Setting up and revising Red Hat Update Infrastructure 4
Abstract

This guide describes how to configure and manage Red Hat Update Infrastructure 4 (RHUI 4).
# Table of Contents

**MAKING OPEN SOURCE MORE INCLUSIVE** .................................................. 4

**CHAPTER 1. ABOUT RED HAT UPDATE INFRASTRUCTURE** .................... 5

1.1. INSTALLATION OPTIONS ................................................................. 5
   1.1.1. Option 1: Full installation ...................................................... 6
   1.1.2. Option 2: Installation with an existing storage solution .......... 6
   1.1.3. Option 3: Installation with an existing load-balancer solution .. 6
   1.1.4. Option 4: Installation with existing storage and load-balancer solutions .. 7

1.2. RHUI 4 COMPONENTS ................................................................. 8
   1.2.1. Red Hat Update Appliance ....................................................... 8
   1.2.2. Content delivery server ......................................................... 8
   1.2.3. HAPProxy load-balancer ......................................................... 10
   1.2.4. Repositories and content ....................................................... 12

1.3. CONTENT PROVIDER TYPES .......................................................... 12
1.4. COMPONENT COMMUNICATIONS ..................................................... 12
1.5. CHANGING THE ADMIN PASSWORD ............................................... 13
1.6. ADDITIONAL RESOURCES ............................................................. 14

**CHAPTER 2. MANAGING REPOSITORIES** ........................................... 15

2.1. AVAILABLE CHANNELS ............................................................... 15
2.2. LISTING REPOSITORIES CURRENTLY MANAGED BY RHUI 4 .......... 15
2.3. DISPLAYING DETAILED INFORMATION ON A REPOSITORY .......... 16
2.4. ADDING A NEW RED HAT CONTENT REPOSITORY ......................... 17
2.5. CREATING A NEW CUSTOM REPOSITORY (RPM CONTENT ONLY) .... 19
2.6. DELETING A REPOSITORY FROM RHUI 4 ..................................... 21
2.7. UPLOADING CONTENT TO A CUSTOM REPOSITORY (RPM CONTENT ONLY) ......................................................... 21
2.8. UPLOADING CONTENT FROM A REMOTE WEB SITE (RPM CONTENT ONLY) ................................................................. 22
2.9. LISTING THE PACKAGES IN A REPOSITORY (RPM CONTENT ONLY) .. 23

**CHAPTER 3. CREATING AN ENTITLEMENT CERTIFICATE AND A CLIENT CONFIGURATION RPM** .................................................. 25

3.1. CREATING A CLIENT ENTITLEMENT CERTIFICATE WITH THE RED HAT UPDATE INFRASTRUCTURE MANAGEMENT TOOL .................. 25
3.2. CREATING A CLIENT ENTITLEMENT CERTIFICATE WITH THE CLI .... 26
3.3. CREATING A CLIENT CONFIGURATION RPM WITH THE RED HAT UPDATE INFRASTRUCTURE MANAGEMENT TOOL .................. 27
3.4. CREATING A CLIENT CONFIGURATION RPM WITH THE CLI ........... 27

**CHAPTER 4. MANAGING RED HAT ENTITLEMENT CERTIFICATES** .......... 29

4.1. RED HAT UPDATE APPLIANCE CERTIFICATES ............................ 29
4.2. CONTENT DELIVERY SERVER CERTIFICATES .................................. 29
4.3. CLIENT CERTIFICATES ............................................................... 29
   4.3.1. Listing the entitled products for a certificate ......................... 30
   4.3.2. Listing custom repository entitlements ................................. 30

**CHAPTER 5. CHECKING SYNCHRONIZATION STATUS AND SCHEDULING** .................. 32

5.1. DISPLAYING REPOSITORY SYNCHRONIZATION SUMMARY .............. 32
5.2. DISPLAYING RUNNING SYNCHRONIZATIONS .................................. 32
5.3. VIEWING THE DETAILS OF THE LAST REPOSITORY SYNCHRONIZATION ................................................................. 33
5.4. SYNCHRONIZING AN INDIVIDUAL REPOSITORY IMMEDIATELY ........ 33
5.5. CANCELING ACTIVE SYNCHRONIZATION TASKS ......................... 34
5.6. CANCELING WAITING SYNCHRONIZATION TASKS ......................... 35
5.7. VIEWING AND CHANGING A REPOSITORY AUTO-PUBLISH STATUS .... 36
5.8. VIEWING AND ADVANCING REPOSITORY WORKFLOW .................... 37
5.9. EXPORTING A REPOSITORY TO THE FILE SYSTEM

CHAPTER 6. MANAGING CONTENT DELIVERY SERVERS ........................................... 39
  6.1. LISTING ALL KNOWN CDS INSTANCES MANAGED BY RHUI 4 39
  6.2. REGISTERING A NEW CDS 39
  6.3. REINSTALLING AND REAPPLYING CONFIGURATION TO A CDS 41
  6.4. CONFIGURING A CDS TO ACCEPT LEGACY CAS 42
  6.5. CONFIGURING A CDS TO STOP ACCEPTING LEGACY CAS 42
  6.6. UNREGISTERING A CDS 43

CHAPTER 7. MANAGING AN HAPROXY LOAD-BALANCER INSTANCE ......................... 44
  7.1. LISTING ALL KNOWN HAPROXY LOAD-BALANCER INSTANCES MANAGED BY RHUI 4 44
  7.2. REGISTERING A NEW HAPROXY LOAD-BALANCER 44
  7.3. REINSTALLING AND REAPPLYING THE CONFIGURATION TO AN HAPROXY LOAD-BALANCER 45
  7.4. UNREGISTERING AN HAPROXY LOAD-BALANCER 46

CHAPTER 8. CONFIGURATION FILES, STATUS CODES, AND LOG FILES ........................ 48

CHAPTER 9. WORKING WITH RHUI 4 COMMANDS ............................................. 50
  9.1. USING RHUI 4 MENU OPTIONS 50
  9.2. USING RHUI 4 CLI OPTIONS 53
    9.2.1. cert 53
    9.2.2. packages 54
    9.2.3. repo 54
    9.2.4. cds 55
    9.2.5. migrate 56
    9.2.6. haproxy 56
    9.2.7. status 57
    9.2.8. client 57

CHAPTER 10. CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION WORKFLOW ...... 58
  10.1. ADDITIONAL RESOURCES 58

CHAPTER 11. RESOLVING COMMON PROBLEMS IN RHUI 4 .................................... 59
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
CHAPTER 1. ABOUT RED HAT UPDATE INFRASTRUCTURE 4

Red Hat Update Infrastructure 4 (Red Hat Update Infrastructure 4) is a highly scalable, highly redundant framework that enables you to manage repositories and content. It also enables cloud providers to deliver content and updates to Red Hat Enterprise Linux (RHEL) instances. Based on the upstream Pulp project, RHUI allows cloud providers to locally mirror Red Hat-hosted repository content, create custom repositories with their own content, and make those repositories available to a large group of end users through a load-balanced content delivery system.

As a system administrator, you can prepare your infrastructure for participation in the Red Hat Certified Cloud and Service Provider program by installing and configuring the Red Hat Update Appliance (RHUA), content delivery servers (CDS), repositories, shared storage, and load balancing.

Configuring RHUI comprises the following tasks:

- Creating and synchronizing a Red Hat repository
- Creating client entitlement certificates and client configuration RPMs
- Creating client profiles for the RHUI servers

Experienced RHEL system administrators are the target audience. System administrators with limited RHEL skills should consider engaging Red Hat Consulting to provide a Red Hat Certified Cloud Provider Architecture Service.

Learn about configuring, managing, and updating RHUI with the following topics:

- the RHUI components
- content provider types
- the command line interface (CLI) used to manage the components
- utility commands
- certificate management
- content management

1.1. INSTALLATION OPTIONS

The following table presents the various Red Hat Update Infrastructure 4 components.

Table 1.1. Red Hat Update Infrastructure components and functions

<table>
<thead>
<tr>
<th>Component</th>
<th>Acronym</th>
<th>Function</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Update Appliance</td>
<td>RHUA</td>
<td>Downloads new packages from the Red Hat content delivery network and copies new packages to each CDS node</td>
<td>None</td>
</tr>
<tr>
<td>Component</td>
<td>Acronym</td>
<td>Function</td>
<td>Alternative</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Content Delivery Server</td>
<td>CDS</td>
<td>Provides the <strong>yum</strong> repositories that clients connect to for the updated packages</td>
<td>None</td>
</tr>
<tr>
<td>HAProxy</td>
<td>None</td>
<td>Provides load balancing across CDS nodes</td>
<td>Existing load balancing solution</td>
</tr>
<tr>
<td>Shared storage</td>
<td>None</td>
<td>Provides shared storage</td>
<td>Existing storage solution</td>
</tr>
</tbody>
</table>

The following table describes how to perform installation tasks.

**Table 1.2. Red Hat Update Infrastructure installation tasks**

<table>
<thead>
<tr>
<th>Installation Task</th>
<th>Performed on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install RHEL 8</td>
<td>RHUA, CDS, and HAProxy</td>
</tr>
<tr>
<td>Subscribe the system</td>
<td>RHUA, CDS, and HAProxy</td>
</tr>
<tr>
<td>Attach a RHUI subscription</td>
<td>RHUA, CDS, and HAProxy</td>
</tr>
<tr>
<td>Apply updates</td>
<td>RHUA, CDS and HAProxy</td>
</tr>
<tr>
<td>Install <strong>rhui-installer</strong></td>
<td>RHUA</td>
</tr>
<tr>
<td>Run <strong>rhui-installer</strong></td>
<td>RHUA</td>
</tr>
</tbody>
</table>

**1.1.1. Option 1: Full installation**

- A RHUA
- Two or more CDS nodes with shared storage
- One or more HAProxy load-balancers

**1.1.2. Option 2: Installation with an existing storage solution**

- A RHUA
- Two or more CDS nodes with an existing storage solution
- One or more HAProxy load-balancers

**1.1.3. Option 3: Installation with an existing load-balancer solution**

- A RHUA
1.1.4. Option 4: Installation with existing storage and load-balancer solutions

- A RHUA
- Two or more CDS nodes with existing shared storage
- An existing load-balancer

The following figure depicts a high-level view of how the various Red Hat Update Infrastructure 4 components interact.

Figure 1.1. Red Hat Update Infrastructure 4 overview

NOTE

You need to subscribe the RHUA as --type rhui and have a Red Hat Certified Cloud and Service Provider subscription to install RHUI. You also need an appropriate content certificate.
Install the RHUA and CDS nodes on separate x86_64 servers (bare metal or virtual machines). Ensure all the servers and networks that connect to RHUI can access the Red Hat Subscription Management service.

1.2. RHUI 4 COMPONENTS

Understanding how each RHUI component interacts with other components will make your job as a system administrator a little easier.

1.2.1. Red Hat Update Appliance

There is one RHUA per RHUI installation, though in many cloud environments there will be one RHUI installation per region or data center, for example, Amazon’s EC2 cloud comprises several regions. In every region, there is a separate RHUI set up with its own RHUA node.

The RHUA allows you to perform the following tasks:

- Download new packages from the Red Hat content delivery network (CDN). The RHUA is the only RHUI component that connects to Red Hat, and you can configure the synchronization schedule for the RHUA.

- Copy new packages to the shared network storage.

- Verify the RHUI installation’s health and write the results to a file located on the RHUA. Monitoring solutions use this file to determine the RHUI installation’s health.

- Provide a human-readable view of the RHUI installation’s health through a CLI tool.

RHUI uses two main configuration files: /etc/rhui/rhui-tools.conf and /etc/rhui/rhui-subscription-sync.conf.

The /etc/rhui/rhui-tools.conf configuration file contains general options used by the RHUA, such as the default file locations for certificates, and default configuration parameters for the Red Hat CDN synchronization. This file normally does not require editing.

The Red Hat Update Infrastructure Management Tool generates the /etc/rhui/rhui-subscription-sync.conf configuration file based on user-inputted values. It contains all the information that drives the running of a RHUA in a particular region. An example configuration includes the destination on the RHUA to download packages.

The RHUA employs several services to synchronize, organize, and distribute content for easy delivery.

RHUA services

Pulp

The service that oversees management of the supporting services, providing a user interface for users to interact with

PostgreSQL

A PostgreSQL database used to keep track of currently synchronized repositories, packages, and other crucial metadata.

1.2.2. Content delivery server
The CDS nodes provide the repositories that clients connect to for the updated content. There can be as few as one CDS. Because RHUI provides a load-balancer with failover capabilities, we recommended that you use multiple CDS nodes.

The CDS nodes host content to end-user RHEL systems. While there is no required number of systems, the CDS works in a round-robin style load-balanced fashion (A, B, C, A, B, C) to deliver content to end-user systems. The CDS uses HTTP to host content to end-user systems via httpd-based yum repositories.

During configuration, you specify the CDS directory where packages are synchronized. Similar to the RHUA, the only requirement is that you mount the directory on the CDS. It is up to the cloud provider to determine the best course of action when allocating the necessary devices. The Red Hat Update Infrastructure Management Tool configuration RPM linked the package directory with the NGINX configuration to serve it.

Currently, RHUI supports the following shared storage solutions:

**NFS**
If NFS is used, rhui-installer can configure an NFS share on the RHUA to store the content as well as a directory on the CDS nodes to mount the NFS share. The following rhui-installer options control these settings:

- `--remote-fs-mountpoint` is the file system location where the remote file system share should be mounted (default: /var/lib/rhui/remote_share)
- `--remote-fs-server` is the remote mount point for a shared file system to use, for example, nfs.example.com:/path/to/share (default: nfs.example.com:/export)

**CephFS**
If using CephFS, you must configure CephFS separately and then use it with RHUI as a mount point. The following rhui-installer options control these settings:

- `--remote-fs-server` is the remote mount point for a shared file system to use, for example, ceph.example.com:/path/to/share (default: ceph.example.com:/export)

**NOTE**
This document does not provide instructions to set up or configure Ceph shared file storage. For any Ceph related tasks, consult your system administrator, or see the Ceph documentation.

If these default values are used, the /export directory on the RHUA and the /var/lib/rhui/remote_share directory on each CDS are identical.

The expected usage is that you use one shared network file system on the RHUA and all CDS nodes, for example, NFS. It is possible the cloud provider will use some form of shared storage that the RHUA writes packages to and each CDS reads from.
NOTE

The storage solution must provide an NFS or CephFS endpoint for mounting on the RHUA and CDS nodes. If local storage is implemented, shared storage is needed for the cluster to work. If you want to provide local storage to the RHUA, configure the RHUA to function as the NFS server with a `rhua.example.com:/path/to/nfs/share` endpoint configured.

Do not set up Ceph shared file storage on any of the RHUI nodes. You must configure CephFS on independent dedicated machines.

The only nonstandard logic that takes place on each CDS is the entitlement certificate checking. This checking ensures that the client making requests on the `yum` repositories is authorized by the cloud provider to access those repositories. The check ensures the following conditions:

- The entitlement certificate was signed by the cloud provider’s Certificate Authority (CA) Certificate. The CA Certificate is installed on the CDS as part of its configuration to facilitate this verification.
- The requested URI matches an entitlement found in the client’s entitlement certificate.

If the CA verification fails, the client sees an SSL error. See the CDS node’s NGINX logs under `/var/log/nginx/` for more information.

```
[root@cds01 ~]# ls -1 /var/log/nginx/
access.log
error.log
gunicorn-auth.log
gunicorn-content_manager.log
gunicorn-mirror.log
ssl-access.log----
```

IMPORTANT

The NGINX configuration is handled through the `/etc/nginx/conf.d/ssl.conf` file during the CDS installation.

If multiple clients experience problems updating against a repository, this may indicate a problem with the RHUI. See `Yum generates 'Errno 14 HTTP Error 401: Authorization Required' while accessing RHUI CDS` for more details.

1.2.3. HAProxy load-balancer

If more than one CDS is used, a load-balancing solution must be in place to spread client HTTPS requests across all servers. RHUI ships with HAProxy, but it is up to you to choose what load-balancing solution (for example, the one from the cloud provider) to use during the installation. If HAProxy is used, you must also decide how many nodes to bring in.

Clients are not configured to go directly to a CDS; their repository files are configured to point to HAProxy, the RHUI load-balancer. HAProxy is a TCP/HTTP reverse proxy particularly suited for high-availability environments. HAProxy performs the following tasks:

- Routes HTTP requests depending on statically assigned cookies
Spreads the load among several servers while assuring server persistence through the use of HTTP cookies

Switches to backup servers in the event a main server fails

Accepts connections to special ports dedicated to service monitoring

Stops accepting connections without breaking existing ones

Adds, modifies, and deletes HTTP headers in both directions

Blocks requests matching particular patterns

Persists client connections to the correct application server, depending on application cookies

Reports detailed status as HTML pages to authenticated users from a URI intercepted from the application

NOTE
If you use an existing load-balancer, ensure port 443 is configured in the load-balancer for the cds-lb-hostname forwarded to the pool and that all CDSs in the cluster are in the load-balancer’s pool.

The exact configuration depends on the particular load-balancer software you use. See the following configuration, taken from a typical HAProxy setup, to understand how you should configure your load-balancer:

```
[root@rhui4proxy ~]# cat /etc/haproxy/haproxy.cfg
# This file managed by Puppet
global
  chroot /var/lib/haproxy
daemon
group haproxy
  log 10.10.153.149 local0
  maxconn 4000
  pidfile /run/haproxy.pid
  stats socket /var/lib/haproxy/stats
  user haproxy

defaults
  log global
  maxconn 8000
  option redispatch
  retries 3
  stats enable
  timeout http-request 10s
  timeout queue 1m
  timeout connect 10s
  timeout client 1m
  timeout server 1m
  timeout check 10s

listen https00
  bind 10.10.153.149:443
  balance roundrobin
```
option tcplog
tcp-check
server cds01.example.com cds01.example.com:443 check
server cds02.example.com cds02.example.com:443 check

Keep in mind that when clients fail to connect, it is important to review the nginx logs on the CDS under /var/log/nginx/ to ensure that any request reached the CDS. If requests do not reach the CDS, issues such as DNS or general network connectivity may be at fault.

1.2.4. Repositories and content

A repository is a storage location for software packages (RPMs). RHEL uses yum commands to search a repository, download, install, and configure the RPMs. The RPMs contain all the dependencies needed to run an application. RPMs also download updates for software in your repositories.

RHEL uses core technologies such as control groups (cgroups) for resource management, namespaces for process isolation, and SELinux for security, enabling secure multiple tenancy, and reducing the potential for security exploits. These technologies enable rapid application deployment, simpler testing, maintenance, and troubleshooting while improving security.

Content, as it relates to RHUI, is the software (such as RPMs) that you download from the Red Hat CDN for use on the RHUA and the CDS nodes. The RPMs provide the files necessary to run specific applications and tools. Clients are granted access by a set of SSL content certificates and keys provided by an rpm package, which also provides a set of generated yum repository files.

Additional resources

- What Channels Can Be Delivered at Red Hat’s Certified Certified Cloud & Service Provider (CCSP) Partners?

1.3. CONTENT PROVIDER TYPES

There are three types of cloud computing environments:

- public cloud
- private cloud
- hybrid cloud

This guide focuses on public and private clouds. We assume the audience understands the implications of using public, private, and hybrid clouds.

1.4. COMPONENT COMMUNICATIONS

All RHUI components use the HTTPS communication protocol over port 443.

Table 1.3. Red Hat Update Infrastructure communication protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Update Appliance</td>
<td>Red Hat Content Delivery Network</td>
<td>HTTPS</td>
<td>Downloads packages from Red Hat</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Protocol</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Load-Balancer</td>
<td>Content Delivery Server</td>
<td>HTTPS</td>
<td>Forwards the client’s yum</td>
</tr>
<tr>
<td>Client</td>
<td>Load-Balancer</td>
<td>HTTPS</td>
<td>Used by yum on the client to download packages from a CDS</td>
</tr>
<tr>
<td>Content Delivery Server</td>
<td>Red Hat Update Appliance</td>
<td>HTTPS</td>
<td>Might request information from Pulp API about content</td>
</tr>
</tbody>
</table>

RHUI nodes require the following network access to communicate with each other.

**NOTE**

Make sure that the network port is open and that network access is restricted to only those nodes that you plan to use.

Table 1.4. Red Hat Update Infrastructure network access

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHUA</td>
<td>443</td>
<td>RHUA, CDS01, CDS02, ... CDSn</td>
</tr>
<tr>
<td>HAProxy</td>
<td>443</td>
<td>Client virtual machines</td>
</tr>
</tbody>
</table>

1.5. CHANGING THE ADMIN PASSWORD

The `rhui-installer` sets the initial RHUI login password. It is also written in the `/etc/rhui/rhui-subscription-sync.conf` file. You can override the initial password with the `--rhui-manager-password` option.

If you want to change the initial password later, you can change it through the `rhui-manager` tool or through `rhui-installer`. Run the `rhui-installer --help` command to see the full list of `rhui-installer` options.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press `u` to select manage RHUI users.

3. From the User Manager screen, press `p` to select change admin's password (followed by logout):

   ```
   -= User Manager =-
   ```
p  change admin’s password (followed by logout)

rhui (users) => p

Warning: After password change you will be logged out.
Use ctrl-c to cancel password change.
New Password:

4. Enter your new password; reenter it to confirm the change.

New Password: 
Re-enter Password:

[localhost] env PULP_SETTINGS=/etc/pulp/settings.py /usr/bin/pulpcore-manager reset-
admin-password -p ********

Verification

1. The following message displays after you change the admin password:

Password successfully updated. For security reasons you have been logged out.
[root@ip-10-141-150-145 ~]#

1.6. ADDITIONAL RESOURCES

- Red Hat Cloud Access Reference Guide
- Red Hat Enterprise Linux 8
- Managing storage devices
- HAProxy
- Pulp project
2.1. AVAILABLE CHANNELS

Certified Cloud and Service Provider (CCSP) partners control what channels and packages are delivered through their service. See Red Hat Enterprise Linux repositories that can be delivered through Red Hat’s Certified Cloud and Service Provider (CCSP) partners via RHUI for the most current information regarding what channels are available for the various operating system versions.

The repositories available for use with RHEL 8 are as follows:

- Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (RPMs)
- Red Hat Enterprise Linux 8 for x86_64 - BaseOS from RHUI (RPMs)
- Red Hat Enterprise Linux 8 for x86_64 - High Availability (RPMs) from RHUI
- Red Hat Enterprise Linux 8 for x86_64 - Resilient Storage (RPMs) from RHUI
- Red Hat Enterprise Linux 8 for x86_64 - Supplementary (RPMs) from RHUI
- Red Hat CodeReady Linux Builder for RHEL 8 x86_64 (RPMs) from RHUI

Contact your CCSP if a required channel is missing.

Additional resources

- Red Hat Ecosystem Catalog

2.2. LISTING REPOSITORIES CURRENTLY MANAGED BY RHUI 4

A repository is a server node that contains downloadable software for a Linux distribution. You use **yum** to search for, install, and control RPMs from the repository to your RHUA and CDS nodes.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press **r** to select **manage repositories**.

3. From the **Repository Management** screen, press **l** to select **list repositories currently managed by the RHUI**:  

   ```
   ...  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.0)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.1)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.2)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.3)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)  
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8)  
   ```
2.3. DISPLAYING DETAILED INFORMATION ON A REPOSITORY

You can use the Repository Management screen to display information about a particular repository.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press r to select manage repositories.

3. From the Repository Management screen, press i:

   Enter value (1-1631) to toggle selection, ‘c’ to confirm selections, or ‘?’ for more commands:

4. Select the repository by entering the value beside the repository name. Enter one repository selection at a time before confirming your product selection.

5. Press c to confirm:

   Name: Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Debug RPMs) from RHUI (8.4)
   ID: rhel-8-for-aarch64-appstream-debug-rhui-rpms-8.4
   Type: Red Hat
   Version: 0
   Relative Path: content/dist/rhel8/rhui/8.4/aarch64/appstream/debug
   GPG Check: Yes
   Custom GPG Keys: (None)
   Red Hat GPG Key: Yes
   Content Unit Count: 
   Last Sync: 2021-11-15 15:56:06
   Next Sync: 2021-11-15 22:00:00

   Name: Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)
   ID: rhel-8-for-aarch64-appstream-rhui-rpms-8.4
   Type: Red Hat
   Version: 0
   Relative Path: content/dist/rhel8/rhui/8.4/aarch64/appstream/os
CHAPTER 2. MANAGING REPOSITORIES

GPG Check: Yes
Custom GPG Keys: (None)
Red Hat GPG Key: Yes
Content Unit Count:
Last Sync: 2021-11-15 19:50:20
Next Sync: 2021-11-16 01:55:00

Name: Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8.4)
ID: rhel-8-for-aarch64-appstream-source-rhui-rpms-8.4
Type: Red Hat
Version: 0
Relative Path: content/dist/rhel8/rhui/8.4/aarch64/appstream/source/SRPMS
GPG Check: Yes
Custom GPG Keys: (None)
Red Hat GPG Key: Yes
Content Unit Count:
Last Sync: 2021-11-15 15:56:51
Next Sync: 2021-11-15 22:00:00

Verification

1. A similar output displays for your selections.

2.4. ADDING A NEW RED HAT CONTENT REPOSITORY

Based on the upstream Pulp project, RHUI allows cloud providers to locally mirror Red Hat-hosted repository content, create custom repositories with their own content, and make those repositories available to end users through a load-balanced content delivery system.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press r to select manage repositories.

3. From the Repository Management screen, press a to select add a new Red Hat content repository.

4. Wait for the Red Hat Update Infrastructure Management Tool to determine the entitled repositories. This might take several minutes:

   rhui (repo) => a

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

5. The Red Hat Update Infrastructure Management Tool prompts for a selection method:
6. Press 2 to select the **By Product** method.

7. Select which repositories to add by typing the number of the repository at the prompt. You can also choose the range of repositories, for instance, by entering 1 - 5.

8. Continue until all repositories you want to add are checked.

9. Press c when you are finished selecting the repositories. The Red Hat Update Infrastructure Management Tool displays the repositories for deployment and prompts for confirmation:

   The following products will be deployed:
   - Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI
   - Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI
   Proceed? (y/n)

10. Press y to proceed. A message indicates each successful deployment:

    Importing Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8.4)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8.3)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8.2)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8.1)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8.0)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8)...
    Importing Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8.4)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8.3)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8.2)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8.1)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8.0)...
    Importing product repository Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI (8)...

    Content will not be downloaded to the newly imported repositories until the next sync is run.
Verification

1. From the **Repository Management** screen, press **l** to check that the correct repositories have been installed.

Additional resources

- Red Hat Enterprise Linux repositories that can be delivered through Red Hat’s Certified Cloud and Service Provider (CCSP) partners via RHUI

2.5. CREATING A NEW CUSTOM REPOSITORY (RPM CONTENT ONLY)

You can create custom repositories that can be used to distribute updated client configuration packages or other non-Red Hat software to the RHUI clients. A protected repository for 64-bit RHUI servers (for example, **client-rhui-x86_64**) will be the preferred vehicle for distributing new non-Red Hat packages, such as an updated client configuration package, to the RHUI clients.

Like Red Hat content repositories, all of which are protected, protected custom repositories that differ only in processor architecture (**i386** versus **AMD64**) are consolidated into a single entitlement within an entitlement certificate, using the **$basearch** yum variable.

In the event of certificate problems, an unprotected repository for RHUI servers can be used as a fallback method for distributing updated RPMs to the RHUI clients.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press **r** to select **manage repositories**.

3. From the **Repository Management** screen, press **c** to select **create a new custom repository (RPM content only)**.

4. 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 valid entries.

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

5. Enter a display name for the repository. This name is used to identify the repository within the Red Hat Update Infrastructure Management Tool.

   ```
   Display name for the custom repository [repo_1]:
   ```

6. Specify the path that will host the repository. The path must be unique across all repositories hosted by RHUI. For example, if you specify the path at this step as **some/unique/name**, then the repository will be located at **//server/pulp/repos/some/unique/name**.

   ```
   Unique path at which the repository will be served [repo_1]:
   ```

7. Select **sha256** as the checksum type to be used for the repository metadata.
NOTE

Use sha256 when you create a custom repository for RHEL 6, RHEL 7, or RHEL 8. Use sha1 if you create repositories for RHEL 5 client.

Algorithm to use when calculating the checksum values for repository metadata:

1 - sha256 (default)
2 - sha1 (RHEL 5)

Enter value (1-2) or 'b' to abort:

8. Choose whether to protect the new repository. If you answer no to this question, any client can access the repository. If you answer yes, only clients with an appropriate entitlement certificate can access the repository.

WARNING

As the name implies, the content in an unprotected repository is available to any system that requests it, without any need for a client entitlement certificate. Be careful when using an unprotected repository to distribute any content, particularly content such as updated client configuration RPMs, which will then provide access to protected repositories.

9. Answer yes or no to the following questions as they appear:

Should the repository require clients to perform a GPG check and verify packages are signed by a GPG key? (y/n)

Will the repository be used to host any Red Hat GPG signed content? (y/n)

Will the repository be used to host any custom GPG signed content? (y/n)

Enter the absolute path to the public key of the GPG key pair:

Would you like to enter another public key? (y/n)

Enter the absolute path to the public key of the GPG key pair:

Would you like to enter another public key? (y/n)

10. The details of the new repository displays. Press y at the prompt to confirm the information and create the repository.

Verification

1. From the Repository Management screen, press I to check that the correct repositories have been installed.

Additional resources
2.6. DELETING A REPOSITORY FROM RHUI

When the Red Hat Update Infrastructure Management Tool deletes a Red Hat repository, it deletes the repository from the RHUA and all applicable CDS nodes.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press r to select manage repositories.

3. From the Repository Management screen, press d at the prompt to delete a Red Hat repository. A list of all repositories currently being managed by RHUI displays.

4. Select which repositories to delete by typing the number of the repository at the prompt. Typing the number of a repository places a checkmark next to the name of that repository. You can also choose the range of repositories, for instance, by entering 1 - 5.

5. Continue until all repositories you want to delete are checked.

6. Press c at the prompt to confirm.

   NOTE

   After you delete the repositories, the client configuration RPMs that refer to the deleted repositories will not be available to be used by yum.

2.7. UPLOADING CONTENT TO A CUSTOM REPOSITORY (RPM CONTENT ONLY)

You can upload multiple packages and upload to more than one repository at a time. Packages are uploaded to the RHUA immediately but are not available on the CDS node until the next time the CDS node synchronizes.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press r to select manage repositories.

3. From the Repository Management screen, press u:

   Select the repositories to upload the package into:
   - 1: test

4. Enter the value (1-1) to toggle the selection.
5. Press c to confirm your selection.

6. 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/localuser/bear-4.1-1.noarch.rpm

   The following RPMs will be uploaded:
   bear-4.1-1.noarch.rpm

7. Press y to proceed or n to cancel:

   Uploaded /home/ec2-user/bear-4.1-1.noarch.rpm

Verification

1. A similar message displays if the content uploaded successfully:

   Uploaded /home/ec2-user/bear-4.1-1.noarch.rpm
   Total of 1 packages uploaded.
   1 RPM(s) associated to repo test.

2.8. UPLOADING CONTENT FROM A REMOTE WEB SITE (RPM CONTENT ONLY)

You can upload packages that are stored on a remote server without having to manually download them first. The packages must be accessible by HTTP, HTTPS, or FTP.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press r to select manage repositories.

3. From the Repository Management screen, press ur:

   Select the repositories to upload the package into:
   - 1: test

4. Enter the value (1-1) to toggle the selection.

5. Press c to confirm your selection:

   ### WARNING ### WARNING ### WARNING ### WARNING ### WARNING ###
   WARNING ###
   # Content retrieved from non-Red Hat arbitrary places can contain unsupported or malicious software. Proceed at your own risk. #
   #
   #******************************************************************************


6. Enter the remote URL of the packages to upload. If the location is an RPM, the file will be uploaded. If the location is a web page, all RPMs linked off that page will be uploaded:

```
```

```
Found 1 RPMs to download
Retrieving https://repos.fedorapeople.org/pulp/pulp/demo_repos/zoo/bear-4.1-1.noarch.rpm
```

The following RPMs will be uploaded:

```
bear-4.1-1.noarch.rpm
```

7. Press **y** to proceed or **n** to cancel:

```
Uploaded /tmp/rhui.318mfp81.tmp/bear-4.1-1.noarch.rpm
```

**Verification**

1. A similar message displays if the content uploaded successfully:

```
Uploaded /tmp/rhui.318mfp81.tmp/bear-4.1-1.noarch.rpm
Total of 1 packages uploaded.
1 RPM(s) associated to repo test.
```

**2.9. LISTING THE PACKAGES IN A REPOSITORY (RPM CONTENT ONLY)**

When listing repositories within the Red Hat Update Infrastructure Management Tool, only repositories that contain fewer than 100 packages display their contents. Results with more than 100 packages only display a package count.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

```
[root@rhua ~]# rhui-manager
```

2. Press **r** to select **manage repositories**.

3. From the **Repository Management** screen, press **p**.

4. Select the number of the repository you want to view. The Red Hat Update Infrastructure Management Tool asks if you want to filter the results. Leave the line blank to see the results without a filter.

```
Enter value (1-1631) or 'b' to abort: 1
Enter the first few characters (case insensitive) of an RPM to filter the results
```
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:
bear-4.1-1.noarch.rpm

Verification

1. One of three types of messages displays:

   Packages:
bear-4.1-1.noarch.rpm

   Package Count: 8001

   No packages in the repository.
CHAPTER 3. CREATING AN ENTITLEMENT CERTIFICATE AND A CLIENT CONFIGURATION RPM

RHUI uses entitlement certificates to ensure that the client making requests on the repositories is authorized by the cloud provider to access those repositories. The entitlement certificate must be signed by the cloud provider’s Certificate Authority (CA) Certificate. The CA Certificate is installed on the CDS as part of its configuration.

3.1. CREATING A CLIENT ENTITLEMENT CERTIFICATE WITH THE RED HAT UPDATE INFRASTRUCTURE MANAGEMENT TOOL

When Red Hat issues the original entitlement certificate, it grants access to the repositories you requested. When you create client entitlement certificates, you decide how to subdivide your clients and create a separate certificate for each one. Each certificate can then be used to create individual RPMs.

Prerequisites

- The entitlement certificate must be signed by the cloud provider’s CA Certificate.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press e to select create entitlement certificates and client configuration RPMs

3. Press e to select generate an entitlement certificate

4. 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 places an x next to the name of that repository. Continue until all repositories you want to add have been checked.

   **IMPORTANT**

   Include only repositories for a single RHEL version in a single entitlement. Adding repositories for multiple RHEL versions leads to an unusable yum configuration file.

5. Press c at the prompt to confirm.

6. Enter a name for the certificate. This name helps identify the certificate within the Red Hat Update Infrastructure Management Tool and 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.

7. Enter a path to save the certificate. Leave the field blank to save it to the current working directory.
8. Enter the number of days the certificate should be valid for. Leave the field blank for 365 days. The details of the repositories to be included in the certificate display.

Repositories to be included in the entitlement certificate:

Red Hat Repositories
- Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Debug RPMs) from RHUI
- Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI
- Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI

Proceed? (y/n)

9. Press y at the prompt to confirm the information and create the entitlement certificate.

Verification

1. You will see a similar message if the entitlement certificate was created:

..........................+++++
....+++++
Entitlement certificate created at ./rhel8-for-rhui4.crt

3.2. CREATING A CLIENT ENTITLEMENT CERTIFICATE WITH THE CLI

When Red Hat issues the original entitlement certificate, it grants access to the repositories you requested. When you create client entitlement certificates, you decide how to subdivide your clients and create a separate certificate for each one. Each certificate can then be used to create individual RPMs.

Prerequisites

- The entitlement certificate must be signed by the cloud provider’s CA Certificate.

Procedure

1. Use the following command to create an entitlement certificate from the RHUI CLI:

```
# rhui-manager client cert --repo_label rhel-8-for-x86_64-appstream-eus-rhui-source-rpms --name rhuiclientexample --days 365 --dir /root/clientcert

.............................+++++
...........................................+++++
Entitlement certificate created at /root/clientcert/rhuiclientexample.crt
```

NOTE

Use Red Hat repository labels, not IDs. To get a list of all labels, run the `rhui-manager client labels` command. If you include a protected custom repository in the certificate, use the repository’s ID instead.

Verification

1. A similar message displays if you successfully created and entitlement certificate:
Entitlement certificate created at /root/clientcert/rhuiclientexample.crt

3.3. CREATING A CLIENT CONFIGURATION RPM WITH THE RED HAT UPDATE INFRASTRUCTURE MANAGEMENT TOOL

When Red Hat issues the original entitlement certificate, it grants access to the repositories you requested. When you create client entitlement certificates, you need to decide how to subdivide your clients and create a separate certificate for each one. You can then use each certificate to create individual RPMs for installation on the appropriate guest images.

Use this procedure to create RPMs with the RHUI Management Tool.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:
   
   [root@rhua ~]# rhui-manager

2. Press e to select create entitlement certificates and client configuration RPMs.

3. From the Client Entitlement Management screen, press c to select create a client configuration RPM from an entitlement certificate.

4. Enter the full path of a local directory to save the configuration files to:

   Full path to 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):

5. Enter the name of the RPM.

6. Enter the version of the configuration RPM. The default version is 2.0.

7. Enter the release of the configuration RPM. The default version is 1.

8. Enter the full path to the entitlement certificate authorizing the client to access specific channels.

9. Enter the full path to the private key for the entitlement certificate.

10. Select any unprotected custom repositories to be included in the client configuration.

11. Press c to confirm selections or ? for more commands.

Verification

1. A similar message displays if the RPM was successfully created:

   Successfully created client configuration RPM.
   Location: /tmp/clientrpmtest-2.0/build/RPMS/noarch/clientrpmtest-2.0-1.noarch.rpm

3.4. CREATING A CLIENT CONFIGURATION RPM WITH THE CLI

When Red Hat issues the original entitlement certificate, it grants access to the repositories you
requested. When you create client entitlement certificates, you need to decide how to subdivide your clients and create a separate certificate for each one. You can then use each certificate to create individual RPMs for installation on the appropriate guest images.

Use this procedure to create RPMs with the CLI.

**Procedure**

1. Use the following command to create an RPM with the RHUI CLI:

   ```
   # rhui-manager client rpm --entitlement_cert /root/clientcert/rhuiclientexample.crt --private_key /root/clientcert/rhuiclientexample.key --rpm_name clientrpmtest --dir /tmp --unprotected_repos unprotected_repo1
   Successfully created client configuration RPM.
   Location: /tmp/clientrpmtest-2.0/build/RPMS/noarch/clientrpmtest-2.0-1.noarch.rpm
   ```

   **NOTE**

   When using the CLI, you can also specify the URL of the proxy server to use with RHUI repositories, or you can use *none* (including the underscores) to override any global yum settings on a client machine. To specify a proxy, use the `--proxy` parameter.

**Verification**

1. A similar message displays if you successfully created a client configuration RPM:

   ```
   Successfully created client configuration RPM.
   Location: /tmp/clientrpmtest-2.0/build/RPMS/noarch/clientrpmtest-2.0-1.noarch.rpm
   ```
CHAPTER 4. MANAGING RED HAT ENTITLEMENT CERTIFICATES

4.1. RED HAT UPDATE APPLIANCE CERTIFICATES

The RHUA in RHUI uses the following certificates and keys:

- Content certificate and private key
- Entitlement certificate and private key
- SSL certificate and private key
- Cloud provider’s CA certificate

The RHUA is configured with the content certificate and the entitlement certificate. The RHUA uses the content certificate to connect to the Red Hat CDN. It also uses the Red Hat CA certificate to verify the connection to the Red Hat CDN. As the RHUA is the only component that connects to the Red Hat CDN, it is the only RHUI component that has this certificate deployed. It should be noted that multiple RHUI installations can use the same content certificate. For instance, the Amazon EC2 cloud runs multiple RHUI installations (one per region), but each RHUI installation uses the same content certificate.

Clients use the entitlement certificate to permit access to packages in RHUI. To perform an environment health check, the RHUA attempts a `yum` request against each CDS. To succeed, the `yum` request must specify a valid entitlement certificate.

4.2. CONTENT DELIVERY SERVER CERTIFICATES

Each CDS node in RHUI uses the following certificates and keys:

- SSL certificate and private key
- Cloud provider’s CA certificate

The only certificate necessary for the CDS is an SSL certificate, which permits HTTPS communications between the client and the CDS. The SSL certificates are scoped to a specific hostname, so a unique SSL certificate is required for each CDS node. If SSL errors occur when connecting to a CDS, verify that the certificate’s common name is set to the fully qualified domain name (FQDN) of the CDS on which it is installed.

The CA certificate is used to verify that the entitlement certificate sent by the client as part of a `yum` request was signed by the cloud provider. This prevents a rogue instance from generating its own entitlement certificate for unauthorized use within RHUI.

4.3. CLIENT CERTIFICATES

Each client in the RHUI uses an entitlement certificate and private key as well as the cloud provider’s CA certificate.

The entitlement certificate and its private key enable information encryption from the CDS back to the client. Each client uses the entitlement certificate when connecting to the CDS to prove it has permission to download its packages. All clients use a single entitlement certificate.
The cloud provider’s CA certificate is used to verify the CDS’s SSL certificate when connecting to it. This ensures that a rogue instance is not impersonating the CDS and introducing potentially malicious packages into the client.

The CA certificate verifies the SSL certificate, not the entitlement certificate. The reverse is true for the CDS node. The SSL certificate and private key are used to encrypt data from the client to the CDS. The CA certificate present on the CDS verifies that the CDS node should trust the entitlement certificate sent by the client.

4.3.1. Listing the entitled products for a certificate

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

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press n to select manage Red Hat entitlement certificates

3. From the Entitlements Manager screen, press l to list data about the current content certificate:

   rhui (entitlements) => l

   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Debug RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

   Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

   Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

   Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Source RPMs) from RHUI  
   Expiration: 02-27-2022  Certificate: c885597492374720bb5d398c3f65d1ed.pem

Verification

1. You will see a list of the entitled products in the current Red Hat content certificates.

4.3.2. Listing custom repository entitlements

You can use the Entitlements Manager screen to list custom repository entitlements.

Procedure


1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press `n` to select manage Red Hat entitlement certificates

3. From the Entitlements Manager screen, press `c` 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
CHAPTER 5. CHECKING SYNCHRONIZATION STATUS AND SCHEDULING

A repository is a storage location for software packages (RPMs). RHEL uses `yum` commands to search a repository, download, install, and configure the RPMs. The RPMs contain all the dependencies needed to run an application. RPMs also download updates for software in your repositories.

The length of the initial synchronization of Red Hat content can vary. If you choose to synchronize repositories as soon as possible, you can synchronize all repositories in Red Hat Update Infrastructure 4 by running `rhui-manager repo sync_all` in the CLI.

5.1. DISPLAYING REPOSITORY SYNCHRONIZATION SUMMARY

You can use the `Synchronization Status` screen to display information about a particular repository.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```bash
   [root@rhua ~]# rhui-manager
   ```

2. Press `s` to select `synchronization status and scheduling`

3. From the `Synchronization Status` screen, press `dr`:

   ```
   -= Repository Summary Synchronization Status =-
   Last Refreshed: 02:01:22
   (updated every 5 seconds, ctrl+c to exit)
   
   Last Sync Last Result
   Red Hat Enterprise Linux 8 for ARM 64 - BaseOS (Debug RPMs) from RHUI (8) Never None
   ....
   ....
   Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2)
   2021-07-29 17:45:41 Running
   Associating Content: 11001 (97%)
   Downloading Artifacts: 7376
   ```

5.2. DISPLAYING RUNNING SYNCHRONIZATIONS

You can use the `Synchronization Status` screen to check the status on running synchronization tasks.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```bash
   [root@rhua ~]# rhui-manager
   ```

2. Press `s` to select `synchronization status and scheduling`
3. From the **Synchronization Status** screen, press **rr**:

```
Last Refreshed: 02:06:46
(updated every 5 seconds, ctrl+c to exit)

Current Sync               Result
-------------------------------------------------
Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2)
2021-07-29 17:45:41       Running
Associating Content: 11001 (97%)
Downloading Artifacts: 7376
```

5.3. VIEWING THE DETAILS OF THE LAST REPOSITORY SYNCHRONIZATION

You can use the **Synchronization Status** screen to view the details of the last repository synchronization.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press **s** to select **synchronization status and scheduling**

3. From the **Synchronization Status** screen, press **vr**.

4. Enter the number for the repository that you want to see details for:

   Enter value (1-66) or 'b' to abort:

**Verification**

1. A similar message displays if the selected repository has not been synchronized:

   Repo: Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2)
   No syncs have been completed for this repository.

5.4. SYNCHRONIZING AN INDIVIDUAL REPOSITORY IMMEDIATELY

The initial synchronization of content can take a while, typically 10 to 20 minutes. If you choose to synchronize repositories as soon as possible, you can synchronize all repositories in Red Hat Update Infrastructure 4 by running `rhui-manager repo sync_all` in the CLI.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press **s** to select **synchronization status and scheduling**
3. From the **Synchronization Status** screen, press **sr**.

   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. Sync requests for repositories with tasks in running or pending state will be ignored.

<table>
<thead>
<tr>
<th>Last Result</th>
<th>Next Sync</th>
<th>Repository</th>
</tr>
</thead>
</table>

4. Select the repository by entering the value beside the repository name. Enter one repository selection at a time before confirming your product selection:

   x 714: Error 2021-11-17 20:30:00 Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)

5. Press **c** to confirm:

   The following repositories will be scheduled for synchronization:
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)
   Proceed? (y/n) y

6. Press **y** to proceed:

   Scheduling sync for Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)...
   ... successfully scheduled for the next available timeslot.

   **NOTE**
   This message displays if a task for the selected repository is running. *Ignoring sync request for Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2) as the repo is currently reserved by a running task.*

5.5. CANCELING ACTIVE SYNCHRONIZATION TASKS

Most environments synchronize repositories on a scheduled basis. You may encounter a situation where you need to cancel active synchronization tasks.

**Prerequisites**

- There are existing repositories.
- There are active synchronization tasks.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press **s** to select **synchronization status and scheduling**
3. From the **Synchronization Status** screen, press **ca** to select **cancel active sync tasks**

4. Enter the value for the task or tasks that you want to cancel:

   Select one or more repositories for which you want to cancel their active tasks.
   
   - 1: Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2)
   
   Enter value (1-1) to toggle selection, 'c' to confirm selections, or '?' for more commands:

5. Press **c** to confirm your selection.

6. Press **y** to cancel the synchronization task or tasks:

   The active tasks will be canceled for the following repositories:

   Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2)

   Proceed? (y/n)

**Verification**

1. A similar message displays if you cancel an active synchronization task:

   Canceling active task for repo Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (Debug RPMs) (8.2) ...

   ... done

### 5.6. CANCELING WAITING SYNCHRONIZATION TASKS

Most environments synchronize repositories on a scheduled basis. You may encounter a situation where you need to cancel pending synchronization tasks.

**Prerequisites**

- There are existing repositories.
- There are scheduled synchronization tasks.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press **s** to select **synchronization status and scheduling**

3. From the **Synchronization Status** screen, press **cw** to select **cancel waiting sync tasks**

4. Enter the value for the task or tasks that you want to cancel:

   Select one or more repositories for which you want to cancel their pending tasks.
   
   - 1: Single Sign-On 7.4 for RHEL 8 x86_64 (Source RPMs) from RHUI
   
   Enter value (1-1) to toggle selection, 'c' to confirm selections, or '?' for more commands: 1

5. Press **c** to confirm your selection:
Select one or more repositories for which you want to cancel their pending tasks.

x 1: Single Sign-On 7.4 for RHEL 8 x86_64 (Source RPMs) from RHUI

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

6. Press y to proceed:

The pending tasks will be canceled for the following repositories:
Single Sign-On 7.4 for RHEL 8 x86_64 (Source RPMs) from RHUI

Proceed? (y/n) y

Verification

1. A similar message displays if the cancellation is successful:

Canceling pending task for repo Single Sign-On 7.4 for RHEL 8 x86_64 (Source RPMs) from RHUI ...
... done

2. The following message displays if there are no pending synchronization tasks:

There are no repositories with pending sync related tasks.

5.7. VIEWING AND CHANGING A REPOSITORY AUTO-PUBLISH STATUS

You can use the Synchronization Status screen to look at and modify a repository's auto-publish status.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press s to select synchronization status and scheduling

3. From the Synchronization Status screen, press ap:

   rhui (sync) => ap

   Select one or more repositories to toggle the auto-publish status.
   The operation will be executed as soon as possible depending on other tasks that may be executing in the RHUI.

   Status | Repository
   -------------------------------------------------------------------------------------

   Select one or more repositories:

   Custom Repositories

   Red Hat Repositories: yum
- 713: AUTO Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.3)
- 714: AUTO Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)
- 719: AUTO Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8.3)
- 720: AUTO Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8.4)

4. Enter a value (1-1631) to toggle the selection, c to confirm selections, or ? for more commands:

   The following repositories will have their auto-publish status changed:
   Red Hat Repositories
   yum
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8)

5. Press c to confirm your selection.

6. Press y to proceed.

Verification

1. A similar message displays when you make and confirm a selection:

   Scheduling a task to turn off auto-publish status of repository Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8)

Additional resources

- Red Hat Enterprise Linux repositories that can be delivered through Red Hat’s Certified Cloud and Service Provider (CCSP) partners via RHUI

5.8. VIEWING AND ADVANCING REPOSITORY WORKFLOW

You can use the Synchronization Status screen to look at and change a repository’s workflow.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press s to select synchronization status and scheduling

3. From the Synchronization Status screen, press wf.

4. Enter a value (1-1631) to toggle the selection, c to confirm selections, or ? for more commands:

   The following repositories will be scheduled for workflow push:
   Red Hat Repositories
   yum
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4)
5. Press y to proceed:

Verification

1. A similar message displays if the scheduling was successful:

Scheduling a task for generating metadata version 0 for repo Red Hat Enterprise Linux 8 for ARM 64 - AppStream (RPMs) from RHUI (8.4) ... task scheduled.

5.9. EXPORTING A REPOSITORY TO THE FILE SYSTEM

You can use the Synchronization Status screen to export a repository to a file system.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press s to select synchronization status and scheduling

3. From the Synchronization Status screen, press ex.

4. Enter a value to toggle the selection.

5. Press c to confirm the selection:

   The following repositories will be exported:
   Red Hat Repositories
   yum
   Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8)

6. Press y to proceed.

Verification

1. A similar message displays if the repository is exported to a file system:

   [1/1] Exporting version 1 of the repo Red Hat Enterprise Linux 8 for ARM 64 - AppStream (Source RPMs) from RHUI (8).
CHAPTER 6. MANAGING CONTENT DELIVERY SERVERS

CDS nodes are the main component of a content delivery network (CDN), offering high availability to the client. Running servers in a geographically dispersed manner can also improve response time.

You can use the Content Delivery Server (CDS) Management screen to list, add, delete, and reinstall CDS nodes.

It is up to the cloud provider to determine the best course of action when allocating the necessary devices. The Red Hat Update Infrastructure Management Tool configuration RPM links the package directory with the NGINX configuration to serve it.

**IMPORTANT**

The NGINX configuration is handled through the `/etc/nginx/conf.d/ssl.conf` file during the CDS installation.

If multiple clients experience problems updating against a repository, this might indicate a problem with the RHUI.

### 6.1. LISTING ALL KNOWN CDS INSTANCES MANAGED BY RHUI 4

You can use the Content Delivery Server (CDS) Management screen to list all CDS nodes managed by Red Hat Update Infrastructure 4.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   ```
   [root@rhua ~]# rhui-manager
   ```

2. Press `c` to select manage content delivery servers (CDS)

3. From the Content Delivery Server (CDS) Management screen, press `l` to list all known CDS nodes that Red Hat Update Infrastructure 4 manages:

   ```
   Hostname: <cds1.example.com>
   SSH Username: <cloud-user>
   SSH Private Key: /<cloud-user>/.ssh/id_rsa
   ```

### 6.2. REGISTERING A NEW CDS

The Red Hat Update Infrastructure Management Tool provides several options for configuring a CDS within the RHUI.

**Prerequisites**

- Make sure `sshd` is running on the CDS node and that `port 443` is open.

**Procedure**

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:
2. Press c to select **manage content delivery servers (CDS)**

3. From the **Content Delivery Server (CDS) Management** screen, press a to add a new CDS instance.

4. Enter the hostname of the CDS to add:

```
Hostname of the CDS instance to register:
cds1.example.com
```

5. Enter the user name that will have SSH access to the CDS and have sudo privileges.

```
Username with SSH access to <cds1.example.com> and sudo privileges:
<cloud-user>
```

6. Enter the absolute path to the SSH private key for logging in to the CDS and press **Enter**.

```
Absolute path to an SSH private key to log into <cds1.example.com> as <cloud-user>:
/<cloud-user>/.ssh/id_rsa
```

```
The following CDS has been successfully added:

Hostname: <cds1.example.com>
SSH Username: <cloud-user>
SSH Private Key: /<cloud-user>/.ssh/id_rsa
```

```
The CDS will now be configured:
```
```
The CDS was successfully configured.
```

7. If adding the content delivery server fails, check that the firewall rules permit access between the RHUA and the CDS.

8. Run the **mount** command to see if shared storage is mounted as read-write.

```
[root@rhua ~]# mount | grep rhui
```
```
nfs.example.com:/export on /var/lib/rhui/remote_share type nfs4
(rw,relatime,vers=4.2,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.8.41.163,local_lock=none,addr=10.8.41.163)
```

9. After successful configuration, repeat these steps for any remaining CDS nodes. You can also add a CDS using the command line interface:

```
NOTE
You can authorize the key first so that you do not need to use **--unsafe**.
```

```
[root@rhua ~]# rhui-manager cds add --hostname cds01.example.com --ssh_user cloud-user
--keyfile_path /home/cloud-user/.ssh/id_rsa_rhua --unsafe
```
6.3. REINSTALLING AND REAPPLYING CONFIGURATION TO A CDS

You may encounter a situation where you need to reinstall and reapply the configuration for a CDS. The Red Hat Update Infrastructure Management Tool provides an easy way to accomplish this task.

Prerequisites

- At least one installed CDS

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press c to select manage content delivery servers (CDS)

3. From the Content Delivery Server (CDS) Management screen, press r to select reinstall and reapply configuration to an existing CDS instance. The Red Hat Update Infrastructure Management Tool automatically performs all reinstallation and reconfiguration tasks.

4. Select the CDS to reinstall:

   1 -
   Hostname: <cds1.example.com>
   SSH Username: <cloud-user>
   SSH Private Key: /<cloud-user>/.ssh/id_rsa_rhua

5. Enter a value or b to abort: 1:

   Checking that the RHUA services are reachable from the instance...
   Done.

   Installing and configuring the CDS...

   PLAY [Registering a CDS instance] **************************************

   PLAY RECAP ************************************************************
   cloud-user@cds1.example.com : ok=24  changed=10  unreachable=0  failed=0
   skipped=2  rescued=0  ignored=0

   Done.

Verification

1. Check that you successfully reinstalled and reconfigured the CDS by viewing the code output:

   Ensuring that instance ports are reachable ...
   Done.
6.4. CONFIGURING A CDS TO ACCEPT LEGACY CAS

By default, a content delivery server (CDS) node only accepts entitlement certificates signed by the Certificate Authority (CA) that is currently configured on your RHUI system. However, you might want to accept previously created CAs so that clients can continue to work in case you change your main CA or when the CA certificate expires.

This procedure provides instructions to support legacy CAs on RHUI by installing CA certificates on your CDS nodes.

**Prerequisites**

- Ensure you are running the latest version of RHUI.

  **NOTE**

  If you have installed an older version of RHUI, you must reinstall your CDS nodes in `rhui-manager`.

**Procedure**

1. On the CDS node, create the `/etc/pki/rhui/legacy` directory if it does not already exist:

   ```
   # mkdir /etc/pki/rhui/legacy
   ```

2. Save the legacy CA certificate in the directory.

**Verification**

- The CDS node starts accepting legacy CAs as soon as you store the CA certificate in the directory.

6.5. CONFIGURING A CDS TO STOP ACCEPTING LEGACY CAS

To limit your content delivery servers (CDS) nodes from accepting legacy certificate authorities (CAs), remove the respective CA certificates.

**Prerequisites**

- Clients are no longer using the CA.

**Procedure**

1. On the CDS node, navigate to the `/etc/pki/rhui/legacy/` directory:

   ```
   # cd /etc/pki/rhui/legacy/
   ```

2. Optional: Back up the existing CA certificates:

3. Delete the CA certificate that corresponds to the CA you want to limit:

   ```
   # rm example-legacy.crt
   ```
Verification

- The CDS node stops accepting legacy CAs as soon as you delete the CA certificate.

6.6. UNREGISTERING A CDS

You can unregister (delete) a CDS instance that you are not going to use.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press c to select manage content delivery servers (CDS)

3. From the Content Delivery Server (CDS) Management screen, press d to delete a CDS instance.

4. Enter the hostname of the CDS to delete:

   Hostname of the CDS instance to unregister:
   cds1.example.com
CHAPTER 7. MANAGING AN HAPROXY LOAD-BALANCER INSTANCE

If more than one CDS is used, a load-balancing solution must be in place to spread client HTTPS requests across all servers. Red Hat Update Infrastructure 4 ships with HAProxy, but it is up to you to choose what load-balancing solution (for example, the one from the cloud provider) to use during the installation. If HAProxy is used, you must also decide how many nodes to bring in.

7.1. LISTING ALL KNOWN HAPROXY LOAD-BALANCER INSTANCES MANAGED BY RHUI 4

You can use Load-balancer (HAProxy) Management screen to show all known HAProxy load-balancer instances that RHUI 4 is managing.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:

   [root@rhua ~]# rhui-manager

2. Press l to select manage HAProxy load-balancer instances

3. From the Load-balancer (HAProxy) Management screen, press l to list the load-balancer instances that RHUI manages:

   Hostname:       <haproxy1.example.com>
   SSH Username:   <cloud-user>
   SSH Private Key: /<cloud-user>/.ssh/id_rsa_rhua

7.2. REGISTERING A NEW HAPROXY LOAD-BALANCER

Red Hat Update Infrastructure 4 uses DNS to reach the CDN. In most cases, your instance should be preconfigured to talk to the proper DNS servers hosted as part of the cloud’s infrastructure. If you run your own DNS servers or update your client DNS configuration, there is a chance you will see errors similar to yum Could not contact any CDS load balancers. In these cases, check that your DNS server is forwarding to the cloud’s DNS servers for the request or that your DNS client is configured to fall back to the cloud’s DNS server for name resolution.

Using more than one HAProxy node requires a round-robin DNS entry for the hostname used as the value of the --cds-lb-hostname parameter when rhui-installer is run (cds.example.com in this guide) that resolves to the IP addresses of all HAProxy nodes. How to Configure DNS Round Robin presents one way to configure a round-robin DNS. In the context of Red Hat Update Infrastructure 4, these will be the IP addresses of the HAProxy nodes, and they are to be mapped to the hostname specified as --cds-lb-hostname while calling rhui-installer.

Prerequisites

1. Make sure sshd is running on the HAProxy load-balancer node and that port 443 is open.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:
2. Press l to select **manage HAProxy load-balancer instances**.

3. From the **Load-balancer (HAProxy) Management** screen, press a to add a new load-balancer instance.

4. Enter the hostname of the new load-balancer:

   Hostname of the HAProxy Load-balancer instance to register:
   <haproxy1.example.com>

5. Enter the user name that will have SSH access to the load-balancer and have sudo privileges:

   <cloud-user>

6. Enter the absolute path to the SSH private key for logging in to the load-balancer instance and press **Enter**:

   /<cloud-user>/.ssh/id_rsa

   The following load-balancer has been successfully added:

   Hostname: <haproxy1.example.com>
   SSH Username: <cloud-user>
   SSH Private Key: /<cloud-user>/.ssh/id_rsa

   The load-balancer will now be configured:

   ..............................................................

7. If the load-balancer fails to add, check that the firewall rules permit access between the RHUA and the load-balancer.

8. After successful configuration, repeat these steps for any remaining load-balancer instances.

**Verification**

1. The following message displays:

   The HAProxy Load-balancer was successfully configured.

**Additional resources**

- **HAProxy Configuration**

**7.3. REINSTALLING AND REAPPLYING THE CONFIGURATION TO AN HAProxy LOAD-BALANCER**

You may encounter a situation where you need to reinstall and reapply the configuration for an HAProxy load-balancer. The Red Hat Update Infrastructure Management Tool provides an easy way to accomplish this task.
Prerequisites

- Make sure `sshd` is running on the HAProxy load-balancer node and that `port 443` is open.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:
   ```bash
   [root@rhua ~]# rhui-manager
   ```

2. Press `l` to select **manage HAProxy load-balancer instances**

3. From the **Load-balancer (HAProxy) Management** screen, press `r` to reinstall and reapply the configuration to a load-balancer instance.

   **IMPORTANT**
   It is crucial that the files included in the restore retain their current attributes.

The Red Hat Update Infrastructure Management Tool automatically performs all reinstallation and reconfiguration tasks.

1. Select the load-balancer to reinstall:

   1 -
   ```
   Hostname:    <haproxy1.example.com>
   SSH Username:  <cloud-user>
   SSH Private Key:  /<cloud-user>/.ssh/id_rsa_rhua
   ```

2. Enter a value or `b` to abort: 1:

   Installing and configuring the HAProxy Load-balancer...

   PLAY [Registering a load balancer instance] ****************************************

   PLAY RECAP *********************************************************************
   cloud-user@haproxy1.example.com : ok=8  changed=3  unreachable=0  failed=0
   skipped=0  rescued=0  ignored=0
   Done.

Verification

1. Check that you successfully reinstalled and reconfigured the load-balancer by viewing the code output:

   Ensuring that HAProxy is available...
   Done.

7.4. UNREGISTRATION AN HAPROXY LOAD-BALANCER

You can unregister (delete) an HAProxy load-balancer instance that you are not going to use.
Prerequisites

- Make sure `sshd` is running on the HAProxy load-balancer node and that port 443 is open.

Procedure

1. Navigate to the Red Hat Update Infrastructure Management Tool home screen:
   ```bash
   [root@rhua ~]# rhui-manager
   ```
2. Press `l` to select `manage HAProxy load-balancer instances`.
3. From the `Load-balancer (HAProxy) Management` screen, press `d` to delete a load-balancer instance.
4. Enter the hostname of the load-balancer to delete:
   ```
   Hostname of the load-balancer instance to unregister:
   <haproxy1.example.com>
   ```
# CHAPTER 8. CONFIGURATION FILES, STATUS CODES, AND LOG FILES

The following configuration files, status codes, and log files are used in Red Hat Update Infrastructure 4.

## Table 8.1. Configuration Files

<table>
<thead>
<tr>
<th>Component</th>
<th>File or Directory</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Update Appliance</td>
<td>/etc/pulp/*</td>
<td>Pulp config files</td>
</tr>
<tr>
<td></td>
<td>/etc/rhui/rhui-tools.conf</td>
<td>rhui-manager config files</td>
</tr>
<tr>
<td></td>
<td>/etc/pki/rhui/*</td>
<td>Certificates for Red Hat Update Infrastructure</td>
</tr>
<tr>
<td></td>
<td>/root/.rhui/answers.yaml</td>
<td>Used to set up the RHUA</td>
</tr>
<tr>
<td></td>
<td>/etc/rhui/rhuisubscription-sync.conf</td>
<td>Configuration for the subscription synchronization script</td>
</tr>
<tr>
<td>Content Delivery Server</td>
<td>/etc/pki/rhui/certs/</td>
<td>Certificates for CDS</td>
</tr>
<tr>
<td>HAProxy</td>
<td>/etc/haproxy/haproxy.cfg</td>
<td>HAPerapy configuration file</td>
</tr>
</tbody>
</table>

## Table 8.2. Status Codes

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>Repository synchronization error</td>
</tr>
<tr>
<td>32</td>
<td>Entitlement CA certificate expiration warning</td>
</tr>
<tr>
<td>64</td>
<td>Entitlement CA certificate expiration error</td>
</tr>
</tbody>
</table>

## Table 8.3. Log Files

<table>
<thead>
<tr>
<th>Component</th>
<th>File or Directory</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Update Appliance</td>
<td>/root/.rhui/rhui.log*, assuming rhui-manager is run as root</td>
<td>Red Hat Update Infrastructure Management Tool logs</td>
</tr>
<tr>
<td></td>
<td>/var/log/messages</td>
<td>The most recent four versions are kept in addition to the currently written file.</td>
</tr>
<tr>
<td>Component</td>
<td>File or Directory</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>/var/log/nginx/*</td>
<td></td>
<td>NGINX logs</td>
</tr>
<tr>
<td>/var/log/messages</td>
<td></td>
<td>Qpid logs</td>
</tr>
<tr>
<td>/var/log/rhui-subscription-</td>
<td></td>
<td>Subscription synchronization log</td>
</tr>
<tr>
<td>sync.log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Delivery Server</td>
<td>/var/log/nginx/*</td>
<td>NGINX logs</td>
</tr>
<tr>
<td>/nginx/ssl-access.log</td>
<td></td>
<td>Sample Logging – Successful yum repolist: the CDS nodes log this client activity</td>
</tr>
<tr>
<td>Client</td>
<td>/var/log/yum.log for RHEL 7 and earlier versions</td>
<td>yum command logs</td>
</tr>
<tr>
<td>Client</td>
<td>/var/log/dnf.log for RHEL 8 and later versions</td>
<td>dnf command logs</td>
</tr>
<tr>
<td>/var/log/messages</td>
<td></td>
<td>Client syslog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Console output from yum/dnf commands</td>
</tr>
</tbody>
</table>
CHAPTER 9. WORKING WITH RHUI 4 COMMANDS

The screens within the Red Hat Update Infrastructure Management Tool, accessed from the RHUpdate, provide menu options that allow you to configure and update the various Red Hat Update Infrastructure 4 components.

9.1. USING RHUI 4 MENU OPTIONS

The Red Hat Update Infrastructure Management Tool provides interactive commands for configuring and managing RHUI 4.

Table 9.1. Red Hat Update Infrastructure Management Tool menus and commands

<table>
<thead>
<tr>
<th>Screen</th>
<th>Screen Command</th>
<th>Menu Option</th>
<th>Menu Option Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>manage repositories</td>
<td>r</td>
<td>list repositories currently managed by the RHUI</td>
<td>l</td>
</tr>
<tr>
<td>Managed Repositories</td>
<td></td>
<td>display detailed information on a repository</td>
<td>i</td>
</tr>
<tr>
<td></td>
<td></td>
<td>add a new Red Hat content repository</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>create a new custom repository (RPM content only)</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>delete a repository from the RHUI</td>
<td>d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upload content to a custom repository (RPM content only)</td>
<td>u</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upload content from a remote web site (RPM content only)</td>
<td>ur</td>
</tr>
<tr>
<td></td>
<td></td>
<td>list packages in a repository (RPM content only)</td>
<td>p</td>
</tr>
<tr>
<td>manage content delivery servers (CDS)</td>
<td>c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen</td>
<td>Screen Command</td>
<td>Menu Option</td>
<td>Menu Option Command</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Content Delivery Server (CDS) Management</td>
<td></td>
<td>list all known CDS instances managed by the RHUI</td>
<td>l</td>
</tr>
<tr>
<td></td>
<td></td>
<td>register (add) a new CDS instance</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reinstall and reapply configuration to an existing CDS instance</td>
<td>r</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unregister (delete) a CDS instance from the RHUI</td>
<td>d</td>
</tr>
<tr>
<td>manage HAProxy load-balancer instances</td>
<td>l</td>
<td>list all known HAProxy Load-balancer instances managed by the RHUI</td>
<td>l</td>
</tr>
<tr>
<td></td>
<td></td>
<td>register (add) a new HAProxy Load-balancer instance</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reinstall and reapply configuration to an existing HAProxy Load-balancer instance</td>
<td>r</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unregister (delete) a HAProxy Load-balancer instance from the RHUI</td>
<td>d</td>
</tr>
<tr>
<td>synchronization status and scheduling</td>
<td>s</td>
<td>display repo sync summary</td>
<td>dr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>display running syncs</td>
<td>rr</td>
</tr>
<tr>
<td>Synchronization Status</td>
<td></td>
<td>view the details of the last repository sync</td>
<td>vr</td>
</tr>
<tr>
<td>Screen</td>
<td>Screen Command</td>
<td>Menu Option</td>
<td>Menu Option Command</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>sync an individual repository immediately</td>
<td></td>
<td>sr</td>
<td></td>
</tr>
<tr>
<td>cancel active sync tasks</td>
<td></td>
<td>ca</td>
<td></td>
</tr>
<tr>
<td>cancel waiting sync tasks</td>
<td></td>
<td>cw</td>
<td></td>
</tr>
<tr>
<td>view/change repository auto-publish status</td>
<td></td>
<td>ap</td>
<td></td>
</tr>
<tr>
<td>view/advance repository workflow</td>
<td></td>
<td>wf</td>
<td></td>
</tr>
<tr>
<td>export repo to filesystem</td>
<td></td>
<td>ex</td>
<td></td>
</tr>
<tr>
<td>create entitlement certificates and client configuration RPMs</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Entitlement Management</td>
<td>generate an entitlement certificate</td>
<td>e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>create a client configuration RPM from an entitlement certificate</td>
<td>c</td>
<td></td>
</tr>
<tr>
<td>Entitlements Manager</td>
<td>list Red Hat content certificate entitlements</td>
<td>l</td>
<td></td>
</tr>
<tr>
<td></td>
<td>list custom repository entitlements</td>
<td>c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>upload a new or updated Red Hat content certificate</td>
<td>u</td>
<td></td>
</tr>
<tr>
<td>manage RHUI users</td>
<td>change admin's password (followed by logout)</td>
<td>p</td>
<td></td>
</tr>
</tbody>
</table>
9.2. USING RHUI 4 CLI OPTIONS

The majority of administrative tasks for Red Hat Update Infrastructure 4 are in its installation. After installation, it runs on its own, periodically getting updated packages from the Red Hat CDN and automatically making those packages available to clients.

A command line interface called Red Hat Update Infrastructure Management Tool (run with `rhui-manager`) facilitates the installation. This tool provides interactive prompts for the necessary configuration elements for each RHUI component: RHUA, CDS, and load-balancer. This tool also provides a means for taking the content certificate provided by Red Hat for use when connecting to the Red Hat CDN and generating internal, cloud-specific certificates that clients use to connect to RHUI. The Red Hat Update Infrastructure Management Tool allows the cloud provider to generate a client configuration bundle to install on client RHEL instances. This bundle allows the clients to get updates from the RHUI installation.

Red Hat Update Infrastructure Management Tool uses an interactive shell; some functions can also run from a shell prompt. The Red Hat Update Infrastructure Management Tool uses seven main commands. For each command’s subcommand, a list of options is provided if the subcommand expects one or more options other than `-h` and `--help`.

View all options and commands.

```
[root@ip-10-141-150-145 ~]# rhui-manager --help
Usage: rhui-manager [options]

OPTIONS
    -h/--help    show this help message and exit
    --debug      enables debug logging
    --noninteractive prevents console input, used for scripting
    --config     absolute path to the configuration file; defaults to /etc/rhui/rhui-tools.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
    --logout     logout from the active session

COMMANDS
    cert     : Red Hat content certificate management
    packages : package manipulation on repositories
    repo     : repository listing and manipulation
    cds      : CDS listing and manipulation
    migrate  : Migrate from {RHUI3}
    haproxy  : Load balancer listing and manipulation
    status   : RHUI status and health information
    client   : Red Hat client management
```

9.2.1. cert

Red Hat content certificate management

```
# rhui-manager cert upload
upload: uploads a new content certificate
```

```
--cert - full path to the new content certificate (required)
--key - full path to the new content certificate's key

9.2.2. packages

package manipulation on repositories
  list : lists all packages in a repository
  upload : uploads a package or directory of packages to a custom repository
  remote : uploads RPM content from a remote URL to a custom repository

list: lists all packages in a repository
  --repo_id - id of the repository to list packages for (required)

upload: uploads a package or directory of packages to a custom repository
  --repo_id - id of the custom repository where the packages will be uploaded (required)
  --packages - path to an .rpm file or directory of RPMs that will be uploaded (required)

remote: uploads RPM content from a remote URL to a custom repository
  --repo_id - id of the custom repository where the packages will be uploaded (required)
  --url - remote URL of the package or a web page that will be scraped for RPM content (required)

9.2.3. repo

repository listing and manipulation
  list : lists all repositories in the RHUI
  info : displays information on an individual repo
  add : add a Red Hat repository to the RHUA
  add_by_repo: add Red Hat repositories to the RHUA via repo ID
  add_errata: associate errata metadata with a repository
  delete : delete a repository
  sync : sync a repository
  export : export a repository to the filesystem
  enable_sync: enable scheduled synchronization of a repository
  disable_sync: disable scheduled synchronization of a repository
  sync_all : sync all repositories
  metadata : ensure metadata is generated for the latest version of repositories
  enable_autopublish: enable automatic publishing of a new repository version
  disable_autopublish: disable automatic publishing of a new repository version
  create_custom: create a custom repository
  unused : list of products available but not synced to the RHUA

info: displays information on an individual repo
  --repo_id - identifies the repository to display (required)

add: add a Red Hat repository to the RHUA
  --product_name - product to add the RHUA (required)

add_by_repo: add Red Hat repositories to the RHUA via repo ID
  --repo_ids - repo IDs to add, comma-separated (required)
add_errata: associate errata metadata with a repository
   --repo_id - repo ID to associate the metadata with (required)
   --updateinfo - updateinfo file to be applied (required)

delete: delete a repository
   --repo_id - identifies the repository to delete (required)

sync: sync a repository
   --repo_id - identifies the repository to sync (required)

export: export a repository to the filesystem
   --repo_id - identifies the repository to export (required)

metadata: ensure metadata is generated for the latest version of repositories
   --repo_id - explicit repo ID to generate metadata for

enable_sync: enable scheduled synchronization of a repository
   --repo_id - identifies the repository to enable scheduled synchronization for (required)
   --verbose - if present, info on last/next synchronization tasks will be displayed

disable_sync: disable scheduled synchronization of a repository
   --repo_id - identifies the repository to disable scheduled synchronization for (required)
   --verbose - if present, info on last/next synchronization tasks will be displayed

enable autopublish: enable automatic publishing of a new repository version
   --repo_id - identifies the repository to enable automatic publishing for (required)

disable autopublish: disable automatic publishing of a new repository version
   --repo_id - identifies the repository to disable automatic publishing for (required)

create_custom: create a custom repository
   --repo_id - identifies the repository to add (required)
   --path - path to the content being served by CDS; defaults to repo_id
   --display_name - display name for the custom repository
   --entitlement - path used in the entitlement certificate; may use yum variable substitutions
   --legacy_md - if present, the repo will use SHA1, otherwise default value is used (SHA256)
   --redhat_content - repository will host Red Hat GPG signed content
   --protected - make the content protected by entitlement certificate
   --gpg_public_keys - comma separated list of public keys used to sign the served content; the filenames must not contain comma

unused: list all unused Red Hat repositories
Loading latest entitled products from Red Hat...
... listings loaded
Available Repositories

9.2.4. cds

CDS listing and manipulation
list : lists all cds instances in the RHUI
add : register a cds instance to the RHUI
reinstall : reinstalls an already registered cds instance
delete : unregisters cds instances from the RHUI

add: register a cds instance to the RHUI
   --hostname - The hostname of the instance to add. (required)
   --ssh_user - Username with SSH access to the instance and sudo privileges. (required)
   --keyfile_path - Absolute path to an SSH private key to use with the given user. (required)
   --hostfile - Absolute path to a known_hosts file to use to determine the identity of the instance; if
   this is not provided and the instance hostkey is not in the system-wide known_hosts file, this
   command will fail.
   --force - Add the system even if the hostname is already registered.
   --unsafe - Proceed even if the instance host key is not in the known_hosts file. This is not secure!

reinstall: reinstalls an already registered cds instance
   --hostname - The hostname of the instance to reinstall on; this instance must be registered already.
   (required)

delete: unregisters cds instances from the RHUI
   --force - Delete the system, even if it is the last of its kind.
   --hostnames - Comma-separated list of hostnames to delete (unregister) from RHUI. (required)

9.2.5. migrate

Migrate from {RHUI3}
   --hostname : the {RHUI3} hostname
   --password : <your_password>
   --keyfile_path : ~/.ssh/id_rsa_rhua*

9.2.6. haproxy

Load balancer listing and manipulation
list : lists all haproxy instances in the RHUI
add : register a haproxy instance to the RHUI
reinstall : reinstalls an already registered haproxy instance
delete : unregisters haproxy instances from the RHUI

add: register a haproxy instance to the RHUI
   --hostname - The hostname of the instance to add. (required)
   --ssh_user - Username with SSH access to the instance and sudo privileges. (required)
   --keyfile_path - Absolute path to an SSH private key to use with the given user. (required)
   --hostfile - Absolute path to a known_hosts file to use to determine the identity of the instance; if
   this is not provided and the instance hostkey is not in the system-wide known_hosts file, this
   command will fail.
   --force - Add the system even if the hostname is already registered.
   --unsafe - Proceed even if the instance host key is not in the known_hosts file. This is not secure!

reinstall: reinstalls an already registered haproxy instance
   --hostname - The hostname of the instance to reinstall on; this instance must be registered already.
   (required)
delete: unregisters haproxy instances from the RHUI
   --force - Delete the system, even if it is the last of its kind.
   --hostnames - Comma-separated list of hostnames to delete (unregister) from RHUI. (required)

9.2.7. status
This command has no subcommands.

9.2.8. client

Red Hat client management
   labels    : list the labels required for client certificate creation
   cert      : create a content certificate for a rhui client
   rpm       : create a client config rpm
   content_source: create an alternate source config rpm

cert: create a content certificate for a rhui client
   --repo_label - identifies the repositories to add. Comma delimited string of repo labels (required)
   --name - identifies the certificate name (required)
   --days - number of days cert will be valid (required)
   --dir - directory where the certificate will be stored (required)

rpm: create a client config rpm
   --private_key - entitlement private key
   --entitlement_cert - entitlement certificate
   --rpm_version - version number of the client config rpm
   --rpm_release - release of rpm package. Default is 1
   --rpm_name - name of the client config rpm (required)
   --dir - directory where the rpm will be created (required)
   --unprotected_repos - comma-separated list of unprotected repos to include
   --cert - generate certificate also before building client config rpm if given
   --ca_cert - full path to the certificate authority of CDS servers
   --repo_label - identifies the repositories to add. Comma delimited string of repo labels
   --name - identifies the certificate name if it is different from rpm name
   --days - number of days cert will be valid
   --proxy - url/string in case proxy option is necessary in yum repo file

content_source: create an alternate source config rpm
   --private_key - entitlement private key
   --entitlement_cert - entitlement certificate
   --rpm_version - version number of the client config rpm
   --rpm_name - name of the client config rpm (required)
   --dir - directory where the rpm will be created (required)
   --unprotected_repos - comma-separated list of unprotected repos to include
   --cert - generate certificate also before building client config rpm if given
   --ca_cert - full path to the certificate authority of CDS servers
   --repo_label - identifies the repositories to add. Comma delimited string of repo labels
   --name - identifies the certificate name if it is different from rpm name
   --days - number of days cert will be valid
CHAPTER 10. CERTIFIED CLOUD AND SERVICE PROVIDER CERTIFICATION WORKFLOW

The Certified Cloud Provider Agreement requires that Red Hat certifies the images (templates) from which tenant instances are created to ensure a fully supported configuration for end customers.

There are two methods for certifying the images for Red Hat Enterprise Linux. The preferred method is to use the Certified Cloud and Service Provider (CCSP) image certification workflow.

After certifications have been reviewed by Red Hat, a pass/fail will be assigned and certification will be posted to the public Red Hat certification website at Red Hat Ecosystem Catalog.

10.1. ADDITIONAL RESOURCES

- Red Hat Certified Cloud and Service Provider Certification Workflow Guide
- Product Documentation for Red Hat Certified Cloud and Service Provider Certification 7.34
The following table lists known issues with Red Hat Update Infrastructure. If you encounter any of these issues, report the problem through Bugzilla. See Troubleshooting Red Hat Update Infrastructure Issues for more details about common issues.

Table 11.1. Common problems in Red Hat Update Infrastructure

<table>
<thead>
<tr>
<th>Event</th>
<th>Description of known issue</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation and Configuration</td>
<td>You experience communication issues between the RHUA and the CDSs.</td>
<td>Verify the fully qualified domain name (FQDN) is set for the RHUA and CDS and is resolvable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure the HTTP proxy properly as described in Bug 726420 – Quick note on proxy URL.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>You cannot synchronize repositories with Red Hat.</td>
<td>Verify the RHUI SKUs are in your account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify the proper content certificates are loaded to the RHUA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Look for temporary CDN issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Look for any HTTP proxy in your environment and make sure you are not hitting an While syncing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>repositories to RHUA, it fails with &quot;RepoError: Cannot retrieve repository metadata (repomd.xml)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for repository. Please verify its path and try again&quot; when proxy used error.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The RHUA cannot synchronize to CDSs, typically due to expired qpid certificates: See CDS sync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fails with error &quot;sslv3 alert certificate expired&quot; due to expired qpid CA certificates on RHUI for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>more information.</td>
</tr>
<tr>
<td>Event</td>
<td>Description of known issue</td>
<td>Recommendation</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Red Hat Update Appliance/Content Delivery Network Communication | The Red Hat Update Appliance is not communicating with the Content Delivery Network. | Use the content certificate in `/etc/pki/rhui/redhat` (the `.pem` file) to test connectivity and access between the RHUA and the CDN.  

```bash
# cd /etc/pki/rhui/redhat
wget --certificate=8a85f98146a087b80146afacb3362499.pem --ca-certificate=/etc/rhsm/ca/redhat-uep.pem https://cdn.redhat.com/content/dist/rhel/rhui/server/6/6Server/x86_64/os/repodata/repomd.xml
```

Note from the curl (1) man page: If the NSS PEM PKCS#11 module (`libnss.pem.so`) is available, then PEM files may be loaded. If you want to use a file from the current directory, precede it with `./` prefix to avoid confusion with a nickname.

On each CDS, the entitlement certificate in `/etc/pki/pulp/content` can be used to test the availability of the RHUA content using `
curl --cert ./rhui-ec2-20120619.pem`

The URL for the repositories hosted on the RHUA always start with `https://fqdn/pulp/content`. You can divulge the remaining URL by: - Looking at the file path on the RHUA under `/var/lib/rhui/remote_share/sym links/pulp/content/` - Examining the content certificate directly using `openssl` commands because the OIDs ending in 1.6 contain the path
<table>
<thead>
<tr>
<th>Event</th>
<th>Description of known issue</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client/Content Delivery Server Communication</td>
<td><strong>curl</strong> can be used to verify client communications with the content delivery server nodes as well.</td>
<td># curl --cert /etc/pki/entitlement/product/content.crt --key /etc/pki/entitlement/key.pem <a href="https://ip-10-4-58-34.ec2.internal/pulp/repos/content/dist/rhel/rhui/server/6/6Server/x86_64/rhui/2.1/os/repo">https://ip-10-4-58-34.ec2.internal/pulp/repos/content/dist/rhel/rhui/server/6/6Server/x86_64/rhui/2.1/os/repo</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>data/repomd.xml -k &lt;xml version=&quot;1.0&quot; encoding=&quot;UTF-8&quot;?&gt; &lt;repomd xmlns=&quot;http://linux.duke.edu/metadata/repo&quot; xmlns:rpm=&quot;http://linux.duke.edu/metadata/rpm&quot;&gt; &lt;revision&gt;1339940325&lt;/revision&gt; &lt;data type=&quot;other_db&quot; xmlns=&quot;http://linux.duke.edu/metadata/repo&quot; href=&quot;repodata/4f86b0ae203bba90d22a8363120c66edf37da81-other.sqlite.bz2&quot; checksum=&quot;4f86b0ae203bba90d22a8363120c66edf37da81&quot; timestamp=&quot;1339940328.43&quot;/&gt;</td>
</tr>
<tr>
<td>Content Delivery Server Synchronization</td>
<td>The CDS synchronization fails with SSL errors because of expired Qpid certificates</td>
<td>CDS sync fails with error <strong>sslv3 alert certificate expired</strong> due to expired qpid CA certificates on RHUI. See Troubleshooting Red Hat Update Infrastructure Issues for more information.</td>
</tr>
<tr>
<td>Client/HAProxy communication</td>
<td>All HAProxy nodes are down. Clients have lost access to RHUI repositories.</td>
<td>Add and configure at least one new HAProxy node. If you cannot do so for whatever reason, temporarily change the DNS configuration so that the main load balancer host name (cds.example.com in this guide) resolves to the IP address of one of your CDS nodes. This will allow the clients to avoid the unavailable HAProxy nodes and communicate with the CDS directly.</td>
</tr>
</tbody>
</table>