RPMs) \*
- 14: Red Hat Update Infrastructure 1.2 (SRPMS) \*

Enter value from (1-14) to toggle selection, 'c' to confirm selections, or '?'  
for more commands: 13-14

Select one or more repositories to include in the entitlement certificate:  
(an \* next to a Red Hat repository indicates it is deployed in the RHUI)

Custom Repositories

```
x 1 : /protected/$basearch/os
      Repo 1
      Repo 2
```

Red Hat Repositories

```
- 2 : Red Hat Enterprise Linux Server (RPMs)
- 3 : Red Hat Enterprise Linux Server (SRPMS)
- 4 : Red Hat Enterprise Linux Server (STS)
- 5 : Red Hat Enterprise Linux Server 6 Optional Releases
(RPMs)
- 6 : Red Hat Enterprise Linux Server 6 Optional Releases
(SRPMS)
- 7 : Red Hat Enterprise Linux Server 6 Optional Updates (RPMs)
- 8 : Red Hat Enterprise Linux Server 6 Optional Updates
(SRPMS)
- 9 : Red Hat Enterprise Linux Server 6 Releases (RPMs)
- 10: Red Hat Enterprise Linux Server 6 Releases (SRPMS)
- 11: Red Hat Enterprise Linux Server 6 Updates (RPMs)
- 12: Red Hat Enterprise Linux Server 6 Updates (SRPMS)
x 13: Red Hat Update Infrastructure 1.2 (RPMs) *
x 14: Red Hat Update Infrastructure 1.2 (SRPMS) *
```

Enter value from (1-14) to toggle selection, 'c' to confirm selections, or '?'  
for more commands: c

3. Enter a name for the certificate. This name is used to identify the certificate within RHUI Manager, and is also used to generate the name of the certificate and key files.

Name of the certificate. This will be used as the name of the certificate file (name.crt) and its associated private key (name.key). Choose something that will help identify the products contained with it:  
rhui\_and\_custom

4. Enter a path to save the certificate to. Leave the field blank to save to the current working directory:

Local directory in which to save the generated certificate [current directory]:  
/tmp/certs

5. Enter the number of days the certificate should be valid for. Leave the field blank for 365 days:

Number of days the certificate should be valid [365]:

- The details of the repositories to be included in the certificate will be displayed. Type `y` at the prompt to confirm the information and create the entitlement certificate.

If your CA private key requires a pass phrase to sign certificates, enter it at the prompt.

```
Repositories to be included in the entitlement certificate:

Custom Entitlements
  /protected/$basearch/os

Red Hat Repositories
  Red Hat Update Infrastructure 1.2 (RPMs)
  Red Hat Update Infrastructure 1.2 (SRPMS)

Proceed? (y/n) y

.....+++
..+++
Enter pass phrase for /etc/pki/rhui/entitlement-ca-key.pem:
Entitlement certificate created at /tmp/certs/rhui_and_custom.crt

-----
-----
rhui (client) =>
```

### Procedure 7.2. Create a Client Configuration RPM

- From the Create Certificates and Configuration RPMs screen, type `c` at the prompt to create a client configuration RPM:

```
rhui (client) => c
```

- Enter a path to a local directory to save the configuration files to. Leave the field blank to save to the current working directory:

```
Local directory in which the client configuration files generated by
this tool
should be stored (if this directory does not exist, it will be
created):
/tmp/test-client
```

- Enter a name for the RPM. Do not specify the `.rpm` extension:

```
Name of the RPM:
test-client
```

- Enter a version number for the configuration RPM. Leave the field blank to use version 2.0:

```
Version of the configuration RPM [2.0]:
```

- Enter the full path to the entitlement certificate to be used (the entitlement certificate is generated in [Procedure 7.1, “Generate an Entitlement Certificate”](#)):

```
Full path to the entitlement certificate authorizing
the client to access specific channels:
/tmp/certs/rhui_and_custom.crt
```

6. Enter the full path to the private key to be used with the entitlement certificate (the private key is generated in [Procedure 7.1, “Generate an Entitlement Certificate”](#)):

```
Full path to the private key for the above entitlement certificate:
/tmp/certs/rhui_and_custom.key
```

7. Enter the full path to the CA certificate that was used to sign the CDS SSL certificates. This is used by **yum** on the client, when it attempts to connect to the CDS:

```
Full path to the CA certificate used to sign the CDS SSL
certificate:
/etc/pki/rhui/entitlement-ca.crt
```

8. All CDS instances are able to function as load balancers. You will be required to nominate one CDS as a primary load balancer, however if that CDS becomes unavailable, or is unable to function as a load balancer, load balancing tasks will fall to the other available CDS instances. Select a CDS instance to be the primary load balancer for the client:

```
Select the CDS instance that should be the primary load balancer for
the
client. All other CDS instances will be listed as back up load
balancers
in the client's mirror list:

 1 - cds-1.example.com
 2 - cds-2.example.com
Enter value (1-2) or 'b' to abort: 2
```

A list of the CDS instances to be used for load balancing will be displayed, in priority order:

```
Load Balancer Order:
  cds-2.example.com
  cds-1.example.com
```

9. A list of all unprotected repositories will be displayed. Select which repositories (if any) to include in the RPM by typing the number of the repository at the prompt. Typing the number of a repository will place a checkmark next to the name of that repository. Continue until all repositories you wish to add have been checked, and then type **c** at the prompt to confirm. If you don't want to add any repositories to the RPM, leave all repositories unchecked and type **c** at the prompt to confirm.

Unprotected repositories that are added to the RPM will be included in the generated **.repo** file, along with the repository definitions for all entitlements included in the certificate.

```
Select any unprotected repositories to be included in the client
configuration:
- 1 : Unprotected Repo 1
Enter value from (1-1) to toggle selection, 'c' to confirm
selections, or '?'
```



```
for more commands: 1
```

```
Select any unprotected repositories to be included in the client
configuration:
```

```
  x 1 : Unprotected Repo 1
```

```
Enter value from (1-1) to toggle selection, 'c' to confirm
selections, or '?'
```

```
for more commands: c
```

10. The client configuration RPM will be created, and the location of the file displayed:

```
Successfully created client configuration RPM.
```

```
RPMs can be found at /tmp/test-client
```

```
-----
```

```
-----
```

```
rhui (client) =>
```

## CHAPTER 8. MANAGING ENTITLEMENT CERTIFICATES

The Entitlements Manager screen is used to list entitled products in the current Red Hat content certificates and upload new certificates.

To access the Entitlements Manager screen, go to the Home screen and type `n` at the prompt:

```
rhui (entitlements) => n
-----
-----
                    -= Red Hat Update Infrastructure Management Tool -=

-= Entitlements Manager =-

  l  list Red Hat content certificate entitlements
  c  list custom repository entitlements
  u  upload a new or updated Red Hat content certificate

                                                                    Connected:
rhua.example.com
-----
-----
rhui (entitlements) =>
```

### Procedure 8.1. List Certificate Information

- From the Entitlements Manager screen, type `l` at the prompt to list data about the current content certificate.

RHUI Manager will give the following information about the certificate:

**Table 8.1. Certificate Information**

Value	Description
<b>Not Before</b>	The start date of the certificate. The certificate is only valid after this date.
<b>Not After</b>	The expiry date of the certificate
<b>Serial Number</b>	The serial number of the certificate
<b>Entitlements</b>	The entitlements the certificate grants

```
rhui (entitlements) => l

Red Hat Entitlements

  Valid
    Red Hat Enterprise Linux Server (RPMs)
```

```

Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Enterprise Linux Server (SRPMS)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Enterprise Linux Server 6 Releases (RPMs)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Enterprise Linux Server 6 Releases (SRPMS)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Enterprise Linux Server 6 Updates (RPMs)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Enterprise Linux Server 6 Updates (SRPMS)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Update Infrastructure 1.2 (RPMs)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Red Hat Update Infrastructure 1.2 (SRPMS)
Expiration: 01-31-2012      Certificate: big-content-cert.pem

Expired
Red Hat Update Infrastructure 1.1 (RPMs)
Expiration: 06-25-2011      Certificate: content-cert.pem

-----
rhui (entitlements) =>

```

### Procedure 8.2. List Custom Repository Entitlements

- From the Entitlements Manager screen, type **c** at the prompt to list data about the custom repository entitlements.

```

rhui (entitlements) => c

Custom Repository Entitlements

For each entitlement URL listed, the corresponding repositories
that are configured with that entitlement are listed.

/protected/$basearch/os
- Name: Repo 1
  URL: protected/i386/os
- Name: Repo 2
  URL: protected/x86_64/os

-----
rhui (entitlements) =>

```

### Procedure 8.3. Upload Content Certificate

Red Hat might need to issue a new content certificate if your old content certificate is about to expire, or to change the entitlements of the certificate. If Red Hat issues a new content certificate, it will need to be uploaded to RHUI.

**NOTE**

When you upload a new content certificate, it will also be updated in the RHUA, and will be used for synchronizing Red Hat repositories. For this reason, do not upload a new content certificate before it becomes valid, as it will cause your synchronizations to fail until the valid date is reached.

**NOTE**

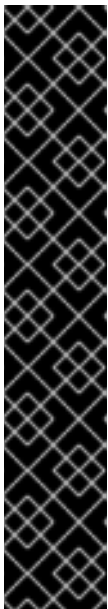
If two or more content certificates provide the same entitlements, the certificate with an expiration date furthest in the future will be used.

RHUI Manager expects that both the content certificate and its private key will be contained in the same file. If you have existing content certificates with separate keys, you can create the single file using the `cat` command at a shell prompt:

```
$ cat content.crt content.key > content-2.0.pem
```

1. From the Entitlements Manager screen, type `u` at the prompt to upload a new content certificate:

```
rhui (entitlements) => u
```

**IMPORTANT**

Content certificates are stored on the same system RHUI Manager is installed on, at `/etc/pki/rhui`. For security reasons, this directory requires root permissions. If you do not have the correct permissions, RHUI Manager will not allow you to proceed:

```
rhui (entitlements) => u
```

```
The current user does not have write privileges to update
the
content cert at /etc/pki/rhui/content-cert.crt.
```

```
-----
```

```
rhui (entitlements) =>
```

2. Enter the full path to the new content certificate:

```
Full path to the new content certificate:
/home/example/rhui-certs/cert-1.pem
```

- The details of the new certificate to be uploaded will be displayed. Type `y` at the prompt to confirm the information and upload the packages. RHUI Manager will then list the current certificates:

```
The RHUI will be updated with the following certificate:
```

```
  Certificate:
/home/example/rhui-certs/cert-1.pem
```

```
Proceed? (y/n) y
```

```
Red Hat Entitlements
```

```
RHEL 5
Expiration: 06-06-2012      Certificate: cert-2.pem
```

```
RHUI 1.1
Expiration: 06-07-2012     Certificate: cert-1.pem
```

```
RHUI 1.2
Expiration: 06-07-2012     Certificate: cert-1.pem
```

```
-----
-----
rhui (entitlements) =>
```

## CHAPTER 9. IDENTITY CERTIFICATES

The Identity Certificate Management screen is used to create new entitlement certificates and configuration RPMs.

An identity certificate is used by Red Hat Update Infrastructure to authenticate the CDS to the RHUA and secure the communication between them. Entitlement certificates grant a client access to a specific set of entitled repositories, but the RHUA monitoring functionality and the load balancer require access to all repositories in the system. The identity certificate can be used to identify each component as part of Red Hat Update Infrastructure, so that the entitlement-checking procedure will not deny it access.

An identity certificate is generated for you the first time you use RHUI Manager. When the identity certificate generated by that process expires, you will need to regenerate the certificate in order to continue using Red Hat Update Infrastructure.

Only one identity certificate is needed for the entire infrastructure. The same certificate is used by both the RHUA and the load balancer.

To access the Identity Certificate Management screen, go to the Home screen and type `i` at the prompt:

```
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= Identity Certificate Management -=

    g   generate a new identity certificate

                                                    Connected:
rhua.example.com
-----
-----
rhui (client) =>
```

### Procedure 9.1. Generate a New Identity Certificate

1. From the Identity Certificate Management screen, type `g` at the prompt to generate a new identity certificate:

```
rhui (client) => g
```

2. Confirm that the new identity certificate will over-write the existing certificate by typing `y` at the prompt:

```
Generating a new RHUI identity certificate will replace
the one currently stored at /etc/pki/rhui/identity.crt. Proceed?
[y/n]: y
```

3. Enter the number of days that the identity certificate should be valid for. If left blank, this field will default to 3650 (ten years):

Enter the number of days the RHUI identity certificate will be valid.

If the identity certificate ever expires, it will need to be regenerated using `rhui-manager` [Default: 3650]:

4. The new identity certificate will be created. You should restart the service to pick up the changes:

```
.....+++
```

```
.....+++
```

```
Successfully regenerated RHUI Identity certificate
```

## CHAPTER 10. STATUS AND SCHEDULING

Synchronization is used to keep data on CDS instances and repositories current. By default, a synchronization will occur every six hours, but this schedule can be adjusted. It is also possible to manually run a synchronization when required. Manual synchronizations are additional to the schedule, and do not change the scheduled synchronization times.

The Synchronization Status and Scheduling screen is used to display the synchronization schedules for CDS instances and repositories, and view past synchronizations. You can also trigger individual synchronizations from this screen.

Within the Synchronization Status and Scheduling screen, the following terms are used to describe the final status of the most recent synchronization:

**Table 10.1. Synchronization Status Descriptions**

Status	Description
<b>In Progress</b>	A synchronization is in progress. You will not be able to trigger another synchronization until after the running one has completed.
<b>Awaiting Execution</b>	A synchronization is ready to run, but is waiting for other tasks to complete.
<b>Success</b>	The last synchronization finished successfully.
<b>Error</b>	The last synchronization failed.

To access the Synchronization Status and Scheduling screen, go to the Home screen and type `s` at the prompt:

```
rhui (home) => s
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= Synchronization Status =-

dr  display repo sync summary
vr  view the details of the last repository sync
sr  sync an individual repository immediately
dc  display CDS sync summary
vc  view the details of the last CDS sync
sc  sync an individual CDS immediately

                                                                    Connected:
rhua.example.com
-----
-----
rhui (sync) =>
```



**Procedure 10.1. List Repository Synchronization Status**

1. From the Synchronization Status and Scheduling screen, type `dr` at the prompt to see the synchronization status of all available repositories:

```

rhui (sync) => dr
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= Repository Synchronization Status =-

Last Refreshed: 13:53:52
(updated every 5 seconds, ctrl+c to exit)

Next Sync          Last Sync          Last
Result
-----
Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-i386)
In Progress        06-20-2011 14:33          Success

Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-x86_64)
In Progress        Never                    Error

Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
In Progress        06-20-2011 13:52          Success

Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
In Progress        06-20-2011 13:52          Success

Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
Awaiting Execution 06-20-2011 13:53          Success

Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-x86_64)
Awaiting Execution 06-20-2011 13:53          Success

                                                    Connected:
rhua.example.com
-----

```

**Last Result**

Shows the result of the last synchronization. Possible values are **Never** if the repository has not been synchronized before, **Success** if the last synchronization completed successfully, or **Error** if the last synchronization did not complete successfully.

**Last Sync**

Shows the time the last synchronization occurred. Possible values are **Never** if the repository has not been synchronized before, or the date and time of the last synchronization.

**NOTE**

Regular scheduled synchronizations will occur even if a manual synchronization as been triggered.

**Next Sync**

Shows when the next synchronization will occur. If a synchronization is currently running, this column will display either **In Progress** if the synchronization is running, or **Awaiting Execution** if a synchronization is ready to run, but is waiting on other tasks to complete.

2. The display will continue to update every five seconds. Press **Ctrl+C** to return to the prompt.

**Procedure 10.2. View Last Synchronization Details**

1. From the Synchronization Status and Scheduling screen, type **vr** at the prompt to see details about the last repository synchronization:

```
rhui (sync) => vr
```

2. A list of all repositories currently being managed by the RHUI will be displayed. Select which repository to view synchronization information for by typing the number of the repository at the prompt:

```
Select a repository:
1 - Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-i386)
2 - Red Hat Enterprise Linux Server 6 Releases (RPMs) (6Server-x86_64)
3 - Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
4 - Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
5 - Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-i386)
6 - Red Hat Update Infrastructure 1.2 (SRPMS) (5Server-x86_64)
Enter value (1-6) or 'b' to abort: 1
```

3. The synchronization information for the selected repository will be displayed:

```
Start Time: 06-20-2011 13:52
Finish Time: 06-20-2011 14:33
Elapsed Time: 0:41:08
Result: Success
```

The **Elapsed Time** displays the amount of time the synchronization took to run, in the format **hours:minutes:seconds**. The **Result** field shows the result of the synchronization, and will display either **Success** if the last synchronization completed successfully, or **Error** if the last synchronization failed. If the last synchronization failed, RHUI Manager will also display **Exception** a one line description of the error, and **Traceback**, a full traceback to be used when reporting the error.

**Procedure 10.3. List CDS Synchronization Status**

1. From the Synchronization Status and Scheduling screen, type `dc` at the prompt to see the synchronization status of all available repositories:

```
rhui (sync) => dc
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= CDS Synchronization Status -=

Last Refreshed: 16:08:54
(updated every 5 seconds, ctrl+c to exit)

cds00133 ..... [ UP
]
cds00175 ..... [ UP
]

Next Sync                Last Sync                Last
Result
-----
cds00133
07-04-2011 16:23         07-04-2011 16:07         Success

cds00175
07-04-2011 16:24         07-04-2011 16:07         Success

Connected: rhua.example.com
-----
```

2. The display will continue to update every five seconds. Press `Ctrl+C` to return to the prompt.

#### Procedure 10.4. Trigger a Repository Synchronization

1. From the Synchronization Status and Scheduling screen, type `sr` at the prompt to trigger a manual repository synchronization. This will trigger another synchronization in addition to the ordinary scheduled synchronizations:

```
rhui (sync) => sr
```

2. A list of available repositories will be displayed. Select which repositories to synchronize by typing the number of each repository at the prompt. Typing the number of a repository will place a checkmark next to the name of that repository. Continue until all repositories you want to synchronize have been checked, and then type `c` at the prompt to confirm:

```
Select one or more repositories to schedule to be synchronized
before its scheduled time.
The sync will happen as soon as possible depending on other tasks
that may be executing
in the RHUI. Only repositories that are not currently synchronizing
```

are displayed.

```

                Last Result          Next Sync          Repository
                -----
- 1 : Success    07-04-2011 19:26  Red Hat Enterprise Linux
Server 6 Updates (RPMs) (6Server-x86_64)
- 2 : Success    07-04-2011 21:12  Red Hat Update Infrastructure
1.1 (RPMs) (5Server-i386)
- 3 : Success    07-04-2011 21:12  Red Hat Update Infrastructure
1.1 (RPMs) (5Server-x86_64)
- 4 : Success    07-04-2011 19:26  Red Hat Update Infrastructure
1.2 (RPMs) (5Server-i386)
- 5 : Success    07-04-2011 19:26  Red Hat Update Infrastructure
1.2 (RPMs) (5Server-x86_64)
Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?' for more commands: 4-5

```

Select one or more repositories to schedule to be synchronized before its scheduled time.

The sync will happen as soon as possible depending on other tasks that may be executing in the RHUI. Only repositories that are not currently synchronizing are displayed.

```

                Last Result          Next Sync          Repository
                -----
- 1 : Success    07-04-2011 19:26  Red Hat Enterprise Linux
Server 6 Updates (RPMs) (6Server-x86_64)
- 2 : Success    07-04-2011 21:12  Red Hat Update Infrastructure
1.1 (RPMs) (5Server-i386)
- 3 : Success    07-04-2011 21:12  Red Hat Update Infrastructure
1.1 (RPMs) (5Server-x86_64)
x 4 : Success    07-04-2011 19:26  Red Hat Update Infrastructure
1.2 (RPMs) (5Server-i386)
x 5 : Success    07-04-2011 19:26  Red Hat Update Infrastructure
1.2 (RPMs) (5Server-x86_64)
Enter value (1-5) to toggle selection, 'c' to confirm selections, or
'?' for more commands: c

```

3. A list of the repositories to be synchronized will be displayed. Type **y** at the prompt to confirm the selection and trigger the synchronizations:

```

The following repositories will be scheduled for synchronization:
  Red Hat Update Infrastructure 1.2 (RPMs) (5Server-i386)
  Red Hat Update Infrastructure 1.2 (RPMs) (5Server-x86_64)
Proceed? (y/n) y

```

```

Scheduling sync for Red Hat Update Infrastructure 1.2 (RPMs)
(5Server-i386)...
... successfully scheduled for the next available timeslot.
Scheduling sync for Red Hat Update Infrastructure 1.2 (RPMs)
(5Server-x86_64)...
... successfully scheduled for the next available timeslot.

```

```
-----
-----
rhui (sync) =>
```

**NOTE**

Manual synchronizations will not always occur immediately, depending on other tasks the RHUI is currently performing. The synchronization will occur as soon as the RHUI has an available timeslot.

**Procedure 10.5. Trigger a CDS Synchronization**

1. From the Synchronization Status and Scheduling screen, type `sc` at the prompt to trigger a manual CDS synchronization. This will trigger another synchronization in addition to the ordinary scheduled synchronizations:

```
rhui (sync) => sc
```

Select one or more CDS instances to schedule to be synchronized before its scheduled time.

The sync will happen as soon as possible depending on other tasks that may be executing in the RHUI. Only CDS instances that are not currently synchronizing are displayed.

```

                Last Result   Next Sync           CDS
-----
-  1 : Error  07-04-2011 16:23  cds00133
-  2 : Error  07-04-2011 16:24  cds00175
Enter value (1-2) to toggle selection, 'c' to confirm selections, or
'?' for more commands: 1-2
```

2. A list of available CDS instances will be displayed. Select which CDS instances to synchronize by typing the number of each CDS instance at the prompt. Typing the number of a CDS instance will place a checkmark next to the name of that CDS. Continue until all CDS instances you want to synchronize have been checked, and then type `c` at the prompt to confirm:

Select one or more CDS instances to schedule to be synchronized before its scheduled time.

The sync will happen as soon as possible depending on other tasks that may be executing in the RHUI. Only CDS instances that are not currently synchronizing are displayed.

```

                Last Result   Next Sync           CDS
-----
x  1 : Error  07-04-2011 16:23  cds00133
x  2 : Error  07-04-2011 16:24  cds00175
Enter value (1-2) to toggle selection, 'c' to confirm selections, or
'?' for more commands: c
```

3. A list of the CDS instances to be synchronized will be displayed. Type `y` at the prompt to confirm the selection and trigger the synchronizations:

■

```
The following CDS instances will be scheduled for synchronization:
  cds00133
  cds00175
Proceed? (y/n) y

Scheduling sync for cds00133...
... successfully scheduled for the next available timeslot.
Scheduling sync for cds00175...
... successfully scheduled for the next available timeslot.

-----
rhui (sync) =>
```



**NOTE**

Manual synchronizations will not always occur immediately, depending on other tasks the RHUI is currently performing. The synchronization will occur as soon as the RHUI has an available timeslot.

## CHAPTER 11. USERS

The User screen is used to change the user password.



### IMPORTANT

Ensure you change the default password for the RHUA before you begin using the system.

To access the User screen, go to the Home screen and type `u` at the prompt:

```
rhui (home) => u
-----
-----
                -= Red Hat Update Infrastructure Management Tool -=

-= User Manager =-

    p   change a user's password

                                                    Connected:
rhua.example.com
-----
-----
rhui (users) =>
```

### Procedure 11.1. Change User Password

1. From the User screen, type `p` at the prompt to change the user password:

```
rhui (users) => p
```

2. Enter the username of the user that requires the password change:

```
Username: admin
```

3. Enter the new password for the user, and re-enter it:

```
New Password:
Re-enter Password:
```

4. RHUI Manager will update the password:

```
Password successfully updated.
```

```
-----
-----
rhui (users) =>
```

## CHAPTER 12. MONITORING

RHUI Manager can display information about the state of the Red Hat Update Infrastructure installation in several different ways. The most human-readable information is available in the Synchronization Status and Scheduling screen, which is described in [Chapter 10, Status and Scheduling](#). Status and monitoring information can also be obtained in a machine-readable state, for use with automated monitoring solutions such as Nagios.

### Procedure 12.1. Monitoring the state of Red Hat Update Infrastructure

1. To retrieve an exit code that provides a summary of the current state of the Red Hat Update Infrastructure, run the `rhui-manager` command from the shell prompt with the `status` command, and `echo` the result to standard output:

```
$ rhui-manager --username admin --password admin status
$ echo $?
0
```

This command should be automated to suit your individual requirements.



#### NOTE

It is recommended that this command always be used with the `--username` and `--password` switches specified, in order to bypass the authentication certificate and avoid the command failing due to expired credentials.

2. An exit status of `0` indicates that the Red Hat Update Infrastructure is running correctly. Any other value indicates that there has been an error.

### Log Files

- `~/.rhui/rhui.log`

RHUI Manager logs

- `/var/log/pulp/pulp.log`

RHUA logs



#### NOTE

The `pulp.log` file is automatically written to a new enumerated log file when the base file reaches 1MB in size. The most recent four versions are kept in addition to the currently written file.

- `/var/log/pulp/grinder.log`

Package synchronization output



**NOTE**

The `grinder.log` file is automatically written to a new enumerated log file when the base file reaches 1MB in size. The most recent four versions are kept in addition to the currently written file.

- `/var/log/pulp-cds/gofer.log`

The `gofer.log` file is located on CDS instances, and logs information about errors related to the CDS function.

- `/var/log/gofer/agent.log`

The `agent.log` file is located on CDS instances, and logs information about communication errors. This file contains information about whether the CDS instance was able to successfully connect to the Qpid broker running on the RHUA.

## CHAPTER 13. UPDATING RED HAT UPDATE INFRASTRUCTURE

This chapter explains how to update your Red Hat Update Infrastructure installation.

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 RHUI Manager, which can then generate an entitlement certificate and client configuration RPM. The RPM is then installed on the RHUA and each CDS instance, and future updates can be downloaded and installed using the `yum` command.

### Procedure 13.1. Updating Red Hat Update Infrastructure

1. Add the Red Hat Update Infrastructure repositories to the RHUA. Use the procedure in [Procedure 5.3, “Add a Red Hat Repository”](#) to install the following repositories:

```
Red Hat Update Infrastructure 2.0 (RPMs) (6Server-x86_64)
Red Hat Update Infrastructure 2.0 (RPMs) (6.0-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.1-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.1-x86_64)
Red Hat Update Infrastructure 2.0 (RPMs) (6Server-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.0-x86_64)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.1-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.0-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.0-x86_64)
Red Hat Update Infrastructure 2.0 (SRPMS) (6Server-x86_64)
Red Hat Update Infrastructure 2.0 (SRPMS) (6Server-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.1-x86_64)
```



#### NOTE

Using the *All in Certificate* method to add the repositories will add all these repositories at the same time. If you prefer to use the *By Product* method, add the product called **Red Hat Update Infrastructure 2.0 (RPMs)** and, optionally, **Red Hat Update Infrastructure 2.0 (SRPMS)**.

2. Check that the correct repositories have been installed using RHUI Manager:

```
-----
-----
rhui (repo) => l

Red Hat Repositories
Red Hat Update Infrastructure 2.0 (RPMs) (6Server-x86_64)
Red Hat Update Infrastructure 2.0 (RPMs) (6.0-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.1-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.1-x86_64)
Red Hat Update Infrastructure 2.0 (RPMs) (6Server-i386)
Red Hat Update Infrastructure 2.0 (RPMs) (6.0-x86_64)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.1-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.0-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.0-x86_64)
Red Hat Update Infrastructure 2.0 (SRPMS) (6Server-x86_64)
```

```
Red Hat Update Infrastructure 2.0 (SRPMS) (6Server-i386)
Red Hat Update Infrastructure 2.0 (SRPMS) (6.1-x86_64)
```

-----  
-----

3. Synchronize the repositories. Use the procedure in [Procedure 10.4, “Trigger a Repository Synchronization”](#).
4. Wait for the repository synchronization to complete, and then synchronize the CDS instances. Use the procedure in [Procedure 10.5, “Trigger a CDS Synchronization”](#).
5. Generate an entitlement certificate for the Red Hat Update Infrastructure repositories. Use the procedure in [Procedure 7.1, “Generate an Entitlement Certificate”](#).

**NOTE**

When you name the client configuration RPM, choose a name that will help you to identify that the RPM is to be used for providing updates to Red Hat Update Infrastructure, such as `rhui-update`.

6. Install the client configuration RPM on the RHUA and each CDS that requires updating:

```
$ rpm -Uvh /tmp/rhui/rhui-update.e16.noarch.rpm
```

7. Perform the update using `yum`. The client configuration RPM will configure a yum repository called `rhui-rhui-2.0`. Use the `yum update` command to update each instance. You will need to perform this command as the root user, or with appropriate `sudo` permissions:

```
# yum update
```

**NOTE**

Running `yum update` will pull updates from all enabled yum repositories. To pull updates from the `rhui-rhui-2.0` yum repository only, use the following command instead:

```
# yum --disablerepo=* --enablerepo=rhui-rhui-2.0 update
```

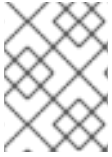
8. Restart the service to pick up any changes.

On the RHUA, restart the `pulp-server` service:

```
$ service pulp-server restart
```

On each CDS instance, restart the `pulp-cds` service:

```
$ service pulp-cds restart
```



**NOTE**

Once the Red Hat Update Infrastructure yum repositories have been configured on the RHUA and the CDS, only the final step [Step 8](#) is required to update those systems.

## APPENDIX A. REVISION HISTORY

<b>Revision 2-19.400</b> Rebuild with publican 4.0.0	<b>2013-10-31</b>	<b>Rüdiger Landmann</b>
<b>Revision 2-19</b> committed missing revision history	<b>Thurs Aug 09 2012</b>	<b>Julie Wu</b>
<b>Revision 2-18</b> added back customer portal images	<b>Wed Aug 08 2012</b>	<b>Julie Wu</b>
<b>Revision 2-17</b> /etc/pulp/client.conf changed to /etc/pulp/admin/admin.conf	<b>Wed May 23 2012</b>	<b>Julie Wu</b>
<b>Revision 2-16</b> BZ#752963: Installation updates BZ#752965: RHUI Installer updates	<b>Mon Jan 9 2012</b>	<b>Lana Brindley</b>
<b>Revision 2-15</b> BZ#752962: Introduction updates	<b>Wed Jan 4 2012</b>	<b>Lana Brindley</b>
<b>Revision 2-14</b> BZ#746798: Identity Certificate updates BZ#747113: RHUI Manager default password	<b>Tue Oct 25 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-13</b> BZ#746799 & BZ#746798: Identity Certificate updates, including new chapter.	<b>Mon Oct 24 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-12</b> Moved Updating chapter to correct location	<b>Fri Oct 14 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-11</b> Added James Slagle to author list	<b>Fri Oct 14 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-10</b> BZ#742347 - Typos BZ#743101 - Edit to instructions in Updating chapter BZ#745468 - Update ISO link and hardware req's in Install Req's chapter	<b>Thu Oct 13 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-9</b> BZ#743197 - Typos BZ#744022 - Update OS Requirements in Install Req's BZ#742347 - Update Answers File procedure BZ#743101 - Added new Updating chapter and populated	<b>Wed Oct 12 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-8</b> BZ#736427 - Changes to RHUI ISO download process	<b>Mon Oct 3 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-7</b> BZ#740859 - Changes to Adding a Custom Repository process	<b>Thu Sep 29 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-6</b> BZ#727048 & BZ#736427 - Updates to installation instructions	<b>Fri Sep 23 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-5</b> BZ#727048 - Updates to installation instructions	<b>Thu Sep 22 2011</b>	<b>Lana Brindley</b>

<b>Revision 2-4</b> BZ#726765 - Updated link to ISO in Installation Req's	<b>Wed Aug 31 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-3</b> BZ#726765 - Updated link to ISO in Installation Req's	<b>Tue Aug 16 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-2</b> BZ#726765 - Added link to ISO in Installation Req's	<b>Tue Aug 2 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-1</b> BZ#726420 - QE Review	<b>Fri Jul 28 2011</b>	<b>Lana Brindley</b>
<b>Revision 2-0</b> Preparation for publication	<b>Thu Jul 27 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-25</b> BZ#725771 - QE Review BZ#726154 - QE Review	<b>Thu Jul 27 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-24</b> BZ#725771 - QE Review	<b>Wed Jul 27 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-23</b> BZ#720019 - QE Review	<b>Tue Jul 26 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-22</b> BZ#722584 - QE Review	<b>Wed Jul 20 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-21</b> BZ#700607 - QE Review BZ#707954 - QE Review BZ#713138 - QE Review BZ#718638 - QE Review BZ#720845 - QE Review BZ#722518 - QE Review	<b>Tue Jul 19 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-20</b> Fixing build error	<b>Mon Jul 18 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-19</b> Feedback from technical review BZ#719205 - QE Review BZ#719471 - QE Review BZ#719473 - QE Review BZ#719475 - QE Review BZ#719960 - QE Review BZ#720019 - QE Review BZ#720842 - QE Review BZ#720843 - QE Review BZ#720844 - QE Review	<b>Mon Jul 18 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-18</b>	<b>Wed Jul 6 2011</b>	<b>Lana Brindley</b>

BZ#718634 - QE Review BZ#718638 - QE Review BZ#718640 - QE Review BZ#718691 - QE Review BZ#718905 - QE Review BZ#718969 - QE Review		
<b>Revision 1-17</b> Feedback from technical review	<b>Mon Jul 4 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-16</b> Feedback from technical review	<b>Fri Jul 1 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-15</b> BZ#706045 - Monitoring BZ#707764 - RHUI Installer BZ#713138 - Content Certificates	<b>Mon Jun 27 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-14</b> BZ#705137 & BZ#715099 - Status and Scheduling BZ#711431 - Client Entitlements and CDS BZ#712231 - CDS BZ#713921 - Client Entitlements	<b>Thu Jun 23 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-13</b> BZ#707764 - Installation Requirements BZ#707954 - Installation Requirements BZ#709872 - Installation	<b>Wed Jun 15 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-12</b> BZ#704633 - QE review	<b>Fri May 27 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-11</b> Structure changes BZ#706045 - QE review	<b>Thu May 26 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-10</b> BZ#695559 - QE review BZ#695704 - QE review BZ#696403 - QE review BZ#703138 - QE review	<b>Wed May 25 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-9</b> BZ#704583 - Technical review BZ#704587 - Technical review BZ#704611 - Technical review BZ#704612 - Technical review BZ#704633 - Technical review BZ#705122 - Technical review BZ#705125 - Technical review BZ#705137 - Technical review BZ#705140 - Technical review BZ#705733 - Technical review BZ#706045 - Technical review	<b>Tue May 24 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-8</b>	<b>Mon May 9 2011</b>	<b>Lana Brindley</b>

Prepared for technical review

<b>Revision 1-7</b> BZ#700607- RHUI Installer: Overview BZ#700609- RHUI Installer: Answers File	<b>Fri May 6 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-6</b> BZ#697214- RHUI Manager Sync status and schedule screen BZ#696403- RHUI Manager Red Hat Entitlement Certificates BZ#696399- RHUI Manager User Screen	<b>Thu May 5 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-6</b> BZ#697214- RHUI Manager Sync status and schedule screen BZ#696403- RHUI Manager Red Hat Entitlement Certificates	<b>Thu May 5 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-5</b> BZ#696406- RHUI Manager Client Entitlements Screen	<b>Wed May 4 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-4</b> BZ#697205- RHUI Manager CDS Screen BZ#697213- RHUI Manager CDS Repository Screen	<b>Wed May 4 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-3</b> BZ#696830- RHUI Manager Repositories	<b>Tue May 3 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-2</b> BZ#695559 - RHUI Manager Concepts BZ#695704 - RHUI Manager First Launch BZ#696398 - RHUI Manager Home Screen BZ#697215 - RHUI Manager CLI	<b>Tue May 3 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-1</b> Preparing for 2.0 updates	<b>Thu April 21 2011</b>	<b>Lana Brindley</b>
<b>Revision 1-0</b> Passed QE review and prepared for publication	<b>Thu Dec 9 2010</b>	<b>Lana Brindley</b>
<b>Revision 0-13</b> BZ#660207 - Installation Requirements	<b>Thu Dec 9 2010</b>	<b>Lana Brindley</b>
<b>Revision 0-12</b> BZ#660207 - Installation Requirements	<b>Thu Dec 9 2010</b>	<b>Lana Brindley</b>
<b>Revision 0-11</b> BZ#660207 - Installation Requirements	<b>Thu Dec 9 2010</b>	<b>Lana Brindley</b>
<b>Revision 0-10</b> BZ#661114 - Operating States BZ#660654 - Entitlement Certificates	<b>Wed Dec 8 2010</b>	<b>Lana Brindley</b>
<b>Revision 0-9</b>	<b>Wed Dec 8 2010</b>	<b>Lana Brindley</b>



BZ#660184 - We Need Feedback		
BZ#661155 - Typos found by QE		
BZ#661166 - Comments made by QE		
BZ#649728 - Introduction		
BZ#649748 - Requirements		
BZ#649778 - Installation		
BZ#649783 - Answers File		
<b>Revision 0-8</b>	<b>Mon Dec 6 2010</b>	<b>Lana Brindley</b>
Results of technical review		
BZ#659082 - Client Instances and Answers File		
<b>Revision 0-7</b>	<b>Thu Dec 2 2010</b>	<b>Lana Brindley</b>
Removed out of date image from Introduction		
<b>Revision 0-6</b>	<b>Tue Nov 30 2010</b>	<b>Lana Brindley</b>
BZ#649723 - Introduction (Images)		
BZ#651530 - Monitoring		
BZ#656499 - RHUA Product Config		
BZ#656925 - Introduction (GPG Key info)		
<b>Revision 0-5</b>	<b>Tue Nov 22 2010</b>	<b>Lana Brindley</b>
BZ#651129 - Client Instances		
BZ#651518 - External Load Balancer		
BZ#649783 - Answers file		
BZ#651538 - Operation		
BZ#651530 - Monitoring		
Added preambles to parts		
<b>Revision 0-4</b>	<b>Mon Nov 22 2010</b>	<b>Lana Brindley</b>
BZ#649847 - Entitlement Certificates		
BZ#655127 - Entitlement Certificates		
BZ#651111 - CDS		
BZ#651052 - RHUA		
BZ#651129 - Client Instances		
<b>Revision 0-3</b>	<b>Thu Nov 18 2010</b>	<b>Lana Brindley</b>
BZ#651052 - RHUA		
Further edits to RHUA		
<b>Revision 0-2</b>	<b>Wed Nov 17 2010</b>	<b>Lana Brindley</b>
Adjusted chunking depth		
Made Revision History visible		
Some rearranging of chapters		
BZ#649778 - Installation		
BZ#651542 - Installation		
Further edits to Installation		
BZ#634586 - Installation Requirements		
Further edits to Installation Requirements		
BZ#649847 - Entitlement Certificates		
Further edits to Entitlement Certificates		
BZ#651039 - Identity Certificates		
<b>Revision 0-1</b>	<b>Tue Nov 16 2010</b>	<b>Lana Brindley</b>

Added DRAFT watermark  
Adjusted chunking depth  
BZ#649728 - Introduction  
BZ#651572 - Introduction  
Further edits to Introduction  
BZ#649748 - Installation Requirements  
Further edits to Installation Requirements

**Revision 0-0**

**Mon Nov 15 2010**

**Lana Brindley**

Renamed and restructured from 1.1 Deployment Guide

---

# INDEX

## C

CDS (see [RHUI Manager](#), [Content Distribution Server](#))

### Certificates

X.509, [Certificates](#)

## I

### installation

hardware, [Installation Prerequisites](#)

qpid SSL, [Setting up SSL](#)

SSL, [Setting up SSL](#)

storage, [Installation Prerequisites](#)

## L

log files, [Monitoring](#)

## M

monitoring, [Monitoring](#)

log files, [Monitoring](#)

## R

### Red Hat Update Appliance

architecture, [Architecture](#)

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

communications, [Communications](#)

monitoring, [Monitoring](#)

requirements, [Installation Requirements](#)

updating, [Updating Red Hat Update Infrastructure](#)

requirements, [Installation Requirements](#)

cloud provider, [Installation Prerequisites](#)

firewall, [Installation Prerequisites](#)

network, [Installation Prerequisites](#)

### RHUI Installer

answers file, [Answers File](#)

configuration, [Answers File](#)

overview, [RHUI Installer](#)

RHUI Manager, [RHUI Manager](#)

add a CDS instance, [Content Distribution Server \(CDS\) Instances](#)  
add a Red Hat repository, [Repositories](#)  
change user password, [Users](#)  
content distribution server, [Content Distribution Server \(CDS\) Instances](#)  
create client configuration RPM, [Client Entitlements](#)  
create configuration RPMs, [Client Entitlements](#)  
create custom repository, [Custom Repositories](#)  
custom repositories, [Custom Repositories](#)  
delete a CDS instance, [Content Distribution Server \(CDS\) Instances](#)  
delete a Red Hat repository, [Repositories](#)  
display repository information, [Repositories](#)  
entitlement certificates, [Client Entitlements](#), [Managing Entitlement Certificates](#)  
exiting, [Using RHUI Manager](#)  
first launch, [RHUI Manager First Launch](#)  
generate entitlement certificate, [Client Entitlements](#)  
identity certificates, [Identity Certificates](#)  
list CDS instances, [Content Distribution Server \(CDS\) Instances](#)  
list CDS synchronization status, [Status and Scheduling](#)  
list certificate information, [Managing Entitlement Certificates](#)  
list custom repository entitlements, [Managing Entitlement Certificates](#)  
list packages in a repository, [Repositories](#)  
list repositories, [Repositories](#)  
list repository synchronization status, [Status and Scheduling](#)  
logging out, [Using RHUI Manager](#)  
navigation, [Using RHUI Manager](#)  
operation, [Using RHUI Manager](#)  
repositories, [Repositories](#)  
screens, [Using RHUI Manager](#)  
shell prompt, [Using RHUI Manager from the Shell Prompt](#)  
shell prompt cert command, [Using RHUI Manager from the Shell Prompt](#)  
shell prompt flags, [Using RHUI Manager from the Shell Prompt](#)  
shell prompt packages command, [Using RHUI Manager from the Shell Prompt](#)  
shell prompt repo command, [Using RHUI Manager from the Shell Prompt](#)  
shell prompt status command, [Using RHUI Manager from the Shell Prompt](#)  
starting, [Using RHUI Manager](#)  
status and scheduling, [Status and Scheduling](#)  
trigger CDS synchronization, [Status and Scheduling](#)  
trigger repository synchronization, [Status and Scheduling](#)  
upload content certificate, [Managing Entitlement Certificates](#)  
upload packages to a custom repository, [Custom Repositories](#)  
users, [Users](#)  
view last synchronization details, [Status and Scheduling](#)

