Pivotal

PRODUCT DOCUMENTATION

Pivotal Command Center

Version 2.3

User Guide

Rev: A01 – September 18, 2014

Copyright

Contents

Chapter 1. PCC Overview 6
About Pivotal Command Center 7
Pivotal Command Center UI and CLI 7
Performance Monitor (nmon) 8
PostgreSQL Database 8
Architectural Overview 9

Chapter 2. PCC Installation Prerequisites 10
Before You Begin Installing PCC 11
Prerequisite Checklist 12
PCC - DNS Lookup 13
PCC - JAVA JDK 14
Verify JDK Version 14
OpenJDK 14
PCC - Verify Package Accessibility 16
PCC - Turn Off iptables 18
PCC - Disable SELinux 19
Disabling SELinux Temporarily 19
Disabling SELinux Permanently 19
PCC - EPEL Yum Repository 20

Chapter 3. Installation Instructions 21
Supported Platforms and Browsers 22
Platforms 22
Browsers 22
PCC Installation Checklist 23
Install PCC 26
PCC - Importing the Packages 29
Import JDK 29
Copy the PHD Service Packages 29
Import PHD Service 30
Import HAWQ/PXF Services 30
Import PRTS (GemFire) Service 30
Launching PCC 32
Starting, Stopping, and Restarting Command Center Services 32

Chapter 4. Uninstalling PCC 33

Chapter 5. Upgrading PCC 34

Chapter 6. Using PCC 36

PCC UI Overview 37
Status indicators 37
Logging In 38
Login Screen 38
PCC UI Settings 39
PCC UI User Management 40
Users 40
Profiles 42
Passwords 42
Cluster Status Page 43
Configuring and Deploying a Cluster 44
Launching the Add Cluster Wizard 44
Create Cluster Definition 45
Versions, Services, and Hosts 45
Host Verification 47
Cluster Topology 47
Cluster Configuration 49
Validation 49
Deployment Status 49
Summary 50
Starting the Cluster from the UI 51
Initializing and Configuring HAWQ 51
Starting, Stopping, and Uninstalling a Cluster 53
Starting 53
Stopping 53
Uninstalling 53
PCC UI Dashboard 54
Cluster Analysis 57
Filtering the Cluster Analysis Screen 57
Cluster Metrics 58
MapReduce Job Monitor 61
Job Details 62
Yarn App Monitor 65
HAWQ Query Monitor 66
Topology 67
Component Information 67
Topology Actions 67
Logs 70
Filtering Logs 70

Viewing Logs 70

Chapter 7. Configuring PCC for LDAP 72

Chapter 8. Command Line Reference 74

Backup and Restore 75

Backup 75

Restore 75

Chapter 1 PCC Overview

This section provides a brief overview of Pivotal Command Center.

Topics:

- About Pivotal Command Center
  - Pivotal Command Center UI and CLI
  - Performance Monitor (nmon)
  - PostgreSQL Database
- Architectural Overview

About Pivotal Command Center

Pivotal Command Center (PCC) allows an administrative user to configure, deploy, monitor, and manage one or more Pivotal HD clusters. The Command Center has both a graphical user interface and command-line tools to deploy, configure, monitor, and administer Pivotal HD clusters.

- For UI operations, see Using PCC.
- For command-line tools, see *Pivotal HD Enterprise Installation and Administration*.

This release of Command Center allows administering and monitoring of only Pivotal HD Enterprise 2.x clusters.

PCC provides complete life cycle management for Pivotal HD Clusters by performing the following two main groups of functions:

- Cluster configuration and deployment
- Cluster monitoring and management

These functions are served through a set of RESTful web services that run as a web application on Jetty server on the Command Center admin host. This is called `gphdmgr-webservices`. This web application stores its metadata and cluster configuration for Pivotal HD cluster nodes and services in the Pivotal Command Center PostgreSQL database. It makes use of a Puppet Server to perform most of its HD cluster installation and configuration. It also has a polling service that retrieves Hadoop metrics from the cluster and stores them in the Command Center PostgreSQL Database at periodic intervals.

Pivotal Command Center UI and CLI

The PCC UI provides the user with a single web-based graphical user interface to configure, deploy, monitor, and manage one or more Pivotal HD cluster. This web application is hosted on a Ruby-on-Rails application which presents the status and metrics of the clusters. The system metrics data is gathered by the Performance Monitor (nmon) component. The Command Center UI invokes the APIs to retrieve all Hadoop-specific cluster metrics and status information. This includes the Hadoop metrics that was previously retrieved by the polling service.

PCC provides a command-line interface (CLI) for more advanced users to perform installation, configuration and uninstalls. This tool invokes the APIs to install and configure the various Pivotal HD services. The CLI also provides a way to perform other administrative actions such as starting and stopping clusters. For how to use this CLI, please refer to *Pivotal HD Enterprise Installation and Administration*.

Performance Monitor (nmon)

Pivotal Command Center comes with a Performance Monitor called `nmon` (for node monitor). This makes use of a highly scalable message passing architecture to gather performance metrics from each node that Command Center monitors. This consists of a master daemon that runs on the Command Center admin host and an daemon that runs on all the cluster nodes that report system metric information to the master. This includes metrics such as CPU, memory, disk I/O and network usage information.

The master on the admin host dumps the system metrics it receives from the agents on the cluster nodes into a PostgreSQL DB. This is then queried by the Command Center UI application to display its cluster analysis graphs.

The agents hosts are deployed throughout the cluster during Pivotal HD cluster deployment itself (see for Using PCC details).

The agents are deployed as services on each host, including on the Pivotal Command Center admin host.

To stop or start the service run the following as `root`:

```
# service nmon stop
```

```
# service nmon start
```

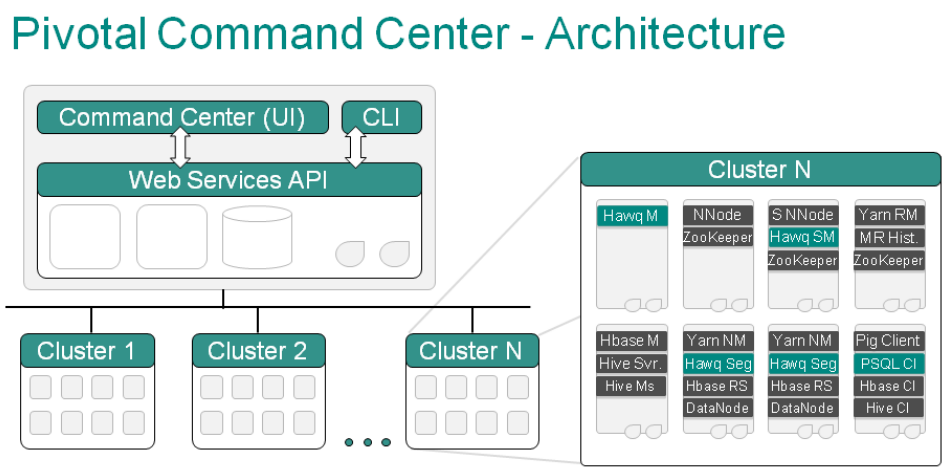
PostgreSQL Database

Pivotal Command Center makes use of a PostgreSQL Database to store the following:

- Cluster configurations
- Hadoop cluster metrics
- System metrics of the cluster
- Pivotal Command Center Metadata

Architectural Overview

For more details about Pivotal HD Enterprise, refer to *Pivotal HD Installation and Administration*.



Chapter 2 PCC Installation Prerequisites

This section provides information you'll need, as well as tasks that must be completed, before you install PCC.

- Before You Begin Installing PCC
- PCC Prerequisite Checklist
- PCC - DNS Lookup
- PCC - JAVA JDK
- PCC - Verify Package Accessibility
- PCC - Turn Off iptables
- PCC - Disable SELinux
- PCC - EPEL Yum Repository

Before You Begin Installing PCC

Before you begin your installation, be sure to read the *PCC Release Notes* for information about the latest features, improvements, resolved and known issues; as well as the latest versioning and compatibility information.

We recommend you have a working knowledge of the following:

- **Yum**: Yum enables you to install or update software from the command line. See http://yum.baseurl.org/.
- **RPM** (Redhat Package Manager). See information on RPM at *Managing RPM-Based Systems with Kickstart and Yum*. See http://shop.oreilly.com/product/9780596513825.do?sortby=publicationDate
- **NTP**. See information on NTP at: http://www.ntp.org
- **SSH** (Secure Shell Protocol). See information on SSH at http://www.linuxproblem.org/art_9.html

Next: Refer to the PCC Prerequisite Checklist

Prerequisite Checklist

The following prerequisite tasks need to be completed before you begin your PCC installation.

Each task is explained in more detail in subsequent sections, click the task name to jump to those details.

Step	Task	Description	Completed

1	DNS Lookup	Verify that hosts can reach each other using hostnames and IP addresses.
		`# ping -c myhost.mycompany.com // The return code should be 0`
		`# ping -c 3 192.168 . 1.2 // The return code should be 0`	

2	Check JDK	Ensure you're running Oracle Java JDK Version 1.7 on the Admin node. Java version 1.7 is required; 1.7u45 is recommended On the Admin node, as `root`, run: `# /usr/java/default/bin/java -version` If not, download and install the appropriate version from Oracle.	
3	**Package Accessibility**	Verify that all hosts have yum access to an EPEL yum repository. On the Admin node, as `root`, run: `# yum list < LIST_OF_PACKAGES >` See Package Accessibility for more details and a list of packages. Note that this is not required if the required rpms are accessible locally.	

4	Verify iptables is turned off	On the Admin node, as `root`, run:
		`# chkconfig iptables off`
		`# service iptables stop`
		`# service iptables status`
		`iptables: Firewall is not running.`	

5	Disable SELinux	On the Admin node, as `root`, run: `# echo 0 > /selinux/enforce`	

PCC - DNS Lookup

Before you can begin your PCC installation, verify the following:

Verify that the admin host (the host on which you will be installing PCC) is able to reach every host that will be part of your cluster using its hostname and IP address. We also recommend that every cluster node is able to reach every other cluster node using its hostname and IP address:

```
# ping -c 3 myhost.mycompany.com // The return code should be 0
# ping -c 3 192.168.1.2 // The return code should be 0
```

Next Prerequisite: Verify Java JDK version.

PCC - JAVA JDK

Before you begin your installation, ensure that you are running Oracle JAVA JDK version 1.7 on the Admin node and that you are not running OpenJDK as your default JDK.

⚠ Version 1.7 is required; version 1.7u45 is recommended.

Verify JDK Version

Perform the following steps on the Admin node as both `root` and `gpadmin` users:

```
$ /usr/java/default/bin/java -version
```

The output of this command should contain 1.7 (version number) and JavaHotSpot(TM) (Java version). For example:

```
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b18)
Java HotSpot(TM) 64-Bit Server VM (build 24.45-b08, mixed mode)
```

If you are not running the correct JDK, download a supported version from the Oracle site at http://www.oracle.com/technetwork/java/javase/downloads/index.html.

⚠ If you have manually installed UnlimitedJCEPolicy files prior to upgrading your JDK, you will need to re-install them post upgrade.

Install the JDK on the admin node and add it to alternatives as follows:

```
# /usr/sbin/alternatives --install "/usr/bin/java" "java" "/usr/java/jdk1.7.0_xx/bin/java" 3
# /usr/sbin/alternatives --install "/usr/bin/javac" "javac" "/usr/java/jdk1.7.0_xx/bin/javac" 3
# /usr/sbin/alternatives --config java
```

OpenJDK

Make sure you are not running OpenJDK as your default JDK.

If you are running OpenJDK, we recommend you remove it.

To check for all versions of JDK that are running on your system, as `root` run:

```
yum list installed | grep jdk
```

An example output from this command is:

```
java-1.6.0-openjdk.x86_64
java-1.7.0-openjdk.x86_64
jdk.x86_64              2000:1.7.0_45-fcs
```

This indicates that there are three versions of JDK installed, two of them are OpenJDK.

To remove all OpenJDK versions, as `root`, run:

```
yum erase *openjdk*
```

Next Prerequisite: PCC - Verify Package Accessibility

PCC - Verify Package Accessibility

Verify that all packages are available in a local yum repository or that you have yum access to an EPEL yum repository.

Pivotal Command Center and Pivotal HD Enterprise expect some prerequisite packages to be pre-installed on each host, depending on the software that gets deployed on a particular host. In order to have a smoother installation, it is recommended that each host have yum access to an EPEL yum repository. If you have access to the Internet, you can configure your hosts to have access to the external EPEL repositories. However, if your hosts do not have Internet access (or you are deploying onto a large cluster), then having a local yum EPEL repo is highly recommended. This will also give you some control on the package versions you want to deploy on your cluster. See Creating a YUM EPEL Repository, for instructions on how to setup a local yum repository or point your hosts to an EPEL repository.

The following packages need to be either already installed on the admin host or be on an accessible yum repository:

- httpd
- mod_ssl
- postgresql
- postgresql-devel
- postgresql-server
- postgresql-jdbc
- compat-readline5
- createrepo
- sigar
- sudo
- python-ldap
- openldap
- openldap-clients
- openldap-servers
- pam_krb5
- sssd

- authconfig
- krb5-workstation
- krb5-libs
- krb5-server

Run the following command on the admin node to make sure that you are able to install the prerequisite packages during installation:

```
# yum list <LIST_OF_PACKAGES>
```

For example:

```
# yum list httpd mod_ssl postgresql postgresql-devel postgresql-server compat-readline5 createrepo
sigar sudo
```

If any of them are not available, then you may have not correctly added the repository to your admin host.

For the cluster hosts (where you plan to install the cluster), the prerequisite packages depend on the software you will eventually install there, but you may want to verify that the following two packages are installed or accessible by yum on all hosts:

- nc
- postgresql-devel

For the cluster hosts, the following packages need to be accessible if you are deploying in secure mode (the default):

- krb5-libs
- krb5-workstation
- openldap
- openldap-clients
- pam_krb5
- sssd
- authconfig
- openssh-clients
- python-ldap

Next Prerequisite: PCC - Turn Off iptables

PCC - Turn Off iptables

Before you begin your installation, verify that iptables is turned off:

As `root`:

```
# chkconfig iptables off
# service iptables stop
```

Next Prerequisite: PCC - Disable SELinux

PCC - Disable SELinux

Before you being your installation, verify that SELinux is disabled:

As `root`:

```
# sestatus
```

If SELinux is disabled, one of the following is returned:

```
SELinuxstatus: disabled
```

or

```
SELinux status: permissive
```

Disabling SELinux Temporarily

If SELinux status is *enabled*, you can temporarily disable it or make it permissive (this meets requirements for installation) by running the following command:

As `root`:

```
# echo 0 > /selinux/enforce
```

This only temporarily disables SELinux; once the host is rebooted, SELinux will be re-enabled. We therefore recommend permanently disabling SELinux, described below, while running Pivotal HD/HAWQ (however, this requires a reboot).

Disabling SELinux Permanently

You can permanently disable SELinux by editing the `/etc/selinux/config` file as follows:

Change the value for the SELINUX parameter to:

`SELINUX=disabled`

Then reboot the system.

Next Steps: Next Steps: If you need to set up an EPEL Yum repository, do that now, otherwise you should now have met all of the prerequisites, and can now proceed with your PCC Installation.

PCC - EPEL Yum Repository

Pivotal Command Center and Pivotal HD Enterprise expect some prerequisite packages to be pre-installed on each host, depending on the software that gets deployed on a particular host. In order to have a smoother installation, we recommend that each host have yum access to an EPEL yum repository. If you have access to the Internet, then you can configure your hosts to have access to the external EPEL repositories. However, if your hosts do not have Internet access (or you are deploying onto a large cluster) or behind a firewall, then having a local yum EPEL repository is highly recommended. This also gives you some control on the package versions you want to deploy on your cluster.

Following are the steps to create a local yum repository from a RHEL or CentOS DVD:

1. Mount the RHEL/CentOS DVD on a machine that will act as the local yum repository.

2. Install a webserver on that machine (e.g. httpd), making sure that HTTP traffic can reach this machine.

3. Install the following packages on the machine:

```
yum-utils
createrepo
```

4. Go to the directory where the DVD is mounted and run the following command:

```
# createrepo ./
```

5. Create a repo file on each host with a descriptive filename in the /etc/yum.repos.d/ directory of each host (for example, CentOS-6.1.repo) with the following contents:

```
[CentOS-6.1]
name=CentOS 6.1 local repo for OS RPMS
baseurl=http://172.254.51.221/centos/$releasever/os/$basearch/
enabled=1
gpgcheck=1
gpgkey=http://172.254.51.221/centos/$releasever/os/$basearch/RPM-GPG-KEY-CentOS-6
```

6. Validate that you can access the local yum repos by running the following command:

```
# yum list
```

You can repeat the above steps for other software. If your local repos don't have any particular rpm, download one from a trusted source on the internet, copy it to your local repo directory and rerun the `createrepo` step.

Chapter 3 Installation Instructions

This section describes how to install PCC.

- Supported Platforms and Browsers
- PCC Installation Checklist
- Install PCC
- PCC - Importing the Packages
- Launching PCC

Supported Platforms and Browsers

The following platforms and browsers are supported:

Platforms

- RHEL 6.4 64-bit, 6.5 64-bit
- CentOS 6.4 64-bit, 6.5 64-bit

Browsers

(Minimum screen resolution: 1280 x 800)

- Firefox 23
- IE 10
- Chrome 33.0.1750.146

PCC Installation Checklist

The table below briefly describes the steps you need to take to install a cluster; more detailed instructions are provided in Installing PCC.

Note that shaded rows depict operations that you perform via a Browser/PCC UI.

Step	Task	Description	Completed

1	Install Pivotal Command Center	On the Admin node, as `root`, run:
		1. Create a directory (`phd`) on the root home directory of the Admin node for your PCC installation:
		`# mkdir phd`
		2. Copy tar file to your specified directory on the admin node, for example:
		`# scp ./PCC-2.3.x.version.build.os.x86_64.tar.gz host:/root/phd/`
		3. Login as `root` and untar to that directory:
		`# cd /root/phd`
		`# tar --no-same-owner -zxvf PCC-2.3.x.version.build.os.x86_64.tar.gz`
		4. Run the installation script from the directory where it was extracted:
		`#./install`
		5. As the rest of the installation is done as the `gpadmin` user, change to that user:
		`# su - gpadmin`
		6. If necessary, enable Secure Connections (see Enabling Secure Connections for details)	

Step	Task	Description	Completed

2	PCC - Importing the Packages	Download and copy the PHD packages to the Admin node, then import the packages, including a downloaded JDK package, to the Admin node:
		
		(as `gpadmin`)
		
		Copy:
		
		1. Copy the Pivotal HD services (PHD, ADS (HAWQ)) tarballs from the initial download location to the `gpadmin` home directory (`home/user/gpadmin`).
		
		2. Change the owner of the packages to `gpadmin` then untar the tarballs.
		
		For example: If the file is a `tar.gz` or `tgz`, use:
		
		`tar -zxf packagename.tgz`
		
		If the file is a `tar`, use:
		
		`tar -xf packagename.tar`
		
		Import:
		
		Deploy the downloaded JDK to the cluster nodes
		
		`$ icm_client import -r <PATH TO JDK>`
		
		For each service (PHD, ADS) you are importing, run the following:
		
		`$ icm_client import -s <PATH TO EXTRACTED PHD SERVICE TAR BALL>`	

3	**Browser:** **Launch Pivotal Command Center UI** See Launching PCC for more details.	Launch a browser and enter the host on which you installed PCC: `https://CommandCenterHost:5443` The Command Center login page is launched in your browser. The default username/password is `gpadmin`/`Gpadmin1` (case sensitive).	
4	**Browser:** **Configure and deploy a cluster** See Configuring and Deploying a Cluster for more details.	After you have logged in to Pivotal Command Center, the Cluster Status page appears. From here, if you are an administrative user, you are able to launch the **Add Cluster Wizard** that enables you to configure and deploy a Pivotal HD Cluster.	

Step	Task	Description	Completed
5	**Browser:** **Start the cluster** See Starting the Cluster for more details.	Return to the PCC UI and start the cluster from the Cluster Status page.	

6	Initializing and Configuring HAWQ	(as `gpadmin`)
		`ssh` to the HAWQ master, the run the following:
		`$ source /usr/local/hawq/pivotal_path.sh`
		`$ /etc/init.d/hawq init`
		
		If you have a HAWQ standby master configured, initialize that:
		
		`$ gpinitstandby -s <STANDBY HAWQ MASTER FQDN>`	

Install PCC

Perform the following installation steps as a `root` user.

Avoid using hostnames that contain capital letters because Puppet has an issue generating certificates for domains with capital letters.

Avoid using underscores, as they are invalid characters in hostnames.

1. Download the PCC package from Pivotal Network .
2. As `root` on the Admin node, create a directory (`phd`) for your PCC installation on the Admin node:

```
# mkdir phd
```

3. Copy the Pivotal Command Center tar file to the Admin node, for example:

```
# scp ./PCC-2.3.x.version.build.os.x86_64.tar.gz host:/root/phd/
```

4. As `root`, `cd` to the directory where the Command Center tar files are located and untar them. For example:

```
# cd /root/phd
# tar --no-same-owner -zxvf PCC-2.3.x.version.build.os.x86_64.tar.gz
```

5. Still as `root` user, run the installation script. This installs the required packages, configures Pivotal Command Center, and starts services.

   Important

   You must run the installation script from the directory where it was extracted; for example: For example: `PCC-2.3.x.version`

   For example:

   ```
   # cd PCC-2.3.x.version
   # ./install
   ```

   You will see installation progress information on the screen.

   You are given the option via a prompt during installation to specify a custom home directory for `gpadmin`. Before you deploy a cluster make sure that this home directory is consistent across all cluster hosts.

   Once the installation successfully completes, you will receive an installation success message on your screen.

6. Enable Secure Connections (optional):
   Pivotal Command Center uses HTTPS to secure data transmission between the client browser and the server. By default, the PCC installation script generates a self-signed certificate.

   Alternatively, you can provide your own Certificate and Key by following these steps:

   a. Set the ownership of the certificate file and key file to `gpadmin`.

   b. Change the permission to owner read-only (mode 400)

   c. Edit the `/etc/httpd/conf.d/pcc- vhost.conf` file and change the following two directives to point to the location of the ssl certificate and key, for example:

      `SSLCertificateFile`: `/usr/local/pivotal-cc/ssl/<servername>.cert`

      `SSLCertificateKeyFile`: `/usr/local/pivotal-cc/ssl/<servername>.key`

   d. Restart PCC by running:

      ```
      # service commander restart
      ```

      See SSL Certificates for details

7. Verify that your PCC instance is running:

```
# service commander status
```

The PCC installation you just completed includes a CLI (Command Line Interface tool: `icm_client`). You can now deploy and manage the cluster using this CLI tool.

You can switch to the `gpadmin` user (created during installation) for the rest of the installation process:

```
$ su - gpadmin
```

If, during the installation of PCC, you receive a facter mismatch error such as the following:

```
PCC-2.3.0-175]# rpm -ev facter

error: Failed dependencies:

facter >= 1.5 is needed by (installed) puppet-2.7.9-1.el6.noarch
```

Remove facter using the command:

```
yum erase facter
```

Then run the PCC installation again.

PCC - Importing the Packages

Once you have Pivotal Command Center installed, you can use the `import` option of the `icm_client` tool to synchronize the PHD service RPMs and a downloaded JDK package from the specified source location into the Pivotal Command Center (PCC) local yum repository of the Admin Node. This allows the cluster nodes to access the packages during deployment.

If you need to troubleshoot this part of the installation process, see the log file located at: `/var/log/gphd/gphdmgr/gphdmgr-import.log`

Import JDK

Note that having JDK 1.7 running on the Admin node is a prerequisite. This step is to import a downloaded JDK package that will be deployed across the cluster.

1. Download a supported JDK package from http://www.oracle.com/technetwork/java/javase/downloads/index.html.
   PHD expects an rpm package, for example: jdk-7u45-linux-x64.rpm

2. Import the downloaded JDK package to the cluster nodes:
   As `gpadmin`, run:

   ```
   $ icm_client import -r <PATH TO JDK>
   ```

Copy the PHD Service Packages

1. Download the PHD service packages (PHD, and optionally ADS and PRTS) from the Pivotal Network.

2. Copy the Pivotal HD, and optionally ADS (HAWQ) and PRTS (GemFire) tarballs from your initial download location to the `gpadmin` home directory on the Admin node (`home/gpadmin`).

3. Change the owner of the packages to `gpadmin` and untar the tarballs. For example:

```
# For PHD: If the file is a tar.gz or tgz, use
$ tar zxf PHD-2.1.x-<BUILD>.tar.gz

# If the file is a tar, use
$ tar xf PHD-2.1.x-<BUILD>.tar

# For Pivotal ADS: If the file is a tar.gz or tgz file, use
$ tar zxf PADS-1.2.x-<BUILD>.tar.gz

# If the file is a tar, use
$ tar xf PADS-1.2.x-<BUILD>.tar

# For PRTS: If the file is a tar.gz or tgz file, use
$ tar zxf PRTS-1.x.x-<BUILD>.tar.gz

# If the file is a tar, use
$ tar xf PRTS-1.x.x-<BUILD>.tar
```

Import PHD Service

1. As `gpadmin`, import the following tarball for Pivotal HD:

```
$ icm_client import -s <PATH_OF_EXTRACTED_PHD_PACKAGE>
```

For example:

```
$ icm_client import -s PHD-2.0.x-x/
```

Import HAWQ/PXF Services

Optional for HAWQ/PXF users.

As `gpadmin`, import the following tarballs for HAWQ and PXF:

```
$ icm_client import -s <PATH_OF_EXTRACTED_ADS_PACKAGE>
```

For example:

```
$ icm_client import -s PADS-1.2.x-x/
```

Import PRTS (GemFire) Service

Optional for GemFire users.

As `gpadmin`, import the following tarball for PRTS:

```
$ icm_client import -s <PATH_OF_EXTRACTED_PRTS_PACKAGE>
```

For example:

```
$ icm_client import -s PRTS-1.x.x-x/
```

You are now ready to configure and deploy a cluster from the Pivotal Command Center UI. See Using PCC for details.

Launching PCC

To launch the PCC UI:

Start a browser and navigate to the host on which you installed Command Center. For example:

```
https://CommandCenterHost:5443
```

The Command Center login page is launched in your browser. The default username/password is `gpadmin`/`Gpadmin1` (case sensitive).

Starting, Stopping, and Restarting Command Center Services

To stop or restart Command Center services, as `root` run the following commands on the Pivotal Command Center admin host:

```
# service commander stop
```

```
# service commander start
```

```
# service commander restart
```

These commands need to be run as `root`.

Next Steps

See Using PCC for details about using the application, including how to change the default password and how to deploy and configure a HD cluster via the Command Center UI.

See *PHD Installation and Administration* for instructions for using the command-line interface (CLI) of Pivotal Command Center to deploy and configure a HD cluster.

Chapter 4 Uninstalling PCC

Follow the steps below to uninstall Pivotal Command Center and the Pivotal HD cluster:

1. As `gpadmin`, stop services on all your clusters (See the *Pivotal HD Enterprise Installation and Administrator Guide* for detailed steps).
2. As `gpadmin`, uninstall all your clusters (See the *Pivotal HD Enterprise Installation and Administrator Guide* for detailed steps).
3. From the directory where you untarred the Pivotal Command Center, run the uninstall script as `root`:

   ```
   # cd /root/phd/PCC-2.x.x.version/
   ```

   ```
   # ./uninstall
   ```

Chapter 5 Upgrading PCC

The following instructions are for upgrading Pivotal Command Center from version 2.2.x to 2.3.

Upgrade Notes

- If you are upgrading to a new version of Pivotal Command Center, make sure you are running compatible versions of Pivotal HD and Pivotal ADS (optional).
- See the latest version of the Pivotal Command Center Release notes for Pivotal Interoperability Matrix.
- You don't have to stop your cluster to upgrade PCC, it can be either running or stopped.

Upgrading PCC should be performed as part of an overall PHD Enterprise upgrade. You should refer to the *PHD Enterprise Installation and Administrator Guide* for more comprehensive upgrade instructions including recommended housekeeping steps you should take prior to an upgrade, such as verifying the state of your cluster.

Follow the steps below to upgrade your PCC to a newer version:

1. Download the new PCC file from Pivotal Network.
2. Copy the new PCC tar file to your installation directory on the admin node, for example:
   ```
   $ scp ./PCC-2.3.x. version.build.os .x86_64.tar.gz host:/root/phd/
   ```
3. Login as `root` and untar to that directory:
   ```
   $ cd /root/phd
   $ tar --no-same-owner -zxvf PCC-2.3.x. version.build.os .x86_64.tar.gz
   ```
4. As `root`, run the PCC installation script from the directory where it is installed:
   ```
   $ ./install
   ```

   There is no need to specify that this is an upgrade; the install utility (`./install`) detects whether it is a fresh install or an upgrade.

5. Make sure that `nmon` is running:
   To check `nmon` status:

   ```
   # service nmon status
   ```

   To start `nmon`:

   ```
   # service nmon start
   ```

⚠ Following an upgrade, the former contents of `/usr/local/config` can be found in `/usr/local/config.bak`.

Chapter 6 Using PCC

This section provides instructions for using the PCC UI.

- PCC UI Overview
- Logging In
- PCC UI Settings
- PCC UI User Management
- Cluster Status Page
- Configuring and Deploying a Cluster
- Starting, Stopping, and Uninstalling a Cluster
- PCC UI Dashboard
- Cluster Analysis
- MapReduce Job Monitor
- Yarn App Monitor
- HAWQ Query Monitor
- Topology
- Logs

PCC UI Overview

Pivotal Command Center UI is a browser-based application for configuring, deploying, administering, and monitoring Pivotal HD clusters. At a high level, the screens consist of:

- Cluster Status Page—Provides status information about any clusters you have configured and deployed. Also provides access to the Add Cluster Wizard that allows you to configure and deploy clusters from the UI. See Configuring and Deploying a Cluster for more details.
- Dashboard—Provides an overview of your Pivotal HD cluster. This screen shows at one glance the most important states and metrics that an administrator needs to know about the Pivotal HD cluster.
- Cluster Analysis—Provides detailed information about various metrics of your Pivotal HD cluster. This provides cluster-wide metrics all the way down to host-level metrics.
- MapReduce Job Monitor—Provides details about all, or a filtered set of MapReduce jobs.
- YARN App Monitor—Provides details about all, or a filtered set of YARN applications.
- HAWQ Queries—When HAWQ (a revolutionary MPP database on Hadoop solution) is deployed on the cluster, Command Center can show the progress of all actively running queries on HAWQ.
- Topology—This screen shows you what roles have been installed on each host. You can also add and remove slaves to/from the cluster from this screen.
- Logs—This screen displays system logs based on filter criteria you select such as log levels, host name, time period, and so on.

Status indicators

Throughout the user interface the following indicators are used to indicate the status of nodes:

- Green: Succeeded
- Blue: Running
- Grey: Stopped/Pending
- Red: Killed/Failed

Logging In

Launch a browser and navigate to the host on which you installed Command Center. For example:

```
https://CommandCenterHost:5443
```

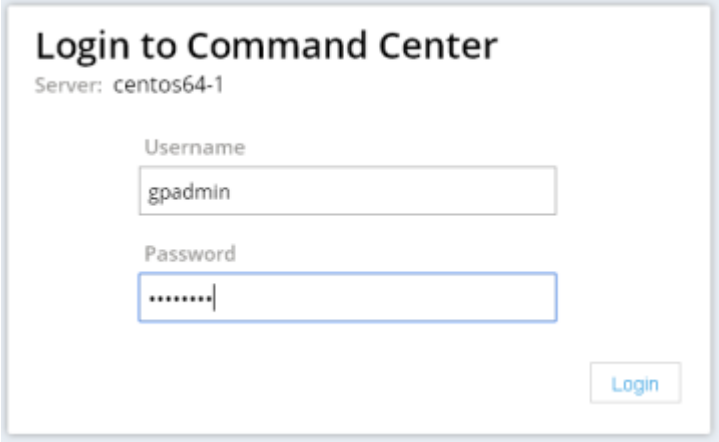
The Command Center login page is launched in your browser. The default username/password is `gpadmin`/`Gpadmin1` (case-sensitive).

To change the default port (5443), update the port settings in the following file:

```
/usr/local/pivotal-cc/config/app.yml
```

Login Screen

The first time you launch the Command Center UI, a login screen appears showing the hostname of this instance of Pivotal Command Center.



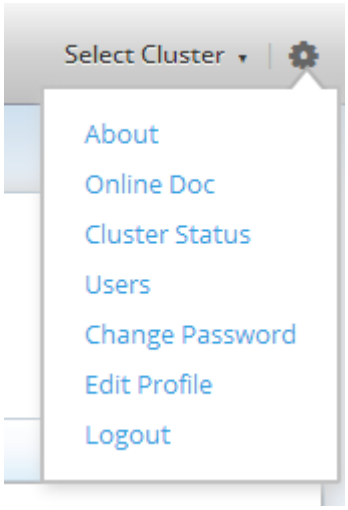
The default admin username/password is `gpadmin`/`Gpadmin1` (case-sensitive). You can change this password via the Settings menu.

Passwords are case-sensitive and must be at least 8 letters long and contain 1 upper-case letter and 1 number.

Once you have entered a valid username/password, click the **Login** button to launch the Command Center UI.

PCC UI Settings

Once you have logged in, you can click the gear icon in the upper right corner of the screen from any PCC page to display the **Settings** menu.



From the settings menu you can select one of:

- **About**. Select this to display version information about this instance of PCC
- **Online Doc**. Select this to link to Pivotal's product documentation home page.
- **Cluster Status**. Select this option to go back to the Cluster Status page to view the list of available clusters.
- **Users**. Select this option to add/edit user information. There are two types of users, administrative and non-administrative (read-only); you will only see this **Users** option if you are an administrative user. See **Users**.
- **Change Password**. Click this to change your password. See Passwords.
- **Edit Profile**. Click this to change your profile. See **Users**.
- **Logout**. Select this option to logout from this instance of PCC.

PCC UI User Management

There are two types of users, administrative (super user) and non-administrative (read-only).

If you are an administrative user, you can add users, edit your own or other users' profiles, change your own or other users' passwords, and delete users.

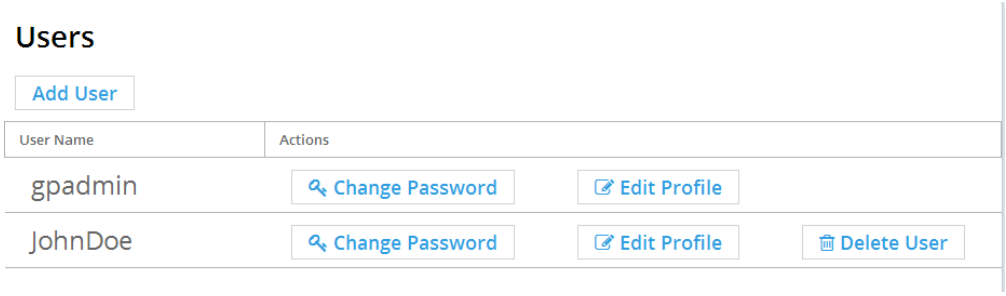
⚠ Non-administrative users are read-only users; their actions are limited to read-only actions.

⚠ For many user management actions, you will be asked to **Re-authenticate to Continue**. In all cases, this means you need to enter the password of the current user performing the action to continue.

Users

You will only see the **Users** option in the **Settings** menu if you are an administrative user.

Select **Users** from the **Settings** menu to see a list of all current users:



Adding a User

1. Click **Add User** to create a new user.

   A New User form appears. Enter the following information about the new user:

   - **First Name**.
   - **Last Name**.
   - ***User Name**. This must be a unique name. (For adding an LDAP user, see below.)
   - **Email**. Must be a valid email address.
   - **Administrator**. Check this box if the new user is to have administrative privileges.
   - **Password**. Enter a password for the new user. This must meet the minimum password requirements. Passwords are case-sensitive and must be at least 8 letters long and contain 1 upper-case letter and 1 number.
   - **Confirm Password**. Confirm the new user's password.

2. Click **OK**.
   A dialog box appears asking you to **Re-authenticate to Continue**.

3. Enter the password of the current user (the administrative user who is creating the new user).

4. Click **OK**.

You are returned to the Users screen where you should now see your new user(s) in the list.

***Adding a New LDAP User**

If your instance of PCC has been set up to use an existing LDAP server for user authentication (see Configuring PCC for LDAP), you will see a **Check username** link adjacent to the Username field. Click this link to see if the username you are attempting to add exists in the LDAP server; if it does, the rest of the fields, except the Password field, are populated with data from LDAP. Once this user has been added, he/she can log into PCC using their LDAP username and password.

Deleting a User

Only administrative users can delete users and the default `gpadmin` user can never be deleted. To delete a user:

1. Select **Users** from the **Settings** menu

2. Click the **Delete User** link adjacent to the user you want to delete.
   A dialog box appears asking you to Re-authenticate to Continue.

3. Enter the password of the current user (the administrative user who is deleting the user).

4. Click **OK**.

You are returned to the Users screen where the user you just deleted should no longer appear in the list.

Profiles

Your profile includes: First Name, Last Name, User Name, Email Address, and User Type (administrative or not); it does not include your password.

All users can edit their own profiles by:

- Selecting **Edit Profile** from the **Settings** menu.

Administrative users can edit their own passwords and also the profiles of other users by:

- Selecting **Users** from the **Settings**, then clicking the **Edit Profile** link adjacent to the user whose profile they wish to edit.

After making edits to any profile, a dialog box appears asking you to **Re-authenticate to Continue**. Enter the password of the current user making the edits to continue, then click **OK**.

Passwords

Passwords are case-sensitive and must be at least 8 letters long and contain 1 upper-case letter and 1 number.

All users can change their own passwords by:

- Selecting **Change Password** from the **Settings** menu.

Administrative users can change their own passwords and also the passwords of other users by:

- Selecting **Users** from the **Settings** menu, then clicking the **Change Password** link adjacent to the user whose password you wish to change.

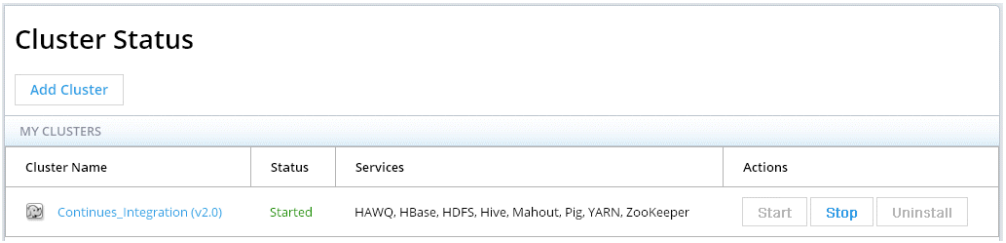
After changing any password, a dialog box appears asking you to **Re-authenticate to Continue**. Enter the password of the current user making the edits to continue, then click **OK**.

For LDAP Users: If you modify a password in PCC, the modified password is stored in PCC only. The password in LDAP is not changed.

Cluster Status Page

Once you have launched Command Center, the initial screen you see is the Cluster Status screen. This displays a list of available clusters to monitor, the status of each cluster (**started**, **stopped**), and a list of services running on that cluster (Hive, Mahout, and so on).

The **Add Cluster** and **Actions** buttons are only visible to administrative users.



From this page you can:

- Administrative users only: Click **Add Cluster** to launch the Add Cluster Wizard.
- Click the cluster name in the table to view the Dashboard for that cluster.
- From any point within Command Center UI, you can always select a different cluster by using the **Select Cluster** drop-down menu in the upper right corner of the screen.
- Administrative users only: You can either **Start**, **Stop**, or **Uninstall** a cluster. Depending on the state of the cluster, some of these buttons will be enabled while others are disabled.

Configuring and Deploying a Cluster

This section describes how to use the Add Cluster Wizard to configure and deploy a cluster:

- Launching the Add Cluster Wizard
- Create Cluster Definition
- Versions, Services, and Hosts
- Host Verification
- Cluster Topology
- Cluster Configuration
- Validation
- Deployment Status
- Summary
- Starting the Cluster from the UI
- Initializing and Configuring HAWQ

Launching the Add Cluster Wizard

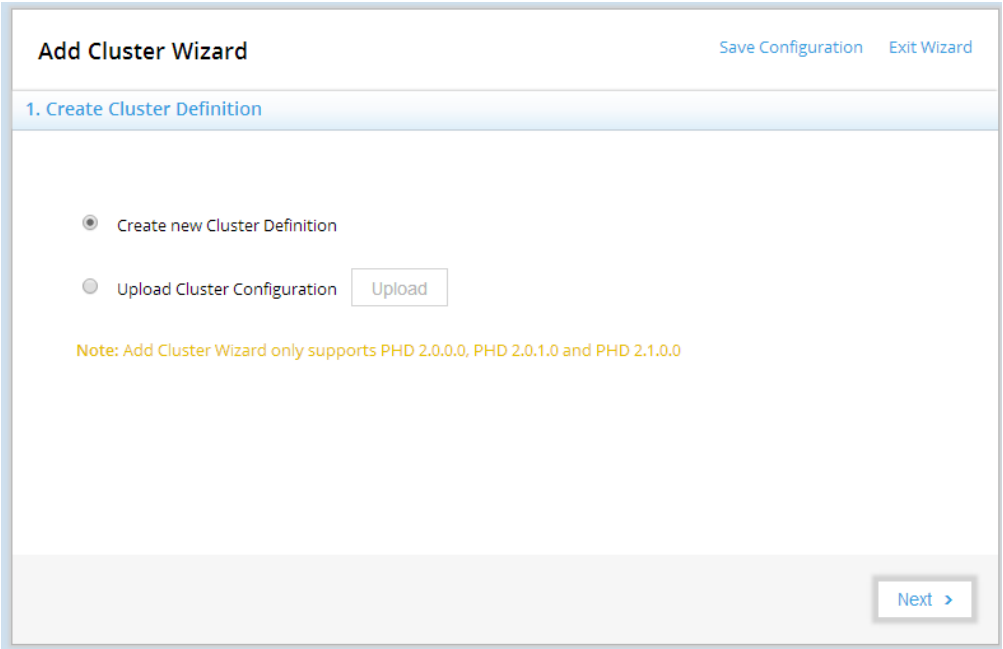
Before you can configure and deploy a cluster, make sure you have already installed the PHD Services using the CLI (`icm_client`) (see Installation Instructions for details).

After you have logged in to Pivotal Command Center, the Cluster Status page appears. From here, if you are an administrative user, you are able to launch the **Add Cluster Wizard** that enables you to configure and deploy a Pivotal HD Cluster.

Clusters deployed via Pivotal Command Center are High Availability enabled by default, and are not secured. You can manually disable High Availability or secure a cluster via the command line; refer to the *PHD Enterprise Installation and Administrator Guide* for instructions.

As you move through the wizard, the right hand pane displays where you are in the deployment process:

Click **Add Cluster**. The Add Cluster Wizard opens:



The Wizard allows you to create a new configuration from scratch or upload and edit any existing configuration. The Summary panel along the right shows you the progress of your configuration and deployment.
As noted on the Cluster Wizard screen, the **Add Cluster Wizard** only supports PHD 2.0.x and PHD 2.1

Click **Next**.

Next Step: Create Cluster Definition

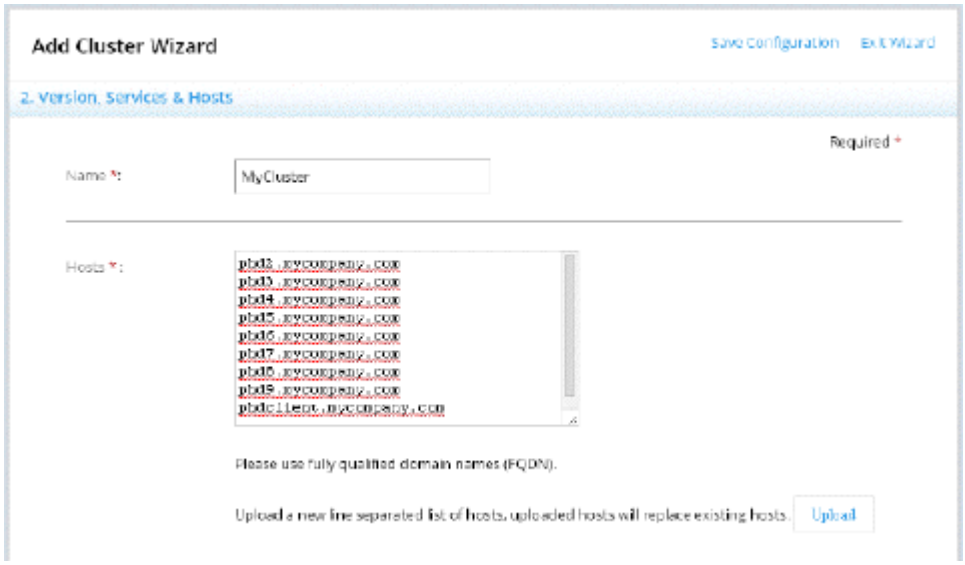
Create Cluster Definition

Either:

1. If you are configuring a new cluster, select **Create a new Cluster Definition** then click **Next**.
2. If you want to edit an existing cluster; select **Upload Cluster Configuration**,click **Upload**, then navigate to the `clusterConfig.xml` file that you wish to edit; then click **Next**. In this case, the following fields in the Wizard will be populated with the cluster definition properties of that `clusterConfig.xml` file you just uploaded. Follow the instructions below to edit those values.

Next Step: Versions, Services, and Hosts

Versions, Services, and Hosts



Notes

- Hosts can be entered individually, newline-separated; or can be expressed in a range, for example `host[1-5].yourdomain.com`. They can also be expressed in multiple ranges, for example `host[1-3].subdomain[1-2].yourdomain.com`. Any hosts expressed in ranges are expanded during host verification. Hosts that do not exist within a specified range will be ignored, so you can specify a wide range and only those hosts that are available within that range will be added.
- If you are editing an existing configuration, some, if not all, of these fields will be pre-populated. Edit where appropriate.
- You need to scroll down to view all the fields on this screen. The **Next** button will not be active until you have entered all the required fields.

Enter the following information:

- **Name**: Required. Enter a name for this cluster. Special characters are not supported.
- **Hosts**: Required. Enter a new line-separated list of FQDN host names. You can also click **Upload** to use a text file containing a new line-separated list of host names.
- **Root Password**: Required. Enter the root password.
- **GP Admin Password**: Required. Enter the `gpadmin` user password. PCC creates this user on all nodes.
- **JDK Path**: Enter the JDK filename (not the absolute path). For example: `jdk-7u51-linux-x64.rpm` .

Note: JDK 1.7.0_15 (min) is a prerequisite.
If not already installed, you should download it then install using `icm_client import -r (see OLD Installing PCC for more details)`

- **Setup NTP**: Check this box if you want to set up NTP (Network Time Protocol).
- **Disable SELinux**: Check this box if you want to disable SELinux. Recommended.
- **Disable IPTables**: Check this box if you want to disable IPTables. Recommended.
- **Run ScanHosts**: Leave this box checked if you want to run scanhosts. The scanhosts command verifies the prerequisites for the cluster node have been met and provides a detailed report of any missing prerequisites. Running this command ensures that clusters are deployed smoothly and is strongly recommended.

  Click **Next**.

Next step: Host Verification

Host Verification

The Host Verification page opens. This step may take a few minutes, it verifies connections to the hosts you just set up. Once the **Eligibilty** field changes from **Pending** to **Eligible** for all hosts, you can click **Next**. You will see any error and informational messages displayed in the comments fields.

 If you specified hosts using ranges, they will be expanded at this point.

Next Step: Cluster Topology

Cluster Topology

This is the section where you specify the roles to be installed on the hosts. For example, you can specify where your hadoop Name Node, Data Node and so on, should be installed. Note that all mandatory roles should have at least one host allocated.

Each service has its own section on this page; you can use the top menu options as shortcuts to those sections on the page, or simply scroll down to each section. Click **Clear** to clear your entries for each service.

Notes

- You need to click **Enter** or **Tab** before each field is accepted. Once you enter the text and click **Enter** or **Tab**, the text will change appearance and appear enclosed in a box, as shown in the figure below. The entry on the left has been accepted, the entry on the right has not.

- Hosts can be specified in ranges, see the notes for **Versions, Services and Hosts**, for more information.
- At any point during this stage you can click **Save Configuration** at the top right of the page. This saves the configuration file and downloads it. Once saved, a link to the configuration file appears at the bottom of the page. Click that link to open and view the `clusterConfig.xml` file. You cannot edit this xml file directly.

These are the roles that need to have installation nodes defined:

- **CLIENTS**: The Pig, Hive, HBase, and Mahout libraries are installed on this host
- **HDFS**: Name Node, Standby Name Node, Journal Node, and Data Nodes
- **YARN**: Resource Manager, History Server, Node Managers
- **HBase**: Hbase Master, HBase Region Servers (note that you can click **Copy from HDFS** to copy the hosts you specified for HDFS)
- **Hive**: Hive Master, Hive Metastore
- **Zookeeper**: Zookeeper Server
- **HAWQ**: Hawq Master Node, Hawq Standby Node, Hawq Segment Nodes (note that you can click **Copy from HDFS** to copy the hosts you specified for HDFS)
- **GFXD** (GemFireXD): GFXD Locator Node, GFXD Server Node
- **PXF**: PXF Server. PXF hosts should contains Name Node (both Active & Standby) and all the Data Nodes.
- **Mahout**: No hosts to configure. Installed on the client host. Click the checkbox to install.
- **Pig**: No hosts to configure. Installed on the client host. Click the checkbox to install.

⚠ HAWQ and GFXD services are both memory intensive and it is best to configure these services to be deployed on different nodes.

Click **Next** once you have finished role-mapping.

Next Step: Cluster Configuration

Cluster Configuration

This page displays a list of all configuration files that define this cluster; the `clusterConfig.xml` (to edit service configuration global values) as well as the service specific configuration files.

All these configuration files are already populated with the values you have already entered; or with default values.

Click any file name to open that configuration file in an editor and enter/edit values.

If you make any changes, click **Save** to return to the Cluster Configuration page.

Once you have completed all your edits, click **Next**.

Next Step: Validation

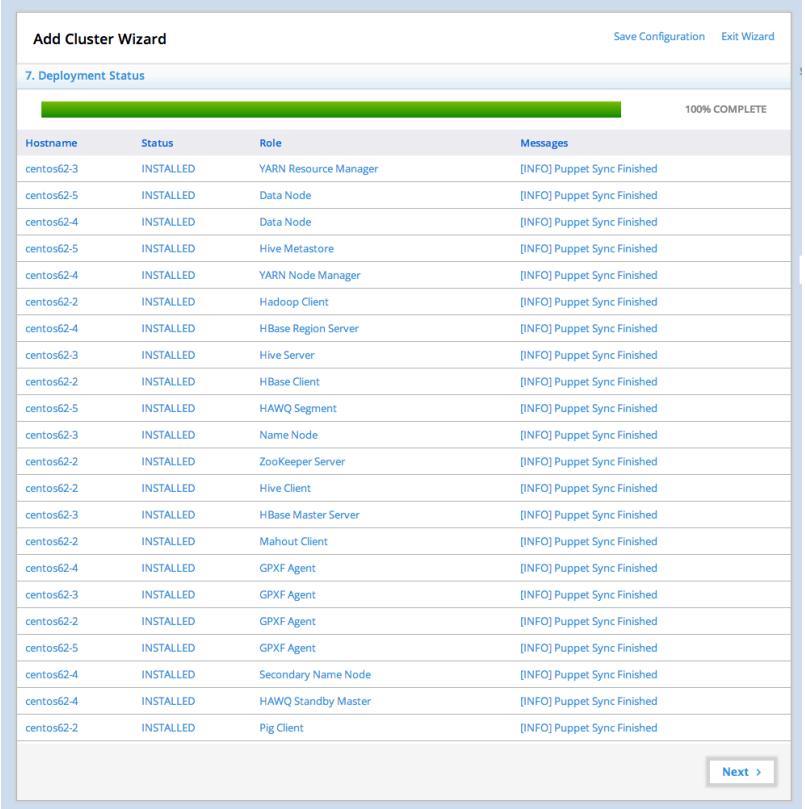
Validation

If the configuration has errors they will be displayed here; otherwise you will see post-deployment instructions.

Click **Deploy**

Next Step: Deployment Status

Deployment Status



This screen shows the progression of the deployment. Information displayed includes:

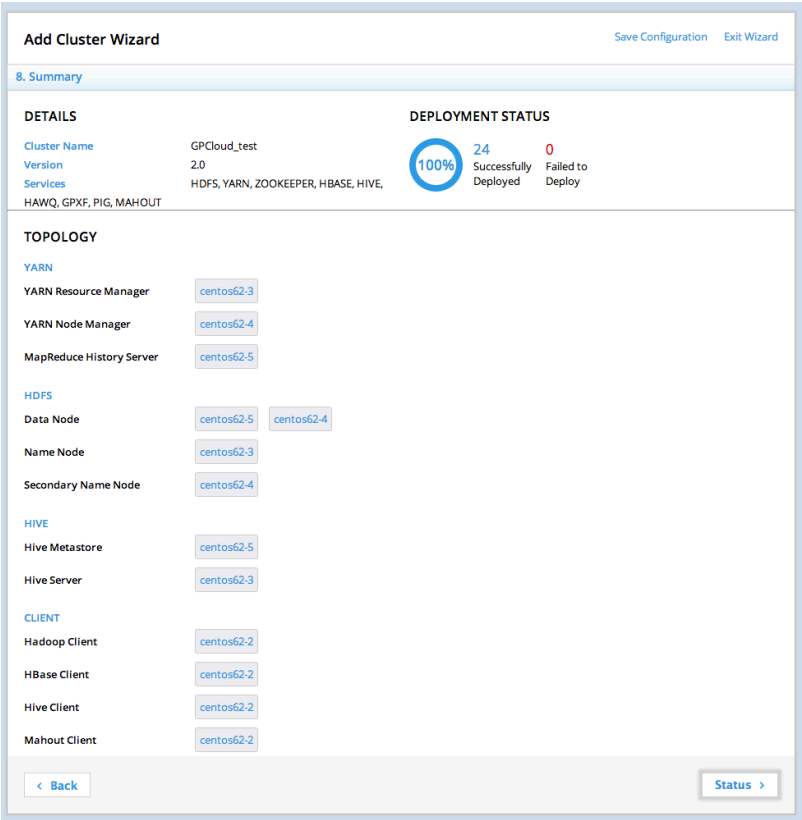
- **Hostname**
- **Status**
- **Role**
- **Messsages**

Once the deployment is complete, click **Next**.

Next Step: Summary

Summary

Once your cluster has successfully deployed, you can view a summary of the cluster, as shown here:



Once you have reviewed this summary, click **Status**, to return to the Cluster Status page. Your new cluster will be listed on this page, with the status of **installed**.

Next Step: Starting the Cluster from the UI

If you are deploying HAWQ you need to initialize and configure HAWQ after you start the cluster. See Initializing and Configuring HAWQ .

Starting the Cluster from the UI

To start your cluster; click **Actions**: **Start** on the Cluster Status page.

Initializing and Configuring HAWQ

For HAWQ users:

`ssh` to the HAWQ master, then as `gpadmin`, run the following:

```
    su - gpadmin
```

```
$ source /usr/local/hawq/greenplum_path.sh
```

```
$ /etc/init.d/hawq init
```

Add the IP address of your instance of Command Center to HAWQ's `pg_hba.conf` file, for example:

```
$ vi /data1/master/gpseg-1/pg_hba.conf

host all gpadmin <Command_center host IP>/24 trust
```

Then restart HAWQ:

```
$ /etc/init.d/hawq restart
```

You have now completed your cluster configuration and deployment.

Starting, Stopping, and Uninstalling a Cluster

These functions are only available to administrative users, also, depending on the state of the cluster, some of these buttons will be enabled while others are disabled.

Starting

To start a cluster:

From the Cluster Status page locate the cluster you want to start, then click the **Actions**: **Start** button.

Stopping

To stop a running cluster:

From the Cluster Status page locate the cluster you want to stop, then click the **Actions**: **Stop** button.

Uninstalling

Only stopped clusters can be uninstalled.

To uninstall a cluster:

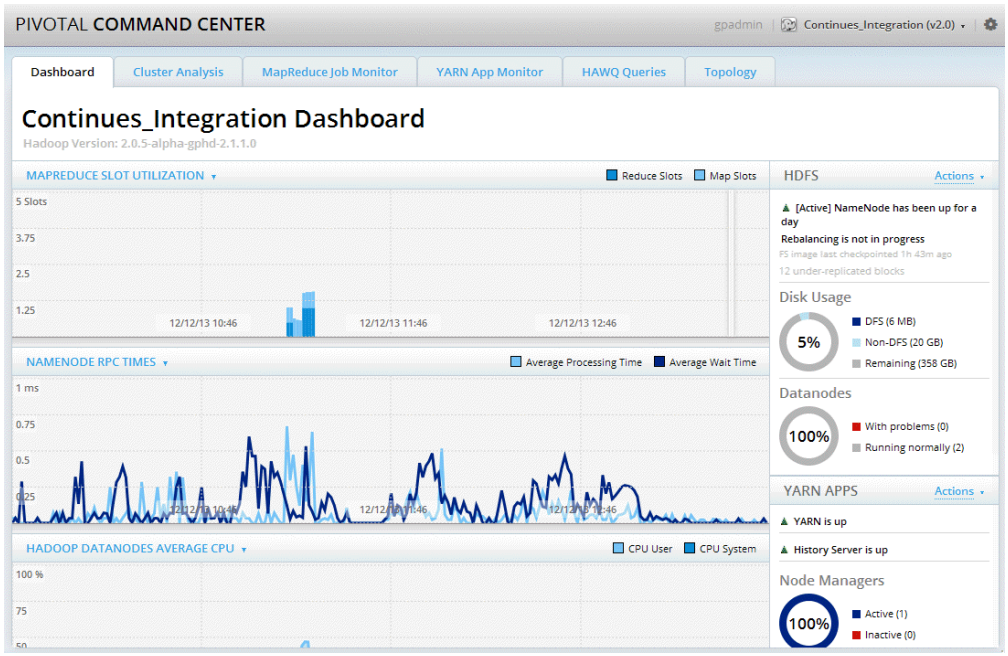
1. From the Cluster Status page locate the cluster you want to uninstall, then click the **Actions**: **Uninstall** button.
2. An Uninstall confirmation dialog appears. Click **Yes** to confirm you want to uninstall this cluster; **No** to cancel the operation and return to the Cluster Status page.
3. Once you confirm you want to continue with the uninstall operation, a Preserve Cluster State dialog appears. You need to specify whether you want to preserve the data for this cluster. Your options are:
   Cancel. This cancels the operation and returns you to the Cluster Status page.
   Yes. This preserves the data for this cluster before uninstalling the cluster and returning you to the Cluster Status page.
   No. This uninstalls the cluster without preserving the data; then returns you to the Cluster Status page.

PCC UI Dashboard

The dashboard gives you a high level view of a cluster at a glance.

You are able to view the status of the most important cluster services, such as HDFS and YARN, and can start and stop each service individually. It also shows you how the most important cluster metrics are trending in a visual way.

The graphs provide a unified view of the state of your system. They are also useful in detecting outliers and pinpointing specific problems that may be present in your system.



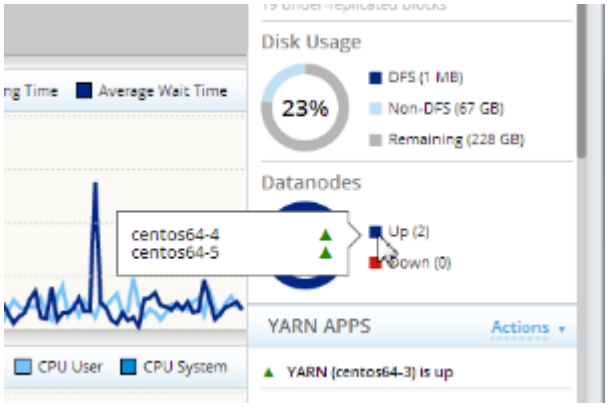
The main portion of the Dashboard displays graphs that provide metrics over time for:

- Mapreduce Slot Utilization
- Namenode RPC Times
- Hadoop Datanodes Average CPU
- Hadoop Datanodes Average Bandwidth
- Namenode Operations Per Second
- Hadoop Datanodes Average Disk Bandwidth
- Hadoop Datanodes Average Memory
- Mapreduce Jobs By Status

Hover over the timeline to see a snapshot of the metrics at that given time.

The right side of the Dashboard displays the state of the following services, provided they have been deployed for this cluster.

Hover over a role to see a list of the relevant nodes, and their statuses, for that role. For example in this cluster there are two datanodes, **centos64-4** and **centos64-5**, both have a status of **up** (running).



The right status pane also displays what the host name for each role, appearing in parenthesis after the role name. For example, in the above screenshot, the hostname for YARN role is **centos64-3**.

HDFS

For HDFS, the dashboard provides the following information/functionality:

- The status of HDFS. You can use the **Actions** dropdown menu to **Start**/**Stop HDFS** depending on its status.
- When the last NameNode checkpoint occurred.
- The percentage of cluster storage being used by HDFS and how much is free.
- The number of DataNodes that are up and whether they are running normally or with problems (hover over to see list of nodes and their statuses)
- The **Actions** dropdown menu allows you to **Rebalance** (redistribute your data across the cluster) your cluster, and to **View Rebalancer Log**.

⚠ The only **Action** option available to non-administrative users is to **View Rebalancer Log**.

⚠ If High Availability (HA) is enabled for your cluster, you will see the status of two NameNodes here.

YARN

For YARN, the dashboard provides the following information:

- The status of YARN. You can use the **Actions** dropdown menu to **Start**/**Stop YARN** depending on its status (not available for non-administrative users).
- Whether or not the YARN History Server is running. Note: The History Server stores a history of the mapreduce jobs run on the cluster.
- The number of Node Managers that are running (hover over to see list of nodes and their statuses).

HBase

For HBase, the dashboard provides the following information:

- The status of the HBase master. You can use the **Actions** dropdown menu to **Start**/**Stop HBase** depending on its status (not available for non-administrative users).
- The number of Region Servers that are running (hover over to see list of nodes and their statuses).

Hive

For Hive, the dashboard provides the following information:

- The status of Hive. You can use the **Actions** dropdown menu to **Start**/**Stop Hive** depending on its status (not available for non-administrative users).

Zookeeper

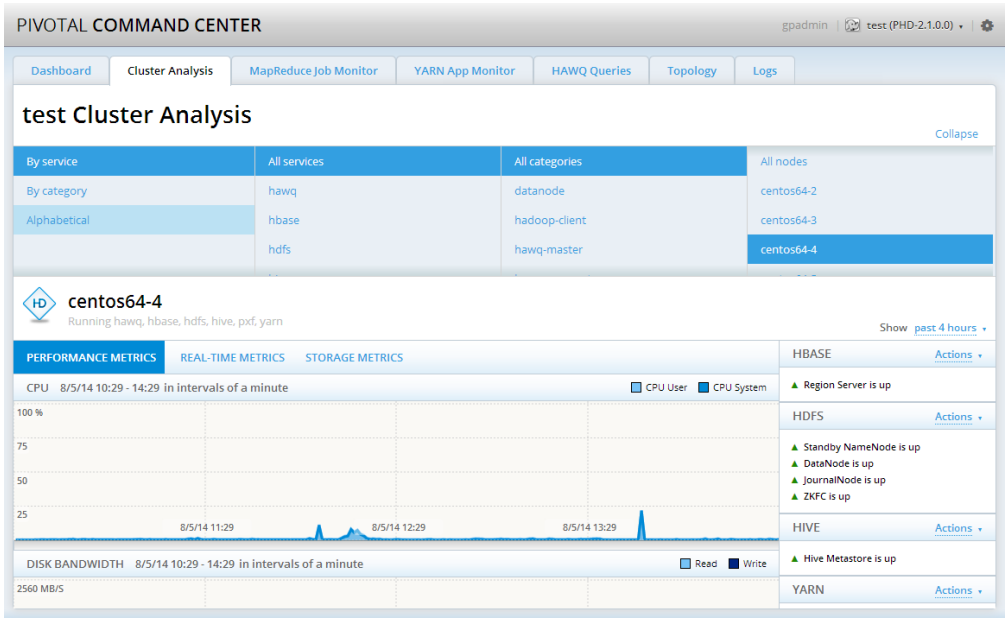
For Zookeeper, the dashboard provides the following information:

- The status of Zookeeper. You can use the **Actions** dropdown menu to **Start**/**Stop Zookeeper** depending on its status (not available for non-administrative users).
- The Status of the Zookeeper server host.

Cluster Analysis

The Cluster Analysis screen provides detailed metrics about your Pivotal HD cluster.

It provides cluster-wide metrics all the way down to host-level metrics. It provides Hadoop-specific metrics, as well as system metrics that you can drill down to if needed.



Filtering the Cluster Analysis Screen

By default the Cluster Analysis screen displays the metrics for all services, all categories, and all nodes. The top portion of the Cluster Analysis screen allows you to filter the information displayed by combinations of several filters. You can **Collapse** or **Expand** this portion of the screen to hide/show the filter selections.

By Service. Metrics can be filtered by services. Select either **All services** (the default), or anyone of the listed services (hawk, hbase, hdfs, and so on). If you filter by one service, for example hawq, the subsequent categories filters are limited to those associated with the selected service (hawq). Once you have selected the services you want to filter by, you can further filter these results to show metrics from **All nodes** (the default), or by any specific node (only those nodes defined for the selected category are displayed).

By Category. Metrics can be filtered by categories such as:

- namenode
- secondarynamenode
- datanode
- yarn-resourcemanager

- yarn-nodemanager
- mapreduce-historyserver
- hawq-master
- hawq-segment

Once you have selected the category you want to filter by, you can further filter these results to show metrics from **All nodes** (the default), or by any specific node (only those nodes defined for the selected category are displayed).

Alphabetically. Metrics can be filtered alphabetically, either for **All nodes** (the default), or for a selected node.

Cluster Metrics

The bottom half of the Cluster Analysis screen displays cluster metrics based on the filters you selected.

Filter by Time

You can further filter these metrics based on a time range. Use the **Show** dropdown menu to limit the metrics displayed here to a specifc time range, either over the **past 4 hours** (the default range); or any of the other available time ranges, from one hour, to the past 8 weeks.

Performance Metrics

Select the **Performance Metrics** tab to display the cluster/node utilization over time.

You can see performance metrics over time for:

- CPU
- Disk Bandwidth
- Network Bandwidth
- Memory
- Load
- Swap Usage
- Swap I/O
- Network Operations
- Disk Operations

Hover over any one of the graphs to see a snap shot of those specific performance metrics at any given time.

⚠ If your instance of Command Center is monitoring two clusters and if any of either cluster's Performance Metrics graphs shows **No Data Available** , restart `nmon` on the admin node to fix the problem:

```
service nmon restart
```

Real-time Metrics

Select the **Real-time Metrics** tab to display the current metrics in real-time.

Per node, you can see the following real-time metrics:

- CPU (User + System/Idle)
- Memory Used (MB)
- Disk Read Rate (MB/s)
- Disk Write Rate (MB/s)
- Net Read Rate (MB/s)
- Net Write Rate (MB/s)

Storage Metrics

Select **Storage Metrics** tab to display metrics about cluster storage.

Per node, you can see the following storage metrics:

- HDFS Used
- System Used
- Available
- Used %

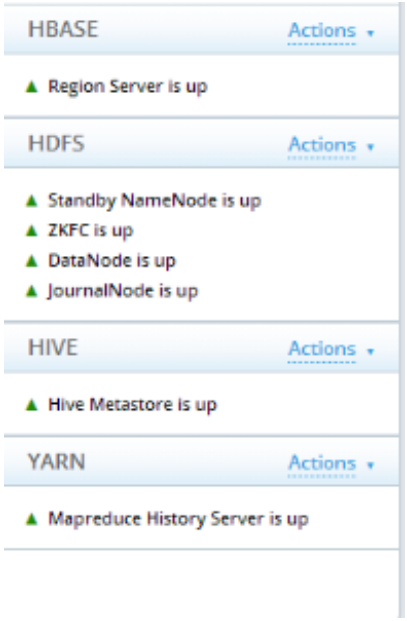
⚠ Storage metrics are only displayed if the nodes in your cluster are identified by their FQDN.

Node Metrics

If you have selected to display cluster metrics by individual node, an additional panel of information is displayed on the right side of the cluster metrics.

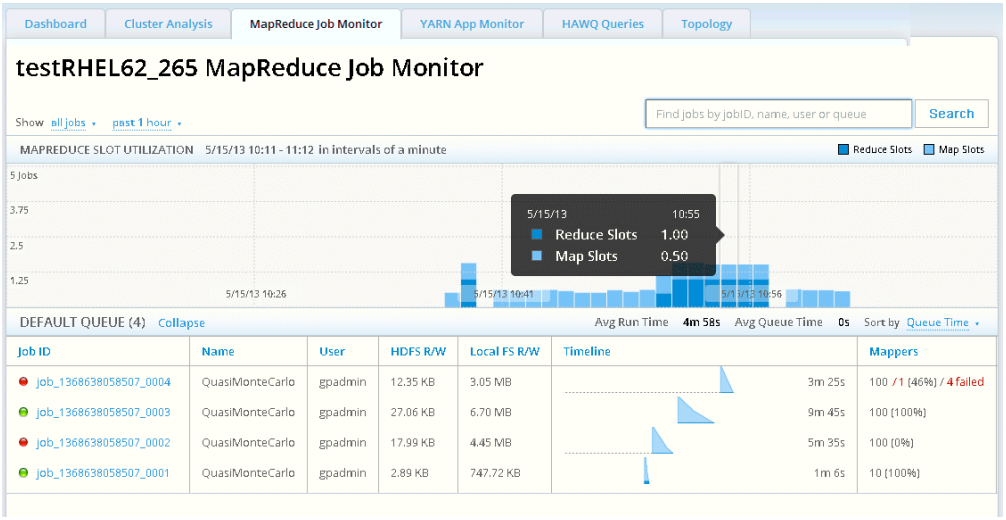
This panel displays all services and roles defined for the selected node.

For each service, you can see the status of each role, and you can use the **Actions** dropdown menu to stop/start a specific role.



MapReduce Job Monitor

The Job Monitor screen tracks the MapReduce jobs that are executed in the Pivotal HD cluster when the YARN MapReduce service is running. It provides details about all, or a filtered set of MapReduce jobs.



The MapReduce jobs displayed can be filtered by state and/or time range.

By state:

- all jobs (set by default)
- currently pending jobs
- currently running jobs
- succeeded jobs
- failed jobs
- killed jobs
- error state jobs

By time range: By selecting a preset time range in hours, weeks, months, year, or by specifying a custom time range.

The MapReduce jobs can also be filtered by searching for values for the following:

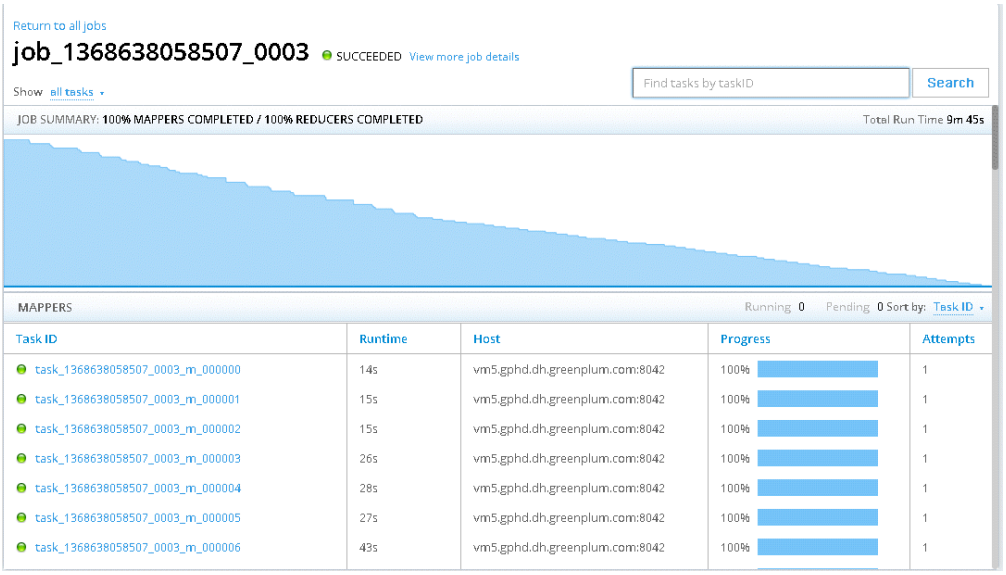
- jobID
- name
- user
- queue

Enter your search value in the search bar in the following format: searchKey=searchValue, where searchKey is one of **jobID**, **name**, **user**, or **queue**.

These are substring searches. For example: **jobID=1363920466130** will locate a job with **jobID=job_1363920466130_0002**

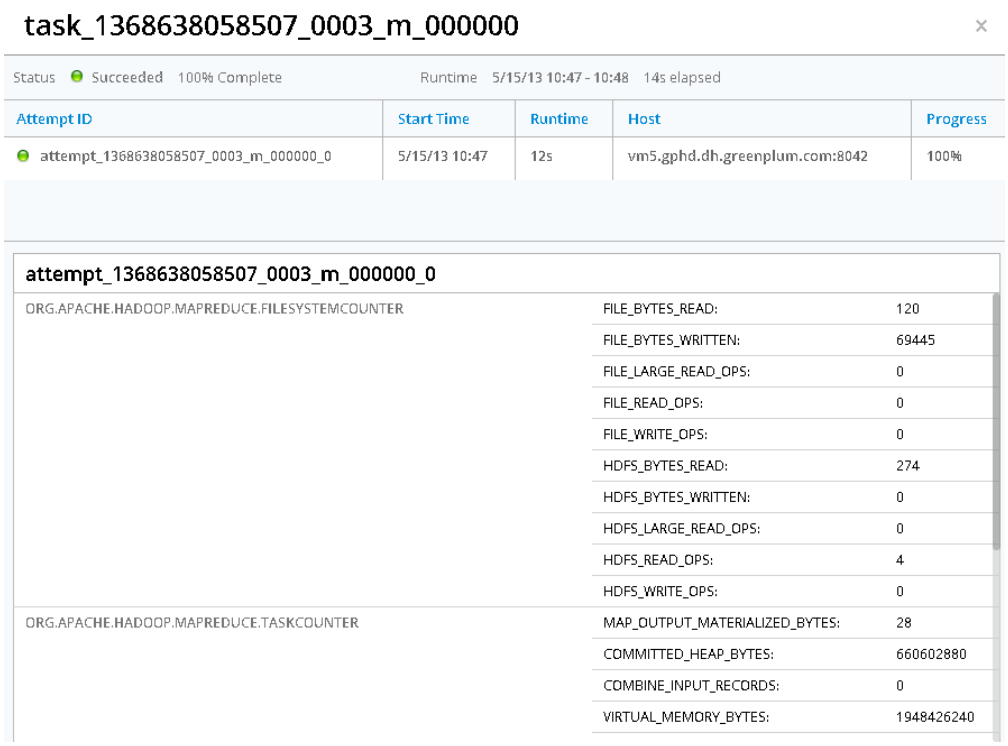
Job Details

When you click on any of the jobs in the Job Monitor more details of the job are shown.

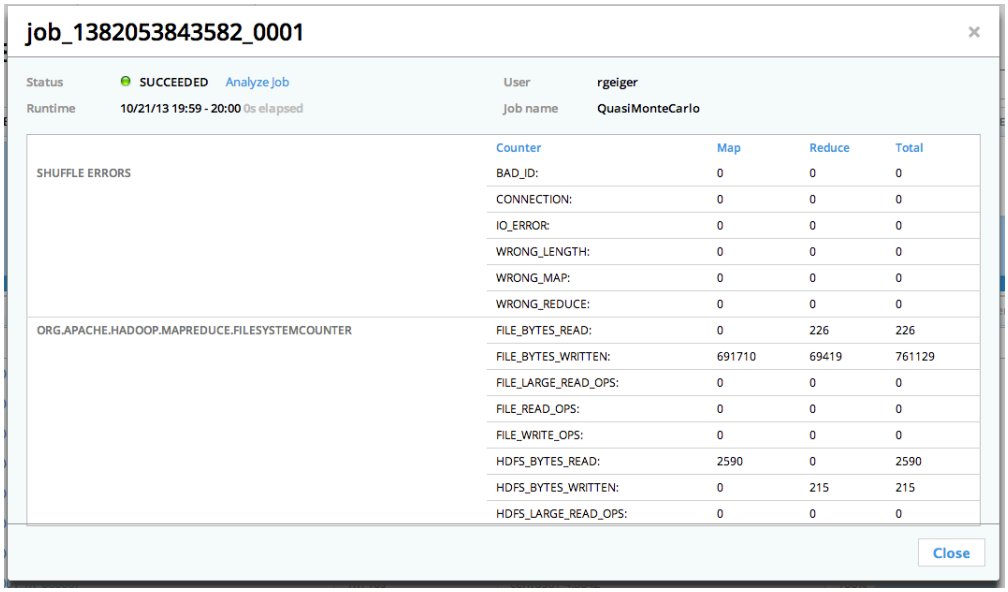


This screen displays all the tasks that are have been allocated for the selected job and their progress. You can see the mapper and the reducer tasks separately. In the above screen capture, the bars in the JOB SUMMARY section represent the two Mapper tasks that have run, one took 19 seconds, the other, 20 seconds.

Clicking on each task ID will show even more details about that particular task. You can also filter on a particular task ID in the search bar.

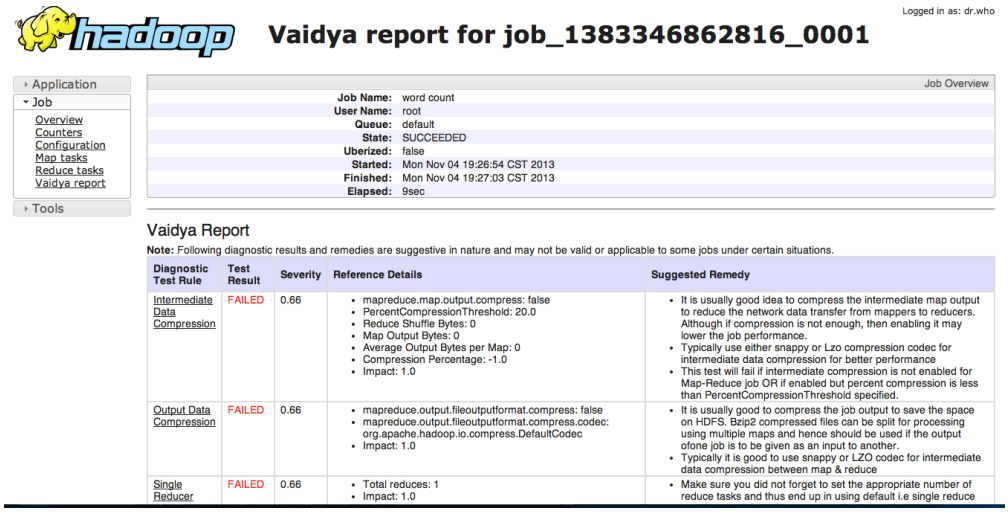


To see job related counters click on View more job details next to the job ID:



Click the **Analyze Job** link adjacent to the Status field to open a Vaidya report about the selected job, as shown below:

⚠ This capability is beta and will be improved in coming releases.



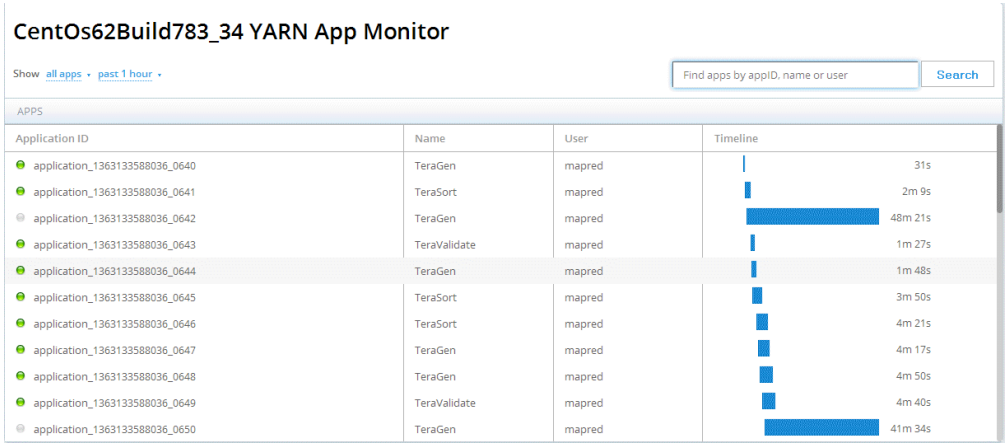
About Vaidya

Vaidya is a diagnostic tool installed with PHD for Map/Reduce jobs. After a job is executed successfully, it uses a job history log and job configuration information to identify any performance or scalability problems with the job. Upon execution, it provides a job analysis report indicating specific problems with the job along with the remedy to correct them.

For more information about Vaidya, see the *PHD Enterprise Stack and Tool Reference Guide*.

Yarn App Monitor

The YARN App Monitor screen tracks YARN applications that are executed in the Pivotal HD Cluster.



The YARN applications displayed can be filtered by category and/or time range:

- By Category:
  - all apps (set by default)
  - currently pending apps
  - currently running apps
  - succeeded apps
  - failed apps
  - killed apps
  - error state jobs
- By Time Range: By selecting a preset time range in hours, weeks, months, year, or by specifying a custom time range.

The YARN applications can also be filtered by the following fields by entering it in the search bar in the following format: searchKey=searchValue:

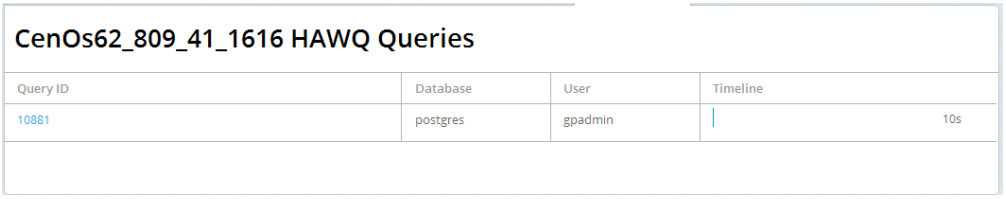
- appID
- name
- user

These are substring searches. For example: **appID=1363920466130** will locate the application with **appID=application_1363920466130_0002**

HAWQ Query Monitor

The HAWQ Query monitor is only displayed when HAWQ is installed on the cluster.

This screen displays all active queries running on the HAWQ cluster:

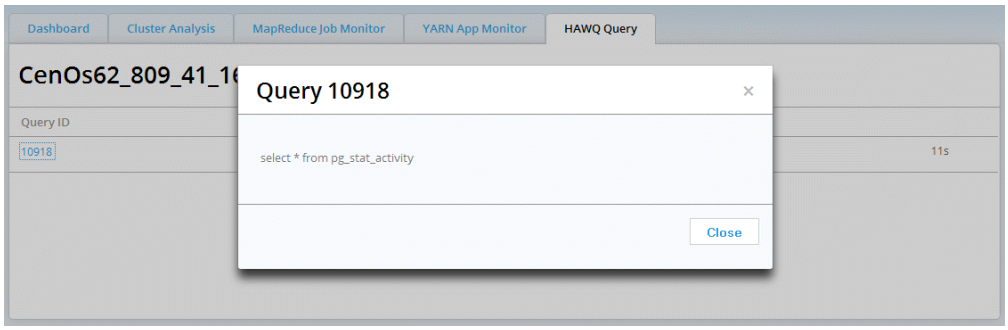


In this release, this screen only displays active queries as can be seen when you run:

```
SELECT * FROM pg_stat_activity;
```

on the HAWQ cluster.

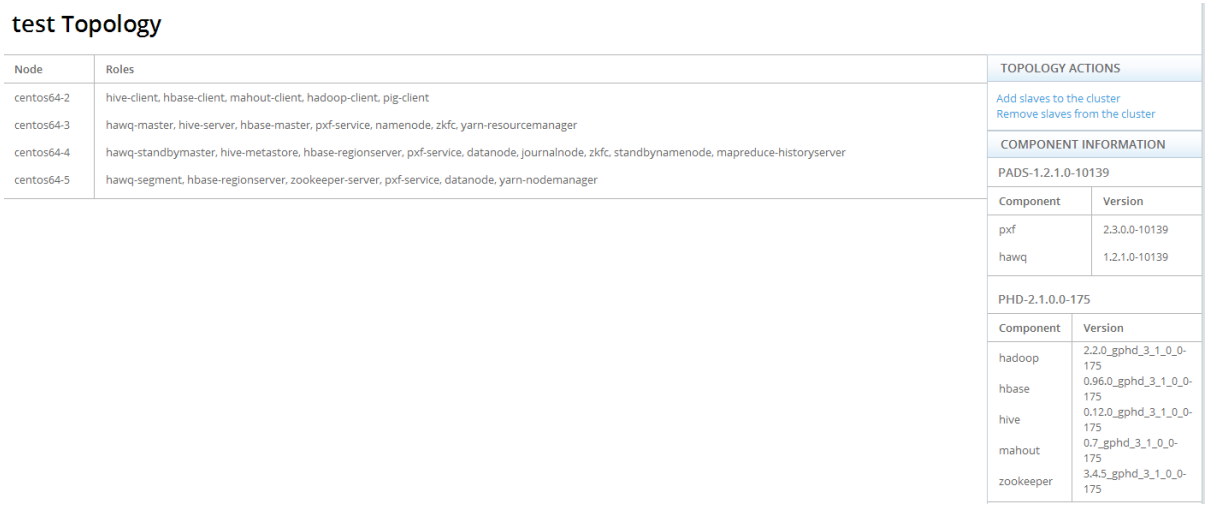
Click on a Query ID to get the syntax of that query:



Topology

This screen shows you the basic topology of your cluster. You can also add/remove slaves to/from the cluster via this screen.

The main portion of this page displays a list of all the nodes in your cluster, and the roles that have been installed on each node.



Component Information

The Component Information pane lists all the components and versions that are part of your PCC installation.

Topology Actions

You can add or remove slaves using the Topology Actions pane.

This functionality is restricted to administrative users.

A node is considered a slave if it contains the following services/roles: `datanode`, `hbase-regionserver`, `yarn-nodemanager`.

Additionally for HAWQ and PXF, a slave node contains the following services/roles: `hawq-segment`, `pxf-service`.

When you add a slave, these services/roles appear on the node. When you remove a slave node; all these services/roles are removed.

Adding Slaves to the Cluster

1. Click on the **Add Slaves to the Cluster** option from the **Topology Actions** menu. An **Add Slaves** dialog appears; this dialog lists all current nodes.
2. Enter the slave nodes you want to add either individually, or as ranges, for example `Node[1-9]`
3. Provide the Root Password
4. If you want to have services for your new slave nodes start automatically, check the **Start services automatically** box.
   If you do not choose to have the services start automatically, you can start them by returning to the Dashboard, navigating to the role defined for that node, then selecting **Action > Start** <service name>, for example **Action > Start Hive**.
5. Click **Add Slaves to Cluster**.

- If you type a node name twice, that name will flash yellow until one is deleted.
- If you type the name of a node that already exists, that name becomes highlighted and you are shown an error message warning you that:

  `Highlighted hosts are duplicates and will not be added`.
- If you close the dialog before the operation is finished, it continues in the background. Refresh the Topology page to see if it has successfully completed.

Removing Slaves from a Cluster

1. Click on the **Remove Slaves from the Cluster** option from the **Topology Actions** menu. A **Remove Slaves** dialog appears; this dialog lists all current slave nodes.
   You are warned that prior to removal, services on slave nodes will be stopped.
2. Enter the slave nodes you want to remove either individually, or as ranges, for example `Node[1-9]`.
3. Click **Remove Slaves from Cluster**.

- You do not need to provide a password to remove slave nodes.
- This text field auto-completes with nodes from the cluster.
- If you try and enter a node that does not exist, the text field does not become active and you are not able to perform the remove operation.
- If you close the dialog before the operation is finished, it continues in the background. Refresh the Topology page to see if it has successfully completed.

Logs

This screen displays all system logs. The log files are grouped by date, the most recent first. Use the **Prev** / **Next** buttons to jump to more pages of logs.

Filtering Logs

Use the upper left dropdown menus to filter the logs displayed based on:

- **Logs Levels**: You can select to display all logs (the default), or filter by one of the following log levels: debug, errors, fatal, info, trace, warnings.
- **Hosts**: You can select to display logs for all hosts (the default), including the Admin Host, or can filter by hostname.
- **Roles**: You can select to display logs for all roles (the default), or can filter by role name. Note that since the `gphdmgr-webservices` role is always on the Admin Host, if you select that role, you can no longer filter by host (in this case the Admin Host is automatically selected).

Use the upper right dropdown menu to filter the logs displayed based on:

- **Time**: You can select the time period over which you want to view logs; either for the **Past 1 hour**, or for one of the other time periods available (up to **Past 8 weeks**)

Search by Keyword

You can also further filter the logs displayed by searching the logs by keyword.

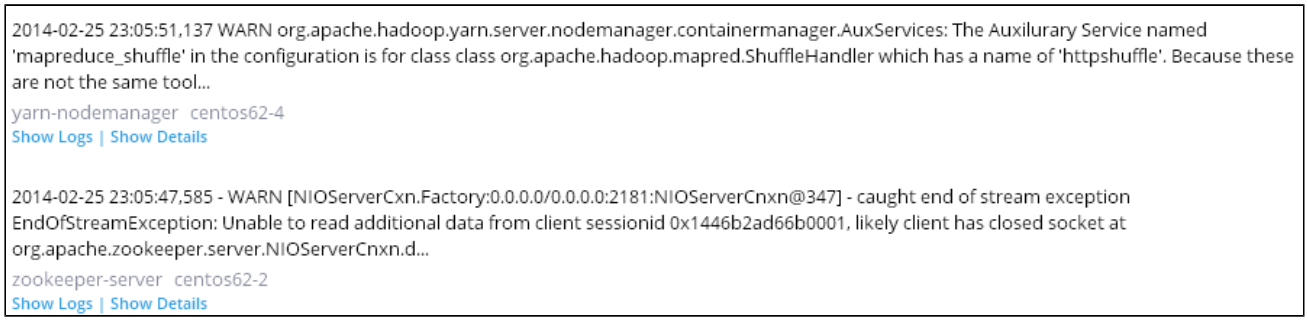
Enter any single keyword (any single string, including numbers) in the search box, then click **Search**.

Note that your keyword search is only applied to the set of logs displayed based on any filters you chose from the dropdown menus, described above.

Viewing Logs

The results of your filters, if any, are displayed on the screen. Often there will be too many to display on one page, use the **Prev**/**Next**/Page numbers at the top of the screen to navigate through them.

Each entry displays the time stamp, a log message, a time stamp, the host and the role, for example:



If the log message is too long to display on the screen it is truncated and a **Show Details** link appears below the message; click to display the entire message.

Click **Show Logs** to display all contents of that log file based on the time stamp. You can see more log messages from before and after that time stamp by clicking the **Scroll Up To Fetch More Logs** /**Scroll Down to Fetch More Logs** links at the top and bottom of the page, respectively.

Chapter 7 Configuring PCC for LDAP

This section describes how you can configure PCC to use an existing LDAP server for user authentication.

1. On the PCC Admin node, navigate to the `/usr/local/pivotal-cc/config` directory:

```
cd /usr/local/pivotal-cc/config
```

2. Open the `ldap.yaml` file in an editor, for example:

```
vi ldap.yaml
```

3. Add the following lines using values from your LDAP setup:

```
enabled: true
host: "ldap.yourdomain.com"
port: 389
username: "cn=Manager,dc=yourdomain,dc=com"
password: "changeme"
base_dn: "ou=Users,dc=yourdomain,dc=com"
```

   Where:
   `host` = The domain name of your LDAP server

   `port` = The port for your LDAP server

   `username` = The common name (cn) user to search the LDAP server

   `password` = The password associated with the username

   `base_dn` = The Base Domain Name where user information is located

   `cn` = Common Name

   ou = Organizational Unit

   dc = Domain Component

4. Save and close `ldap.yaml`

5. Restart PCC:

```
# service commander restart
```

Now when you add a user to PCC (see PCC UI User Management) you can use the **Check username** link to select an LDAP-authenticated user; once set up, this user can then log in to PCC using his/her LDAP username and password.

Chapter 8 Command Line Reference

This section provides descriptions and syntax for the command line operations you can perform.

Topics:

- Backup and Restore
  - Backup
  - Restore

You need to perform command line operations on the Admin node.

Backup and Restore

You can backup data on the admin node where PCC is installed. Having the backup allows you to restore the admin node and PCC to a given state in case of failures or data corruption.

 Backup and restore operations should be performed as `root`.

Backup

Run the backup script to copy all configuration files and all data in the PCC database into a backup file on a local disk. Once the tar file is created you should copy it off the admin node to a different storage to prevent it from being lost if the admin node fails.

 You should backup your data each time you make a configuration or topology change for your cluster or if you add or delete clusters. Trying to restore old backup on the admin node when the cluster topology or configuration has been changed since the backup will result in inconsistent configuration and potentially unusable cluster.

To perform the backup run the following script:

```
# /usr/lib/gphd/gphdmgr/bin/gphdmgr_backup.sh
```

The script does not require any input and produces the backup file `phdmgr_backup_[timestamp].tar.gz` in the current working directory, where `timestamp` is the number corresponding to the current system time.

Restore

Run the restore script to replace all configuration files and all data in the PCC database from a backup file on a local disk. There are two restore scenarios:

- **Restore data on a new node**. If you had a backup from the old admin node and you need to provision a new admin node, install PCC on the new admin node, then restore data from the backup produced on the old admin node. Hostnames, IP addresses and system configuration of the old and new nodes have to be identical.
- **Restore data on the same node**. You can restore data from the backup file on the same admin node where the backup was produced. Make sure the PCC version has not been updated since the backup was made.

⚠ The restore procedure replaces all your configuration files and database data with the data from the backup file, so use with caution.

To perform the restore run the following script:

```
# /usr/lib/gphd/gphdmgr/bin/gphdmgr_restore.sh phdmgr_backup_[timestamp].tar.gz

Your data will be permanently removed. Do you want to continue? y
```

The script takes the name of the backup file as an argument and asks the user for the confirmation before proceeding with the restore. The script takes care of stopping the PCC services, performing the restore, and restarting the services.