MemCloud™: Getting Started Guide

November 2016

Version 1.16

Kodiak Data, Inc.

2570 W El Camino Real
Suite 500
Mountain View, CA 94040
Phone: (650) 383-8374
support@kodiakdata.com
www.kodiakdata.com

TABLE OF CONTENTS

1 Kodiak Data Introduction

Big Data infrastructure has historically been built on shared-nothing clusters of commodity baremetal servers. Software stacks, such as Hadoop, have been designed to take advantage of the economics of commodity servers, disks and networking. Through this model, the cost of storing and processing TBs and PBs of data has been reduced.

Kodiak provides a radically new software architecture that enables Virtualization of Cluster Infrastructure (VCI). VCI requires no changes to existing application and cluster software, and allows many clusters to share resources and gain the management benefits of virtualization.

MemCloud is a hosted service that is built on Kodiak's VCI software, high performance flash (NVMe) and 100Gb networking technology. Using Kodiak's VCI technology, virtual clusters, such as Hadoop, can deliver baremetal performance at much lower cost.

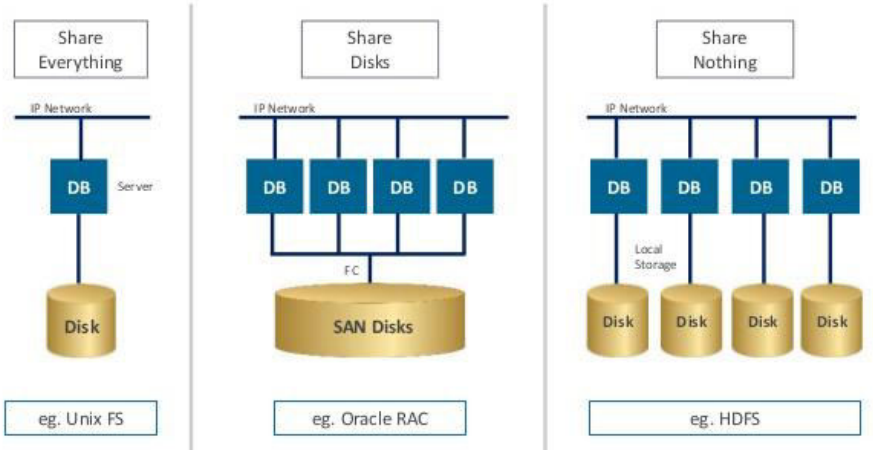


Figure 1: The Evolution to Shared-Nothing Clusters

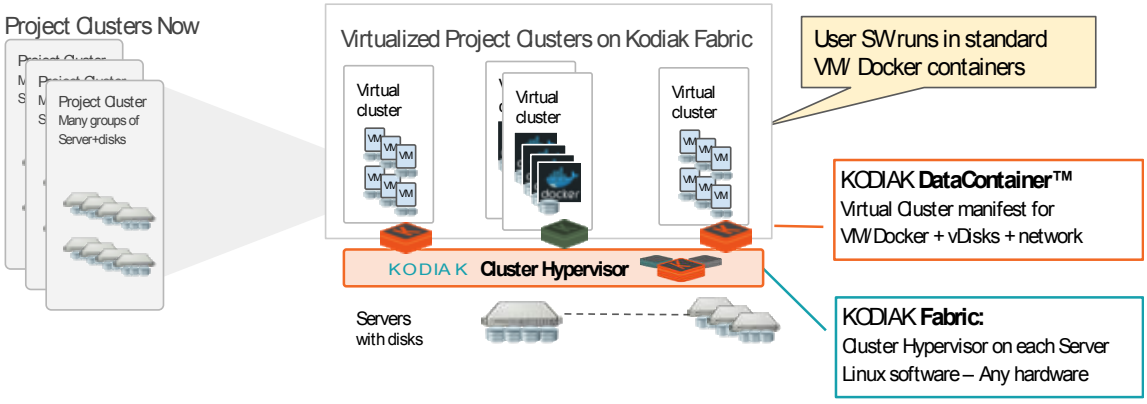
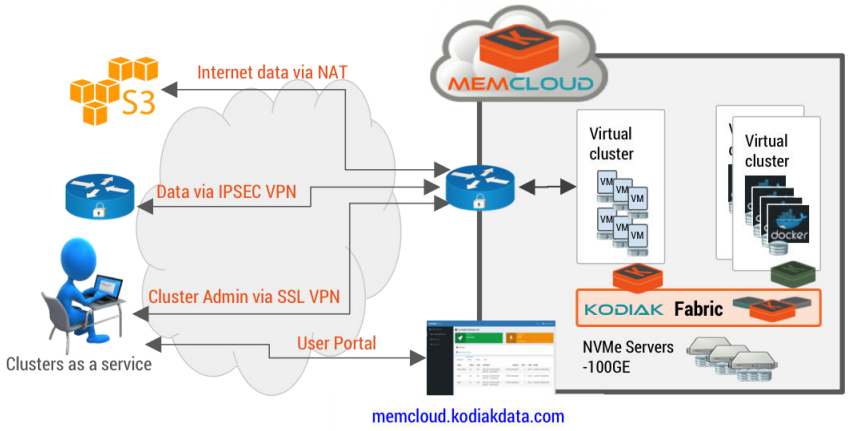


Figure 2: Kodiak's Virtual Cluster Infrastructure Solution

2 Kodiak MemCloud: Industry's 1st Hosted VCI Solution

MemCloud is a hosted service built with Kodiak's VCI software on high performance flash (NVMe) and 100Gb networking infrastructure. MemCloud enables virtual clusters, such as Hadoop, to deliver memory-speed performance at much lower cost.



The MemCloud service delivers ready-to-run clusters to users. These clusters consist of a number of hosts, each with vCPU, RAM, network connectivity and virtual disk (vDisk) assets. The hosts can be bare (Linux-only) or can be prepackaged with cluster software (Hadoop, Docker, etc.). The three key elements of the MemCloud solution are:

DataContainers™: Just like VSI needed VMs, VCI needs DataContainers to describe the application hosts and virtual disks needed for a cluster. It specifies the size and speed of each vDisk and AppHost as well as the software and IP addressing needs of a whole virtual cluster. Each virtual cluster can support one or more software stacks.

Kodiak VCI Fabric: Kodiak's Linux-based software extends the KVM hypervisor and Docker Engine on each server to support cluster hypervisor functions. A scalable IP-based VCI fabric is built using pooled resources of CPU, RAM, disk, flash and network. These resources are virtualized and allocated to specific virtual clusters and their hosts. The Kodiak VCI fabric is designed from the ground-up for use by Enterprises large and small.

MemCloud Portal: MemCloud uses all the APIs provided by the DataContainers and VCI fabric to automate the process of building, monitoring and maintaining virtual clusters. A simple web interface (portal) provides each user with access to their clusters. Clusters can be stopped, started and monitored. IP VPNs are provided to access the virtual cluster hosts.

For more information, visit us at http://www.kodiakdata.com. The following sections guide you through the steps to get started with your 1st cluster.

3 Getting Started with MemCloud

The steps for getting your 1st virtual cluster operating with MemCloud are as follows:

1) Order/request the Virtual Clusters you need.
2) Receive registration information from Kodiak, which will also confirm that the DataContainer with the Virtual Cluster has been loaded. Security information will be provided.
3) Log-in to MemCloud portal and view your DataContainer
4) Get the IP addresses of your cluster hosts from the MemCloud portal
5) Install a VPN client and load the VPN profile provided by Kodiak
6) Connect via the SSL VPN to your cluster network.
7) Use SSH to access and configure each cluster host as needed
8) Use cluster software tools (like Ambari) to set-up and run your cluster
9) Load data into your hosts or cluster

Setting up your 2nd and 3rd clusters is straight forward, especially if you choose a cluster that is prepackaged with cluster software. Many steps can be skipped:

1. Order/request the Virtual Clusters you need.
3. Login to MemCloud portal and view your DataContainer. It will appear when ready.
4. Print or capture the IP addresses of your cluster hosts from the MemCloud portal
8. Use cluster software tools (e.g. Ambari) to set-up and run your cluster
9. Load data into your hosts or cluster

The following sections provide detail on each of these steps.

If you have trouble with any steps, please email Kodiak Data at support@kodiakdata.com. Please include a description of your problem and a phone number to call you back on.

3.1 Request a Virtual Cluster

This can be done online at www.kodiakdata.com/memcloud or work with your Kodiak representative. If you need a representative, use sales@kodiakdata.com.

The basic information required is the type of cluster and capacity needed. Any special requirements should also be communicated.

A basic (1X) virtual cluster will include 3 hosts, each with 8vCPU, 16GB RAM and 4 vdisks, each of which is 250GB. The total capacity of this cluster would be 3TB. Larger clusters can be configured with more hosts or more resources.

If an application is more complex, multiple smaller clusters can be created and placed in the same DataContainer. For example, a Docker Swarm cluster and a NAS system can be merged into the same DataContainer. Contact Kodiak for more complex or custom configurations.

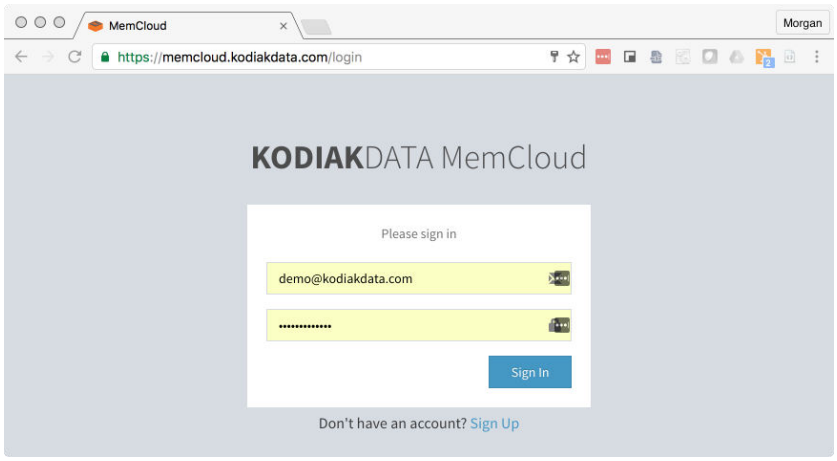
3.2 Receive Registration Information

Kodiak will send you a Registration Document, confirming that the DataContainer with the Virtual Cluster has been loaded. This document will include a password for accessing MemCloud as well as SSL VPN profile for accessing your cluster hosts.

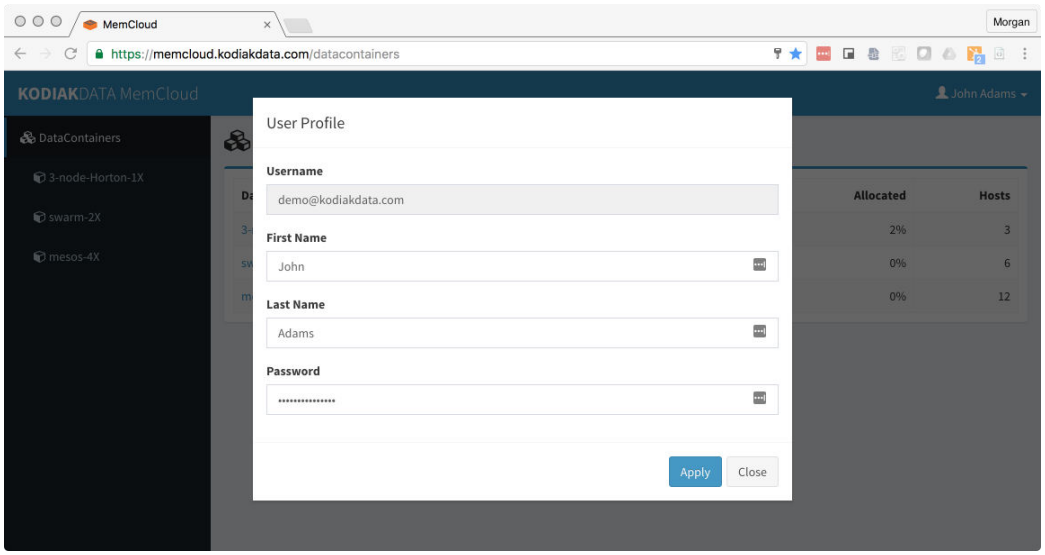
3.3 Login to MemCloud Portal

The MemCloud Portal is available at https://memcloud.kodiakdata.com

You will be prompted for a username and password. The username and password were sent to you in a MemCloud Registration document.

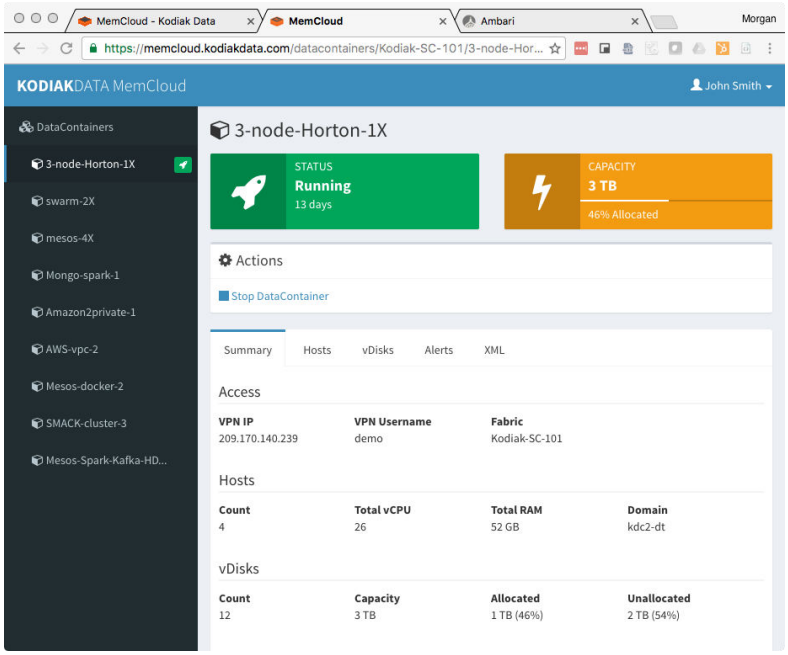


Once you login, you can click on your user identity in the top right of the page and edit your profile. This will let you customize your password for future access.



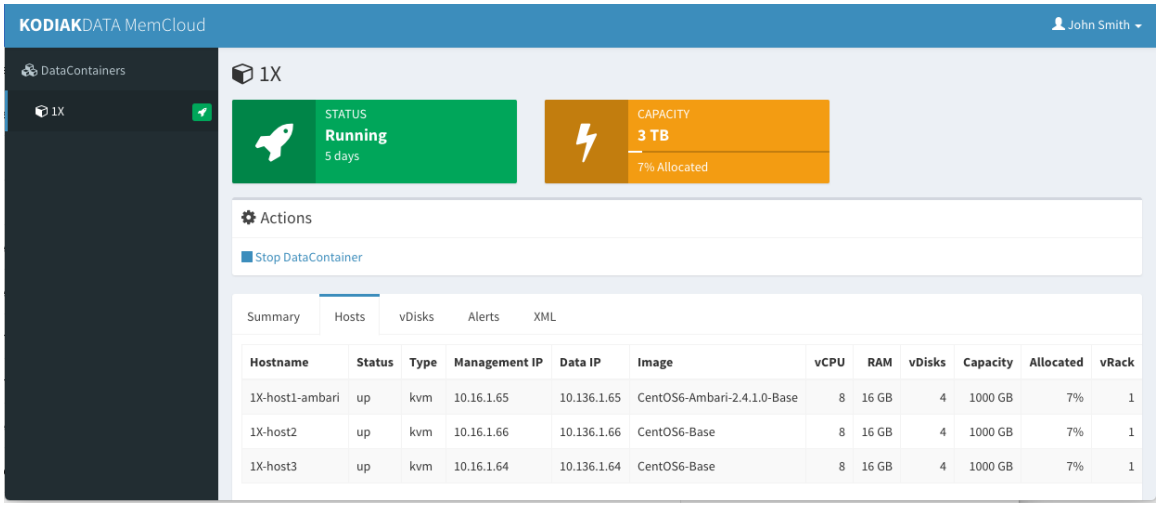
The MemCloud Portal then lets you click on your DataContainers, each of which represents a Virtual Cluster. These screens show you the DataContainer status and the status of the virtual infrastructure.

The Summary Tab shows the high level status of the DataContainer. The name of the DataContainer, the name of the Fabric and the Domain name of the Data interface are shown. The Domain name is used in building the Fully Qualified Domain Name (FQDN).



3.4 Get the Host IP addresses

The Hosts Tab for each DataContainer provides a summary of the virtual hosts in each cluster. Each of these hosts has a Management IP address and a Data IP address that are on different subnets. You can scrape this information to download your hosts and IP address mappings. Print or put the information in a spreadsheet for later reference.



3.5 Install a VPN Client

MemCloud uses OpenVPN as the standard SSL VPN client for accessing cluster hosts. If you have an OpenVPN client installed, you can skip this step.

An OpenVPN profile is sent with your Registration Document for simple configuration of the OpenVPN client. This profile filename is **MemCloud-*user*.ovpn**, where the ***user*** field is unique to a customer.

If you need an OpenVPN client, Kodiak Data has the following recommendations:

Client OS	Software	Download Location	Installation Instructions	VPN Profile Installation
MacOS	Tunnelblick (this includes OpenVPN internally)	The Stable version at: Tunnelblick-MacOS	Instructions are at: Tunnelblick-Install	Add the profile using the instructions at: Tunnelblick-User
Windows	OpenVPN	Select a stable msi installer version at: OpenVPN-Windows	Instructions at: OpenVPN -Windows-Install	Use the local file option of the procedure: OpenVPN-Windows-Profile
Linux	OpenVPN	Package management instructions are at: OpenVPN-Linux	Installation included with package management	Command line: OpenVPN filename

Viscosity for MacOS and Windows is also an OpenVPN client option that can be used. This client is affordably priced and supported.

When installing a Windows OpenVPN client, its important to "Run as Administrator", otherwise there are errors when the VPN connection starts. A step-by-step guide for Windows 10 installation is included in a later section.

3.6 Connect via VPN

Access to your hosts is via a secure SSL VPN. The VPN profile is sent with your Registration Document. When you open the profile, it will automatically be added to your VPN client. Use that profile and your OpenVPN/Tunnelblick client to connect to the MemCloud VPN. The

OpenVPN profile is setup so that only traffic destined for MemCloud will go through the VPN and you standard IP traffic will be routed as normal.

You can test your VPN connectivity by SSH into the 1st host of your virtual cluster using its Management IP address.

```
ssh -l root 10.18.2.65
```

You will also be able to access your hosts via all standard IP tools including web, ftp, etc.

3.7 Manage your Hosts

From your laptop/client you have IP connectivity to any host using its IP address. Ping, SSH, ftp or web access are possible.

If you have a prepackaged MemCloud cluster with an application cluster like Apache Hadoop pre-installed, you will be ready to start your cluster via the cluster management tool (e.g. Ambari).

Once you have SSH connected to the 1st host you can access all other hosts using their IP address or their Hostnames. These hosts all share a DNS/DHCP server that makes this possible. Load your own SSH keys onto each host, if you'd like an extra level of security.

```
ssh Kodiak1-host2
```

The Hostnames are and IP addresses are shown on the "Hosts" page and are derived from the DataContainer names for uniqueness. Upper and lower-case letters are all treated as lower-case letters.

In some cases, like Ambari, you will need to use the Fully Qualified Domain Name (FQDN) of a host. The FQDN of a host is derived as a combination of Hostname and Domain:

- Hostname: e.g. Kodiak1-Host3
- Domain: e.g. kdc14-dt
- FQDN: kodiak1-host3.kdc14-dt

The FQDN of each Host will also be shown in the "Hosts" page of each DataContainer when the mouse is hovered over a host name. The FQDN is the name of the Data IP interface.

Each host has outbound access via a NAT to the Internet. You can use this to install packages, download files or data from sources such as AWS-S3 and Docker-hub. After downloading any additional software, you can then operate your cluster.

3.8 Manage your Cluster

After the application cluster software is loaded, the cluster can be managed using the standard tools for that application cluster. For example, Ambari is used for HortonWorks or Apache Hadoop.

For each cluster type, there are commonly-used IP addresses and web portals that are assigned. For more details on the different DataContainer types, please see the later sections.

3.9 Load Data

Once you clusters are set-up, you will probably need to load and perhaps software. By default, your cluster has outbound NAT access to the Internet. All the standard tools can be used from your hosts to pull data from other sources such as:

- SCP (secure copy)
- AWS S3
- USB drives (physical transfer)

3.9.1 SCP over SSH

SCP provides a direct transfer between your local files (on disk or NAS) and memCloud. It is the fastest mechanism for smaller datasets. In preparation to use SCP:

1. Login to MemCloud user portal and click on Host tab to find the IP address of the first host
2. Make sure MemCloud SSL VPN is connected
3. SSH into the 1st host using root/kodiak as login
4. Create a directory on the host to store the data you are uploading

For Windows Users

5. Download WinSCP from https://winscp.net/eng/download.php
6. Use root/kodiak as login and password to upload files via WinSCP

For Mac or Linux Users

5. Use (Mac OSX) command line: scp <files> root@<first host IP address>:/<destination path>

3.9.2 AWS S3

AWS S3 provides a convenient place to upload and then download data. It's particularly good, if your data is already in AWS. It also provides a temporary backup in case you want to transfer the same data again. Data is transferred in two hops, so the transfer will take longer than SCP. The following steps will be used:

1. If needed, Kodiak will setup a S3 folder/bucket for you to upload data
2. Kodiak will provide AWS IAM user and password
3. Point your browser to https://309140022322.signin.aws.amazon.com/console
4. Use the AWS IAM user and password to login
5. Click on "All Services" then S3
6. Click the following bucket memcloud-uploads/home/<your AWS IAM user>

7. Upload your data
8. Kodiak can then help you setup S3 access on your host to transfer the data

3.9.3 USB Drive

Where the datasets are large relative to your upload bandwidth or are larger than a few TB, it will be faster to physically move the data. Kodiak can provide USB drives (SSD or HDD) which supports the capacity you need. Please contact us at support@kodiakdata.com and follow these steps:

1. Let Kodiak know your capacity size
2. Kodiak will send a suitable USB drive - or use your own
3. Copy your data into the USB drive
4. Send it back to Kodiak at 2570 W El Camino Real, Suite 500, Mountain View, CA 94040
5. Kodiak will connect the USB drive to your host on MemCloud
6. You will then copy data from your USB drive to your file system on MemCloud.

4 DataContainer Types

MemCloud supports many types of DataContainers and virtual clusters. The DataContainers can be standard DataContainers or customized for a specific application. The more common standard DataContainers are described in the following sections.

Each DataContainer can support one or more software stacks. For example, there could be Hadoop, Linux and NAS hosts within a single DataContainer. The DataContainer has a single Data subnet and a Management subnet. Each of these has a DHCP/DNS server to assign addresses and provide name resolution.

By default, each host can connect via IP with each other host unless the user configures specific policies on the hosts. However, hosts from one DataContainer do not have IP connectivity to hosts from another DataContainer unless that is especially configured by Kodiak.

Each software stack will have its own management ports (SSH, Web etc.). These are typically configured on the 1st host of that stack. Use the management IP address of the host for connectivity.

Hosts from a DataContainer are typically deployed over 3 virtual racks. Each virtual rack represents a fault domain. It is unlikely that hosts in two different fault domains will fail simultaneously. Applications like Hadoop can use this information to build a robust environment where virtual racks can fail without the application being brought down. Where virtual racks are used, hosts are often named as host*x-n* where x is the virtual rack number.

Custom DataContainers can be defined very flexibly. Multiple host types can be configured with specific CPU, RAM, vDIsk and software configurations. Multiple clusters can be configured by specifying names and the count of each type of host. The DataContainer is then built with all of these clusters and their specified hosts. The entire DataContainer is then managed as a single entity.

4.1 Linux DataContainer

The Linux DataContainer provides a set of hosts that are available for any Linux application to use. DHCP and DNS are setup for the set of hosts. The Management and Data IP addresses for each host is available in the MemCloud Portal. The hosts are named and arranged in 3 virtual racks or fault domains:

[DataContainer-]Host1-1… Host1-n

[DataContainer-]Host2-1… Host2-n

[DataContainer-]Host3-1… Host3-n

The Operating system loaded can be selected from several Linux distributions including CentOS 7.2 and Ubuntu 14.04

Each host typically has 4 vdisks of size 250GB and these vdisks are named /dev/vd[a,b,c,d]. Each vdisk can be allocated for any application or file system. XFS is high bandwidth and recommended. The vdisks are optionally formatted and mounted as /data[1,2,3,4].

Log in to a host via it Management IP address. The default root password for each host is kodiak. This can be modified after initial login.

```
sudo passwd root
```

After, the hosts are brought up, a unique SSH key pair is generated for each DataContainer. The public key is pushed to all hosts in the cluster. The private SSH key is located on Host1 in the following directory:

```
/root/.ssh/id_rsa
```

The private key will be called `id_rsa` and the associated public key will be called `id_rsa.pub`. Copy these keys to your laptop or administration machine.

After initial use the SSH key pair can be regenerated and pushed to each host. This will ensure Kodiak does not have access to your hosts.

```
ssh-keygen
Generating public/private rsa key pair. Enter file in which to
save the key (/root/.ssh/id_rsa):
ssh-copy-id root@hostN
```

Now that you have secure access to your host, you can build your clusters. Optionally, there can also be a NAS in the DataContainer using the same SSH keys. See the NAS DataContainer.

4.2 Hortonworks DataContainer

The HortonWorks DataContainer provides a set of hosts that are available for a HortonWorks cluster to use. DHCP and DNS are setup for the set of hosts. The Management and Data IP addresses for each host is available in the MemCloud Portal. The hosts are named and arranged in 3 virtual racks or fault domains:

[DataContainer-]Host1-1… Host1-n

[DataContainer-]Host2-1… Host2-n

[DataContainer-]Host3-1… Host3-n

Each host typically has 4 vdisks of size 250GB and these vdisks are named /dev/vd[a,b,c,d]. Each vdisk can be allocated for any application or file system. XFS is high bandwidth and recommended. The vdisks are formatted with XFS and mounted as /data[1,2,3,4], ready for integration with Hadoop.

Log in to a host via its Management IP address. The default root password for each host is kodiak. This can be modified after initial login.

```
sudo passwd root
```

After, the hosts are brought up, a unique SSH key pair is generated for each DataContainer. The public key is pushed to all hosts in the cluster. The private SSH key is located on Host1 in the following directory:

```
/root/.ssh/id_rsa
```

The private key will be called `id_rsa` and the associated public key will be called `id_rsa.pub`. Copy these keys to your laptop or administration machine.

After initial use the SSH key pair can be regenerated and pushed to each host. This will ensure Kodiak does not have access to your hosts.

```
ssh-keygen
Generating public/private rsa key pair. Enter file in which to
save the key (/root/.ssh/id_rsa):
ssh-copy-id root@hostN
```

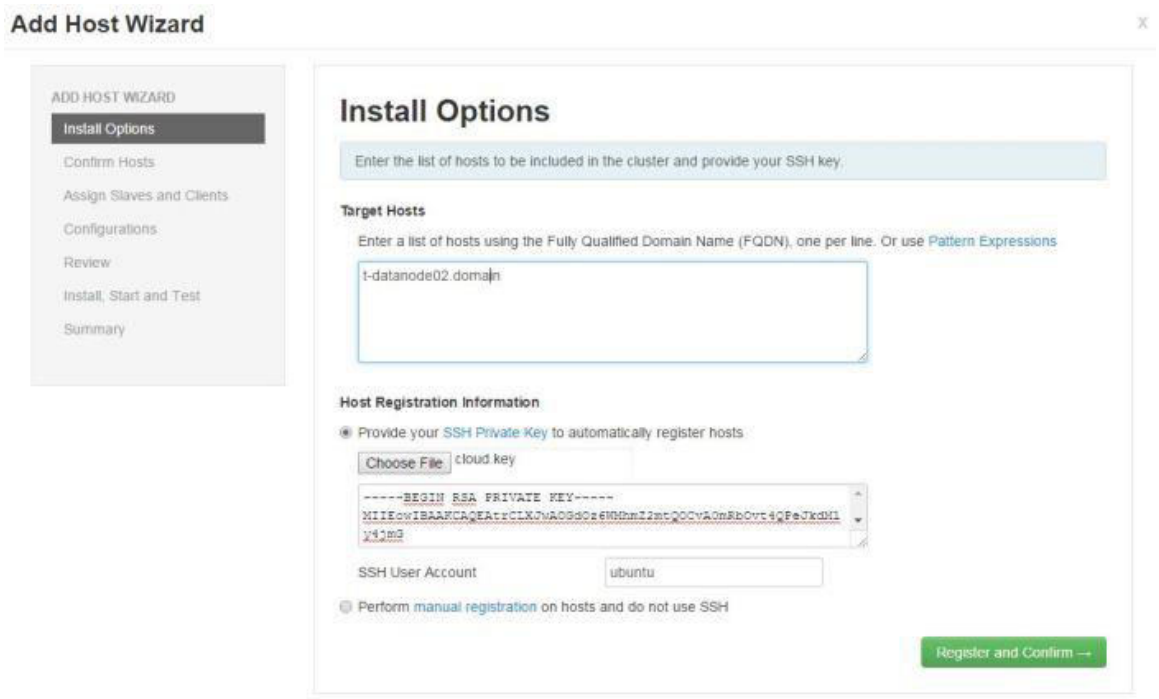
Now that you have secure access to your host, you can build your clusters.

After changing the SSH keys (optional), you may connect to Ambari via a web browser. Point your browser to http://<your.ambari.server>:8080,where <your.ambari.server> is the IP address of your Ambari host or Host1-1. For example, Kodiak's Ambari host is located at http://192.168.129.64:8080.

Log in to the Ambari Server using the default user name/password: admin/admin. You can change these credentials later. Full Ambari Documentation is available here: Ambari-Documentation

Click "install Cluster" to launch the Ambari Install wizard. This lets you name the cluster and select your stack.

Add hosts to the cluster using Ambari. Ambari-addhosts The wizard needs to access the private key file you created in Set Up Password-less SSH. Using the FQDN of the hosts and key file information, the wizard can locate, access, and interact securely with all hosts in the cluster. Use the Target Hosts text box to enter your list of host names. You can use ranges inside brackets to indicate larger sets of hosts. For example, use [DataContainer-]host2-[1-6].[Domain] if you had 6 hosts in Virtual Rack 2.



You can now administer the cluster in the standard way.

It is recommended that Ambari, NameNode and Jobtracker be placed on the "Ambari" host. The DataNode may be disabled on the Ambari host for larger clusters (e.g. 10+ hosts). The replication factor can be optionally changed from the default of 3 to 2.

4.3 Cloudera DataContainer

The Cloudera DataContainer provides a set of hosts that are available for a Cloudera cluster to use. DHCP and DNS are setup for the set of hosts. The Management and Data IP addresses for each host is available in the MemCloud Portal. The hosts are named and arranged in 3 virtual racks or fault domains:

[DataContainer-]Host1-1… Host1-n

[DataContainer-]Host2-1… Host2-n

[DataContainer-]Host3-1… Host3-n

Each host typically has 4 vdisks of size 250GB and these vdisks are named /dev/vd[a,b,c,d]. Each vdisk can be allocated for any application or file system. XFS is high bandwidth and recommended. The vdisks are formatted with XFS and mounted as /data[1,2,3,4], ready for integration with Hadoop.

Log in to a host via its Management IP address. The default root password for each host is kodiak. This can be modified after initial login.

```
sudo passwd root
```

After, the hosts are brought up, a unique SSH key pair is generated for each DataContainer. The public key is pushed to all hosts in the cluster. The private SSH key is located on Host1 in the following directory:

```
/root/.ssh/id_rsa
```

The private key will be called `id_rsa` and the associated public key will be called `id_rsa.pub`. Copy these keys to your laptop or administration machine.

After initial use the SSH key pair can be regenerated and pushed to each host. This will ensure Kodiak does not have access to your hosts.

```
ssh-keygen
Generating public/private rsa key pair. Enter file in which to
save the key (/root/.ssh/id_rsa):
ssh-copy-id root@hostN
```

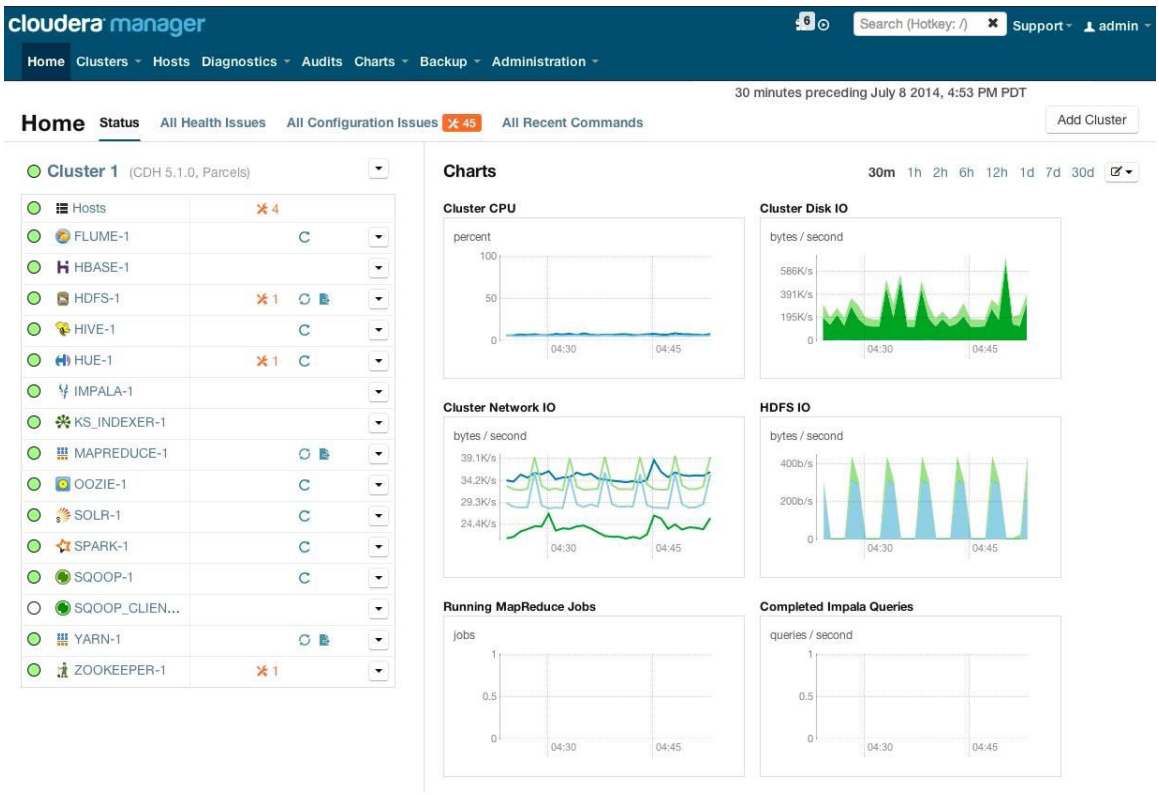
Now that you have secure access to your host, you can build your clusters.

After changing the SSH keys (optional), you may connect to Cloudera Manager via a web browser. Point your browser to https://<your.Host1-1>:7183,where <your.Host1-1> is the IP address of your Host1-1. For example, Kodiak's Cloudera host is located at https://192.168.129.64:7183.

Log in to the Cloudera Manager using the default user name/password: admin/admin. You can change these credentials later. Full Cloudera Documentation is available here: [Cloudera-Documentation]

Specify the hosts on which to install CDH and managed services. You can specify hostnames and/or IP addresses and ranges, for example: 10.1.1.[1-4] or host1-[1-3].domain. You can specify multiple addresses and address ranges by separating them by commas, semicolons, tabs, or blank spaces, or by placing them on separate lines.

You can now administer the cluster in the standard way using Cloudera Manager.



It is recommended that Cloudera manager, NameNode, Hue, Jobtracker be placed on Host1-1. The DataNode may be disabled on Host1-1 for larger clusters (e.g. 10+ hosts). The replication factor can be optionally changed from the default of 3 to 2.

4.4 NAS DataContainer

The NAS DataContainer provides a NAS server that can provide NFS services. The NAS host is typically added to another DataContainer, but instructions are similar.

DHCP and DNS are setup for the set of hosts. The Management and Data IP addresses for each NAS host is available in the MemCloud Portal. The NAS server is typically named:

[DataContainer-]NAS

The software loaded on the NAS is based on FreeBSD and FreeNAS 9.10. The NAS is a ZFS-based NAS with powerful data protection, and data management tools. The NAS is pre-set with a RAID-Z stripe of 2+1 across 3 vdisks. A single volume is created.

You can log in to a host via it Management IP address. The default root password for each host is kodiak. This can be modified after initial login.

```
sudo passwd root
```

Connect to the NAS via a web browser to complete administration and set-up of the NAS. Use the IP address of the management port of the NAS host. The default username and password for the system are root/kodiak. These can be changed as needed.

The documentation on how to use FreeNAS is here.

Typically, you will set-up a NFS share. After that, you will then connect to that share.

To make this share accessible on a BSD or a Linux system, run the following command as the superuser (or with **sudo**) from the client system. Repeat on each client that needs access to the NFS share:

```
mount -t nfs 192.168.2.2:/mnt/data /mnt
```

The **mount** command uses these:

192.168.2.2: replace with the Data IP address of the NAS Host

/mnt/data: replace with the name of the NFS share

/mnt: a mount point on the client system. This must be an existing, **empty** directory. The data in the NFS share will be made available to the client in this directory.

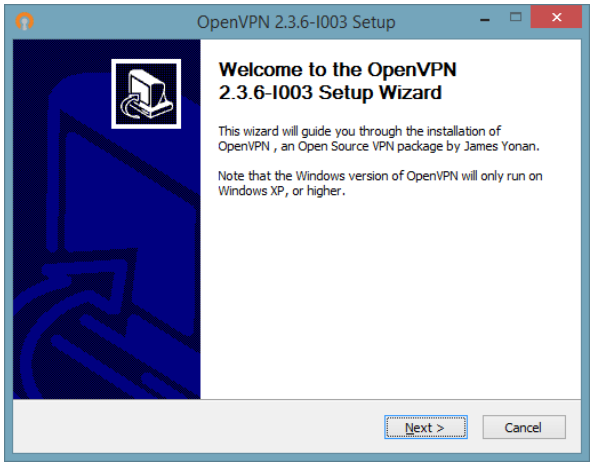
The **mount** command should return to the command prompt without any error messages, indicating that the share was successfully mounted.

5 OpenVPN Client Setup

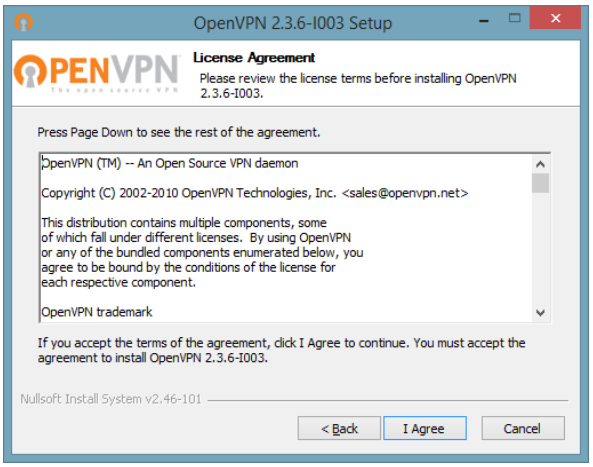
5.1 OpenVPN for Windows 10

OpenVPN on Windows 10 includes a GUI. You can download it for free from swupdate.openvpn.org

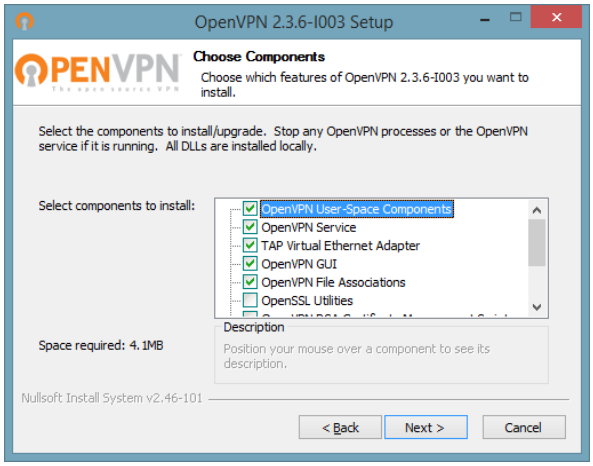
After you've downloaded the software install it:



Click the "Next" button.

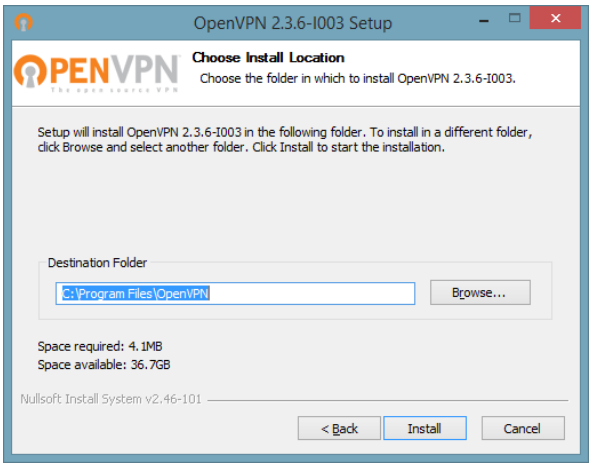


Click the "I Agree" button.



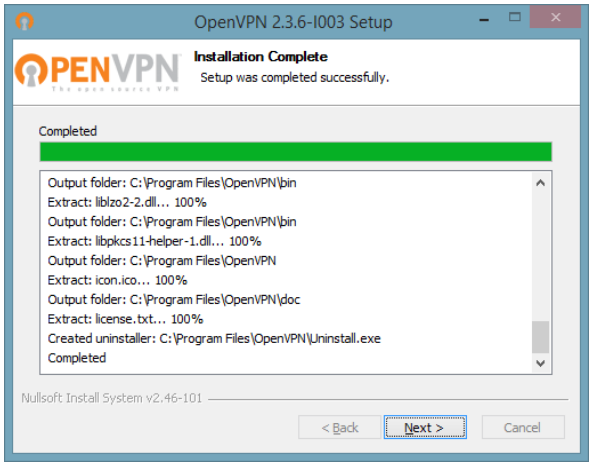
Click the "Next" button.

Click the "Install" button.

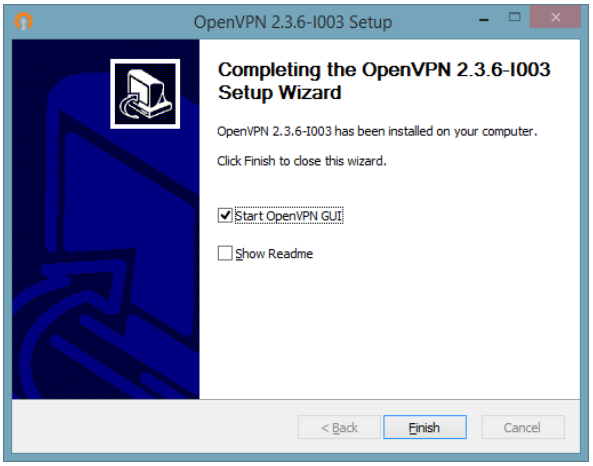


If you have the following message, press "Install".

Click the "Next" button.

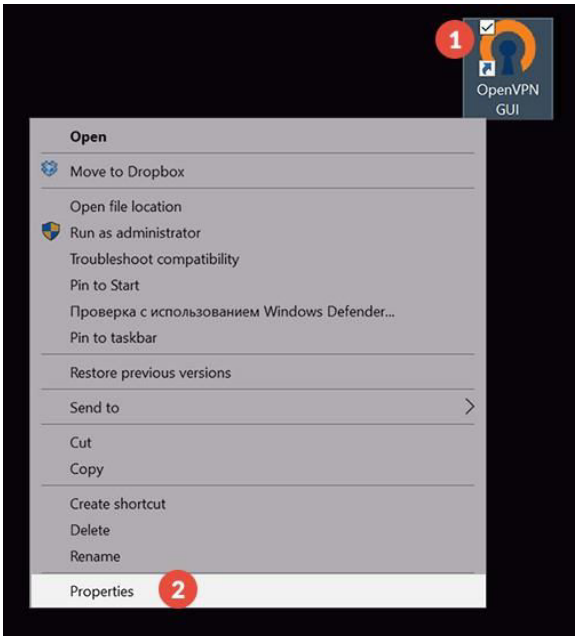


Click the "Finish" button.



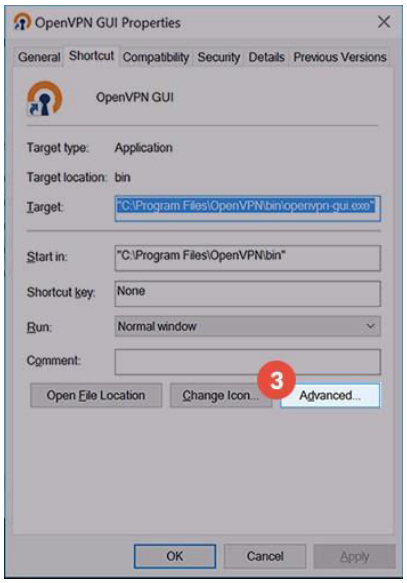
You have to install the MemCloud .ovpn file into the "config" folder of OpenVPN.

Open the "C:\Program Files\OpenVPN\config" folder, and copy the MemCloud .ovpn file into this folder.

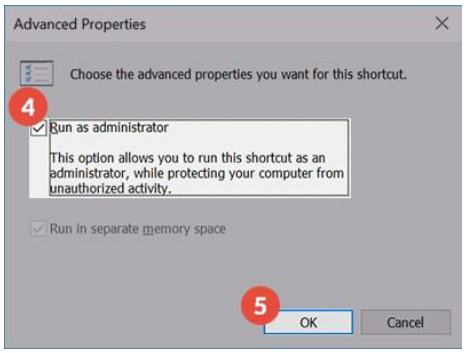


Go to the OpenVPN icon (1) from your desktop, right-click on it and select "Properties" (2).

Click on the "Advanced" button (3).



In the following dialog box check the "Run as administrator" checkbox (4) and click on "OK" (5).



From now on, OpenVPN Gui will always run as administrator if you use the shortcut to launch it. (You'll be prompted by UAC if you have it enabled).

Now, in the system tray, you should see a symbol for OpenVPN. Right click on the symbol with the mouse, choose the server you want to connect and click "Connect". You can select between two different protocols for OpenVPN: TCP and UDP. UDP is usually faster so we recommend to try it first.

To disconnect, just right click on the OpenVPN server you where connected and select Disconnect.

6 MemCloud Benefits

MemCloud makes it much easier to build and deploy high performance big data clusters.

CAPEX Budgets: MemCloud removes the need for CAPEX when you want to build a new cluster. Sandbox in MemCloud and then decide where to build/deploy production clusters.

Sandboxing: Clusters can be rapidly and cost-effectively built and then paused or torn down without wasting valuable data science resources.

Cluster Performance: MemCloud clusters are built on NVMe flash and 100Gb networking coupled with highly efficient VCI software. These clusters will outperform traditional cloud clusters based on 10Gb or less networking.

Fault Management: Virtual disks are isolated from physical disk failure. Your application sees a more reliable and higher performing I/O infrastructure.

Cluster Growth: The traditional isolation between application, compute, storage and network are restored. Virtual hosts and physical servers are added independently. Hosts and vDisks can be scaled independently.

Data Center Operations: You don't need to worry about it. Kodiak is your IT admin and manages the physical infrastructure.

Kodiak's MemCloud use high bandwidth networking to enable utilization of all available SSDs and disks, eliminating the hot spots that typically constrain physical clusters.

For more information on MemCloud, please visit www.kodiakdata.com/memcloud

7 Kodiak Data, Inc.

Kodiak was founded by a team with experience developing groundbreaking IP networking and storage product lines at Cisco, Synoptics, Force10, GridIron and Violin Memory. The very experienced development team is based in Mountain View, California.

Kodiak's products are built on a Virtual Cluster Infrastructure (VCI) software suite that combines networking and storage insights into a unique, patented and cohesive approach.

MemCloud is the hosted service offer that provides clusters as a service.

For more information, please visit our website.

Please contact Kodiak if you would like to learn more about the products and technology associated with VCI and how it can help your organization. Email us at info@kodiakdata.com