About BlueData EPIC™

VERSION 2.4

Notice

BlueData Software, Inc. believes that the information in this publication is accurate as of its publication date. However, the information is subject to change without notice. **THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." BLUEDATA SOFTWARE, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

Use, copying, or distribution of any BlueData software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, please refer to your specific agreements or contact BlueData Technical Support at support@bluedata.com.

The information in this document is subject to change. This manual is believed to be complete and accurate at the time of publication and no responsibility is assumed for any errors that may appear. In no event shall BlueData Software, Inc. be liable for incidental or consequential damages in connection with or arising from the use of this manual and its accompanying related materials.

Copyrights and Trademarks

Contact Information

BlueData Software, Inc.
3979 Freedom Circle, Suite 850
Santa Clara, California 95054
Email: info@bluedata.com
Website: www.bluedata.com

Table of Contents

This page intentionally left blank.

1 - Welcome

The BlueData Elastic Private Instant Clusters platform (referred to as "EPIC" throughout this manual) allows users to provide Big-Data-as-a-Service within their own secure on-premises environments. This guide provides an in-depth overview of the main components and architecture for version 2.3 of the BlueData EPIC software platform.

Virtualization and container technologies have already introduced flexibility, agility, and reduced costs to most applications in the enterprise data center. BlueData EPIC uses Docker containers and proprietary, patent-pending innovations to extend these benefits to Big Data by allowing enterprises to create, modify, and remove virtual clusters on demand without sacrificing performance.

With the BlueData EPIC software platform, enterprises can simultaneously run hundreds of Big Data workloads with automated policy-based scheduling and self-provisioning. Distributed applications are efficient and elastic, thanks to EPIC's proprietary application-sensitive caching, data path, network optimization, and policy-based automation and management. IT administrators use a single interface to monitor Hadoop or Spark clusters, jobs, and infrastructure status. EPIC also automates routine tasks such as provisioning, updates, and monitoring.

BlueData EPIC dramatically reduces Big Data deployment complexity while improving business agility by providing an elastic self-service infrastructure that reduces the time-to-value from months to days while reducing overall costs by 50%-75% compared to traditional, non-virtualized Hadoop and Spark deployments. Users create virtual clusters on demand and execute jobs without ever having to worry about the underlying infrastructure.

Note: Most of the information in this Guide pertains to both EPIC (full version) and EPIC Lite (evaluation version). The key differences between the two versions are outlined in the EPIC Lite Installation Guide.

1.1 - About BlueData EPIC

The BlueData EPIC software platform introduces patent-pending innovations that leverage virtualization and container technology to deliver all of the agility and efficiency benefits of Big-Data-as-a-Service in a secure on-premises deployment.

1.1.1 - Key Features and Benefits

The key features and benefits of BlueData EPIC include:

- **Create virtual clusters:** EPIC duplicates the functionality of physical clusters while adding flexibility and scalability at reduced cost. Each virtual cluster can run a different Hadoop or Spark distribution. You may create, modify, re-prioritize, and remove virtual clusters on demand to respond to ever-changing needs within individual business units/departments. EPIC reduces time-to-value from months to hours.
- **Multi-tenancy and enterprise-grade security model:** EPIC integrates with enterprise LDAP and Active Directory authentication systems. Administrators can then create groupings of users and resources that restrict access to jobs, data, or clusters based on departments and/or roles. The result is a secure, multi-tenant infrastructure.
- **Self-service portal:** EPIC includes a self-service web portal that allows users to create and manage clusters, create and manage nodes, run Big Data jobs, and view monitoring statistics. User visibility and available functionality vary based on each user's role and tenant, in accordance with existing security policies. For example, department administrators can use the portal to provision nodes/clusters to run their own Big Data applications without impacting nodes/clusters that are assigned to different departments and without having to manage the physical infrastructure.
- **RESTful API:** EPIC supports a RESTful API that surfaces programmable access to the same capabilities as the self-service portal.
- **Superior performance:** EPIC includes I/O optimization modules for Big Data applications that deliver high performance without the penalties commonly associated with virtualization. The CPU cores and RAM in each host are pooled and then partitioned into virtual resource groups based on tenants.
- **Works with existing infrastructure:** EPIC leverages your existing datacenter investments by allowing your enterprise to re-purpose its existing infrastructure to run Big Data deployments. EPIC supports your existing physical or virtualized infrastructure, including commodity x86 servers and ESX/AWS virtual machines. Existing storage protocols are also supported (HDFS, HDFS with Kerberos, and NFS).
- **Reduced IT overhead:** EPIC streamlines operations and reduces IT costs by automating provisioning, unifying management, and supporting push-button upgrades.

- **Increases utilization while lowering costs:** EPIC delivers hardware and operational cost savings while simultaneously eliminating the complexity of managing multiple physical clusters.
- **High Availability:** EPIC supports two levels of High Availability to provide redundancy and protection, as described in *"High Availability" on page 29*.

1.1.2 - Hadoop and Spark Support

The BlueData EPIC platform includes out-of-the-box support for major Hadoop distributions, including recent versions of Cloudera (CDH) and Hortonworks (HDP), as well as Spark standalone. Other distributions, services, commercial applications, and custom applications can be easily added to a BlueData EPIC deployment, as described in *"App Store" on page 6*.

BlueData EPIC supports a wide range of Hadoop application services and Hadoop ecosystem products out-of-the-box, such as:

- **Ambari (for HDP 2.3):** Ambari is an open framework that allows system administrators to provision, manage, and monitor Apache Hadoop clusters and integrate Hadoop with the existing network infrastructure.
- **Cloudera Manager (for CDH):** Cloudera Manager provides a real time view of the entire cluster, including a real-time view of the nodes and services running, in a single console. It also includes a full range of reporting and diagnostic tools to help optimize performance and utilization.
- **Cloudera Navigator (for CDH):** Cloudera Navigator is a fully integrated Hadoop data management tool that provides critical data governance capabilities for regulated enterprises or enterprises with strict compliance requirements. These capabilities include verifying access privileges and auditing access to all Hadoop data.
- **Flume:** Flume-NG is a distributed, reliable, and available service for efficiently collecting, aggregating, and moving large amounts of server log data. It is robust and fault tolerant with many failover and recovery mechanisms. It uses a simple extensible data model that allows one to build online analytic applications.
- **Hadoop Streaming:** Hadoop Streaming is a utility that allows you to create and run MapReduce jobs with any script as the mapper and/or the reducer taking its input from `stdin` and writing its output to `stdout`.
- **HAWQ:** Apache HAWQ is a native Hadoop application that combines high-performance MPP-based analytics performance with robust ANSI SQL compliance, integration and manageability within the Hadoop ecosystem, and support for a variety of datastore formats with no connectors required.
- **HBase:** HBase is a distributed, column-oriented data store that provides random, real-time read/write access to very large data tables (billions of rows and millions of columns) on a Hadoop cluster. It is modeled after Google's BigTable system.
- **Hive:** Hive facilitates querying and managing large amounts of data stored on distributed storage. This application provides a means for applying structure to this data and then running queries using the HiveQL language. HiveQL is similar to SQL and supports using custom mappers when needed.

- **Hue:** Hue is an open-source Web interface that integrates the most common Hadoop components into a single interface that simplifies accessing and using a Hadoop cluster.
- **Impala:** Impala by Cloudera is an open source Massively Parallel Processing (MPP) query engine that allows users to query data without moving or transforming that data, thus enabling real-time analytics without the need to migrate data sets. EPIC supports Impala on CDH.
- **Kafka:** Kafka allows a single cluster to act as a centralized data repository that can be expanded with zero down time. It partitions and spreads data streams across a cluster of machines to deliver data streams beyond the capability of any single machine.
- **MapReduce:** MapReduce assigns segments of an overall job to each Worker, and then reduces the results from each back into a single unified set.
- **Oozie:** Oozie is a workflow scheduler system for managing Hadoop jobs that specializes in running workflow jobs with actions that run Hadoop MapReduce and Pig jobs.
- **Pig:** Pig is a language developed by Yahoo that allows for data flow and transformation operations on a Hadoop cluster.
- **Ranger:** Apache Ranger is a central security framework that allows granular access control to Hadoop data access components, such as Hive and HBase. Security administrators manage policies that govern access to a wide array of resources in an individual and/or group basis. Additional capabilities include auditing, policy analytics, and encryption.
- **Sqoop:** Sqoop is a tool designed for efficiently transferring bulk data between Hadoop and structured datastores, such as relational databases. It facilitates importing data from a relational database, such as MySQL or Oracle DB, into a distributed filesystem like HDFS, transforming the data with Hadoop MapReduce, and then exporting the result back into an RDBMS.
- **Sqoop 2:** Sqoop 2 is a server-based tool designed to transfer data between Hadoop and relational databases. You can use Sqoop 2 to import data from a relational database management system (REBMS) such as MySQL or Oracle into the Hadoop Distributed File System (HDFS), transform the data with Hadoop MapReduce, and then export it back into an RDBMS.

BlueData EPIC supports a wide range of Spark application services and Spark ecosystem products out-of-the-box, such as:

- **GraphX:** GraphX works seamlessly with graphs and collections by combining ETL, exploratory analysis, and iterative graph computation within a single system. The Pregel API allows you to write custom iterative graph algorithms.
- **MLlib:** MLlib is Spark's scalable machine learning library that contains common learning algorithms, utilities, and underlying optimization primitives.
- **Spark SQL:** Spark SQL is a Spark module designed for processing structured data. It includes the DataFrames programming abstraction and can also act as a distributed SQL query engine. This module can also read data from an existing Hive installation.
- **SparkR:** This R package provides a lightweight front end for using Spark from R.

- **Spark Streaming:** Spark Streaming is an extension of the core Spark API that enables fast, scalable, and fault-tolerant processing of live data streams.
- **Zeppelin:** Web-based Zeppelin notebooks allow interactive data analytics by bringing data ingestion, exploration, visualization, sharing, and collaboration features to Spark as well as Hadoop.

1.1.3 - App Store

BlueData EPIC offers an **App Store** with one-click deployment for common Big Data applications, including:

- Spark and open source Hadoop distributions from Cloudera and Hortonworks.
- Software applications from partners such as AtScale, Platfora, and Splunk.

The **App Store** contains Docker container images of each available product, allowing fully automated self-service deployment that accelerates time to business value with Big Data analytics. Each image in the **App Store** provides a particular version and starting configuration for these products. EPIC also supports a "bring your own app" model by allowing users to quickly add images for any Big Data application or data processing platform (such as Cassandra) to the **App Store**. The **App Store** contains three classes of images:

- **Major Hadoop, Spark, and other Big Data products provided out-of-the-box by BlueData.** These images contain open source bits of major distributions that are both unmodified and supported by the distribution vendors.
- **Several ETL and business intelligence tools supported out-of-the-box by BlueData.** These include images for AtScale, Platfora, and Splunk applications. The images are validated by BlueData and available in the **App Store** via partnerships with these companies.
- **Custom distributions and applications added specifically by individual customers on a case-by-case basis.** BlueData provides an application workbench that allows customers to create and add their own images to the **App Store**. Users can then deploy these images and use them in a similar way as any of the out-of-the-box images described above.

*Note: **App Store** images are independent of BlueData software. Any distribution or application can be added or removed from your EPIC platform to suit your specific needs.*

The Site Administrator may install or uninstall images. Installed images are available for use by tenant Members when creating jobs and clusters.

BlueData and/or application vendors may provide new images or new versions of existing images. If a new version becomes available for an image that is currently installed, the image will be marked in the **App Store** with an **Upgrade Available** banner, and its tile will provide a button for upgrading to the new version. Other new images or new versions of currently uninstalled images will display a **New** banner.

1.2 - Definitions

This guide uses the following terms:

- **Host:** A *host* is a physical or virtual server that is available to the EPIC platform. Nodes and clusters reside on hosts.
- **Node:** A *node* (also called a *virtual node* or *instance*) is a container that is created when running a transient job or when creating a persistent cluster.
- **EPIC platform:** An *EPIC platform* consists of the hosts that comprise the overall infrastructure available to a virtual cluster.
- **Controller:** A *Controller* is a host that manages the other nodes while also serving as a Worker host in the EPIC platform.
- **Worker host:** A *Worker host* is a host that is managed by a Controller.
- **Master:** A *Master* is a container (node) that manages a transient job or persistent cluster.
- **Worker node:** A *Worker node* is a container (node) that is managed by a Master node in a transient job or persistent cluster.
- **Shadow Controller:** A *Shadow Controller* is a designated Worker host that assumes the Controller host role if the primary Controller host fails. Your EPIC platform must meet all applicable requirements and have High Availability enabled for this protection to be active.
- **Arbiter:** An *Arbiter* is a designated Worker host that triggers the Shadow Controller host to assume the Controller role if the primary Controller host fails.
- **Hadoop job tracker:** Within a virtual cluster running MR version 1, a *Hadoop job tracker* is the node that is responsible for coordinating the MapReduce application efforts of the remaining virtual nodes within that virtual cluster.
- **Hadoop task tracker:** Within a virtual cluster running MR version 1, a *Hadoop task tracker* is a node that accepts tasks (Map, Reduce, and Shuffle operations) from the Hadoop job tracker. Each task tracker configuration specifies the number of "slots" or tasks that it can accept. Task trackers notify the job tracker when tasks complete. They also send out periodic "heartbeat" messages with the number of available slots, to keep the job tracker updated.
- **Resource manager:** Within a virtual cluster running YARN, a *resource manager* is the node that is responsible for coordinating the MapReduce application efforts of the remaining virtual nodes within that virtual cluster.
- **Node manager:** Within a virtual cluster running YARN, a *node manager* is a node that accepts tasks (Map, Reduce, and Shuffle operations) from the resource manager. Each node manager configuration specifies the number of "slots" or tasks that it can accept. Node managers notify the resource manager when tasks complete. They also send out periodic "heartbeat" messages

with the number of available slots, to keep the resource manager updated.

- **Site:** A *site* consists of all of the tenants, nodes, virtual clusters, and users that exist on a given EPIC platform.
- **Tenant:** A *tenant* is a unit of resource partitioning and data/user access control in a given site. The resources of an EPIC platform are shared among the tenants on that platform. Resources used by one tenant cannot be used by another tenant. All users who are a member of a tenant can access the resources and data objects available to that tenant.
- **Virtual node:** A *virtual node* (also called a *node* or *instance*) is a container that forms part of a virtual cluster.
- **Edge node:** An *edge node* is a node running a business intelligence tool that interacts with the cluster's Hadoop or Spark framework.
- **Virtual cluster:** A *virtual cluster* is a collection of virtual nodes that is available to a specific tenant. There are two types of virtual clusters:
  - A *persistent cluster* is not tied to any particular job and remains intact when the job is complete.
  - A *transient cluster* is created on-demand for a job that is not using a persistent cluster; it is destroyed when the job is completed.
- **Node flavor:** A *node flavor* describes the amounts and sizes of resources (virtual CPU cores, memory, and hard disk size) allotted to a virtual node.
- **Site Administrator:** The *Site Administrator* (or *Site Admin*) is a role granted to an EPIC user. A user with this role has the ability to create/delete tenants. This person will probably also be responsible for managing the hosts in the EPIC platform.
- **Tenant Administrator:** A *Tenant Administrator* (or *Tenant Admin*) is a role granted to an EPIC user. A user with this role has the ability to manage the specific tenant(s) for which they have been granted this role, including creating DataTaps for that tenant.
- **Tenant Member:** A *Tenant Member* (or *Member*) is a role granted to an EPIC user. A user with this role has non-administrative access to the specific tenant(s) for which they have been granted this role. Members may use existing DataTaps for reading and writing data.
- **User:** A *user* is the set of information associated with each person accessing the EPIC platform, including the authentication and site roles.
- **DataTap:** A *DataTap* is a shortcut that points to a storage resource on the network. A Tenant Administrator creates a DataTap within a tenant and defines the storage namespace that the DataTap represents (such as a directory tree in a file system). A Tenant Member may then access paths within that resource for data input and/or output. Creating and editing DataTaps allows Tenant Administrators to control which storage areas are available to the members of each tenant, including any specific sharing or isolation of data between tenants.
- **Node storage:** *Node storage* is storage space available for backing the root filesystems of nodes. Each host in the EPIC platform contributes node storage space that is used by the

nodes assigned to that host. The site administrator may optionally specify a quota limiting how much node storage a tenant's nodes may consume.

- **Tenant storage:** *Tenant storage* is a shared storage space that may be provided by either a local HDFS installation on the EPIC platform or a remote storage service. Every tenant is assigned a sandbox area within this space that is accessible by a special, non-editable `TenantStorage` DataTap. All nodes within the tenant can access this DataTap and use it for persisting data that is not tied to the life cycle of a given cluster. Tenant storage differs from other DataTap-accessible storage as follows:
  - A tenant may not access tenant storage outside of its sandbox.
  - The Site Administrator can choose to impose a space quota on the sandbox.
- **Cluster file system:** Many types of EPIC clusters set up cluster-specific shared storage that consists of services and storage resources inside the cluster nodes. For example, an EPIC cluster running Hadoop will set up an in-cluster HDFS instance. This shared storage is referred to as the *cluster file system*. The cluster file system is often used for logs and temporary files. It can also be used for job input and output; however, the cluster file system and all data therein will be deleted when the cluster is deleted.

1.3 - System Requirements

Before installing EPIC, your infrastructure must meet or exceed the requirements listed in this section.

1.3.1 - General

The general infrastructure requirements are:

- DHCP server that supports either assigning IP address by device MAC address or a network with a block of static IP addresses reserved out of the DHCP pool. The host name assigned to the servers during installation must be available through out the life of the EPIC deployment.

Note: EPIC does not support configurations where a DHCP network neither assigns IP addresses by node MAC address nor has a pool of available static IP addresses.

- If you are using a 10 gigabit network, then you should configure your network to use jumbo frames.
- For Red Hat Enterprise Linux (RHEL), you must either be subscribed via the Red Hat Subscription Manager or have appropriate repositories available internally.
- Dedicated EPIC physical or virtual ESX/AWS hosts. BlueData strongly recommends that you do not install any other applications on these hosts.
- Console and SSH access to either the root account or a non-root user account with sudo privileges is required.
- (Optional) Network routing from the individual computers/devices being used to access the EPIC interface to each EPIC Controller host. Each EPIC installation specifies a range of network addresses to be used by EPIC virtual clusters. If your network routes addresses in this range to the Controller host by default, then you will be able to access the Web interface for services running on EPIC virtual clusters via the **<Cluster>** screen, as described in the *User/Administrator Guide*.

1.3.2 - Hosts

EPIC requires at least two physical or virtual hosts to run (such as for a minimal proof of concept installation), and at least five hosts are recommended for larger evaluation installations. The requirements for each host in the EPIC platform are:

- 2.0GHz Intel or AMD x86 CPU with at least 4 cores (8 to 16 cores recommended for higher compute density).
- 32GB RAM (64GB-192GB recommended for higher compute density).
- One 1Gb (minimum) or 10Gb (recommended) Ethernet card. Each host must use the same interface name. See *"Network" on page 12*.
- Two (2) or more 1TB hard drives on the Controller host, and two (2) or more hard drives on each Worker host.
  - The first hard drive is the root drive on both the Controller and Worker hosts. This drive must have at least 300GB of free disk space in the root partition.

Note: If /srv is on a separate partition, then it must have at least 100GB of free space.

  - Any additional available hard drives may be used for tenant storage or node storage.

  See *"Storage" on page 22*.

1.3.3 - Operating System

- 64-bit Red Hat Enterprise Linux or CentOS 6.7 (minimum) or 6.8 (recommended) installed on all hosts with iptables enabled. RHEL systems must have active valid subscriptions in order to access the RHEL RPM repositories. Use the standard OS kernel; modifications may cause EPIC to function unpredictably.

CAUTION: BLUEDATA STRONGLY RECOMMENDS INSTALLING EPIC ON DEDICATED HOSTS WITH CLEAN OS INSTALLATIONS ON THEM. INSTALLING EPIC ON HOSTS WITH OTHER RUNNING APPLICATIONS CAN CAUSE UNPREDICTABLE BEHAVIOR.

Note: For best results, BlueData recommends installing EPIC on hosts that share the same configuration (CPU, RAM, storage, OS, etc.).

CAUTION: EPIC MAY INSTALL AND RUN PROPERLY ON HOSTS WITH VARYING CONFIGURATIONS, BUT THIS CANNOT BE GUARANTEED.

- All hosts must have the sshd service running on port 22.
- The user account that is employed for the initial EPIC Controller installation must also be available on all hosts that will be added as EPIC Worker hosts. Credentials for that account (password or SSH key) must be available for all hosts.
- If installing EPIC as the root user, sshd must be configured to allow root login on all hosts.

- If installing EPIC as a non-root user, that user must have sudo permissions to execute the specific binaries listed in *"Restricted Sudo Privileges" on page 15* without restrictions on all hosts in the EPIC platform. The sudoers file should also include the files located in the /etc/sudoers.d/ directory.
- The IPv6 module should be enabled on the OS. EPIC does not require IPv6 addresses or use the IPv6 infrastructure; however, enabling this module will help avoid runtime errors and warnings.
- The arp settings in the /etc/sysctl.conf for arp_announce and arp_ignore should be set to 0.

```
net.ipv4.conf.eth0.arp_ignore = 0
net.ipv4.conf.eth0.arp_announce = 0
```

1.3.4 - Network

EPIC may be installed on a variety of DHCP and non-DHCP networks. Your network must be able to support two subnets in order for EPIC to manage the hosts and run jobs.

- `proxy-arp` must be enabled on external switches.
- Each host (Controller and Worker) in the EPIC platform must include at least one 1Gb or 10Gb Ethernet card, which will be used for both hosts (Management network) and communications between the virtual nodes in EPIC clusters. If the hosts have two Ethernet cards, then one will be used for the hosts and the other for containers.
- All hosts must use the same NIC interface. For example, if the Controller host has uses an interface named **eth0**, then all the other hosts must also have this interface named **eth0**. For online installation, this NIC must have Internet access.
- EPIC requires each host within the cluster platform to always have the same IP address and host name in order for the Controller and Worker nodes to communicate reliably.
- If your network does not support DHCP, then you will need to manually assign one public LAN IP address and a host name to each host in the EPIC platform.
- If your network does support DHCP, then it must support either of the following schemas in order to be able to guarantee that each host will have the same IP addresses and host name at all times:
  - Assignment of IP addresses by MAC address.
  - Reserved pool of static IP addresses that can be assigned to each of the hosts.

  You will not be able to install EPIC on a DHCP network that does not support one of these two options.
- Network CIDR assigned and managed by EPIC for use by virtual clusters. This subnet must be able to communicate with the hosts where EPIC is installed. The size of the CIDR determines the number of virtual instances that can be created on the system. The external switch acts as the gateway for that CIDR.
- Each host acts as a router for the virtual clusters located on that host.

There are four basic installation scenarios:

- **Scenario 1:** Single NIC, with only one subnet provided by the network team. In this situation, the network must be divided into two subnets. For example, assume that the network uses 172.16.1.0/24, with 172.16.1.1. as the external gateway IP. Configure the subnets as follows:
  - 172.16.1.0/25 for the physical hosts, which means they be assigned IP addresses in the range 172.16.1.2-172.16.1.127.
  - 172.16.1.128/25 for containers.

  In this example, include the following parameters when running the EPIC bundle:

```
<bin_file> \
--int-gateway-ip 172.16.1.128 \
--floating-ip-start 172.16.1.129 \
--floating-ip-end 172.16.1.254 \
--floating-ip-mask 25 \
--floating-ip-extif eth0 \
--floating-ip-nexthop 172.16.1.1
```

- **Scenario 2:** Single NIC, with two subnets provided by the network team, where each subnet has its own external gateway. For example, assume the following:
  - 172.16.1.0/24 for the physical hosts, with the gateway at 172.16.1.1. Hosts will be assigned IP addresses in the range 172.16.1.2-172.16.1.254.
  - 172.16.2.0/24 for containers, with the gateway at 172.16.2.1.

  In this example, include the following parameters when running the EPIC bundle:

```
<bin_file> \
--int-gateway-ip 172.16.2.2 \
--floating-ip-start 172.16.2.3 \
--floating-ip-end 172.16.2.254 \
--floating-ip-mask 24 \
--floating-ip-extif eth0 \
--floating-ip-nexthop 172.16.2.1
```

- **Scenario 3:** Two physical NICs, with two subnets and container external traffic being routed through the second NIC, where eth0 and eth1 are the NIC interfaces and:
  - 172.16.1.0/24 is used for the physical hosts on eth0, with the gateway at 172.16.1.1. Hosts will be assigned IP addresses in the range 172.16.1.2-172.16.1.25.
  - 172.16.2.0/24 is used for containers on eth1, with the gateway at 172.16.2.1. In this case, do not assign an IP address to eth1.

  In this example, include the following parameters when running the EPIC bundle:

```
<bin_file> \
--int-gateway-ip 172.16.2.2 \
--floating-ip-start 172.16.2.3 \
--floating-ip-end 172.16.2.254 \
--floating-ip-mask 24 \
--floating-ip-extif eth1 \
--floating-ip-nexthop 172.16.2.1
```

- **Scenario 4:** One physical NIC with 2 VLAN interfaces (**eth0.40** and **eth0.50**) and two subnets, with container external traffic being routed through the through the second VLAN interface. For example:
  - 172.16.1.0/24 on eth0.40 for the physical hosts, with the gateway at 172.16.1.1. Hosts will have to be assigned IP addresses in the range 172.16.1.2-172.16.1.254.
  - 172.16.2.0/24 on eth0.50 for containers, with the gateway at 172.16.2.1. Do not assign any IP addresses to eth0.50.

  In this example, include the following parameters when running the EPIC bundle:

```
<bin_file> \
--int-gateway-ip 172.16.2.2 \
--floating-ip-start 172.16.2.3 \
--floating-ip-end 172.16.2.254 \
--floating-ip-mask 24 \
--floating-ip-extif eth0.50 \
--floating-ip-nexthop 172.16.2.1
```

1.3.5 - High Availability Requirements

In order to provide High Availability for the EPIC platform Controller host, each of the following requirements must be met:

- The EPIC platform must consist of at least three hosts. You will install EPIC on the Controller host and then add Worker hosts. When enabling High Availability, you should assign a previously-added Worker host as the Shadow Controller host and another previously-added Worker host as the Arbiter host.
- Each of the three hosts (Controller, Shadow Controller, and Arbiter) must have IP addresses that fall within the same subnet. Further, you must have an additional IP address available within the same subnet for use as the cluster IP address.
- The external switch that is connected to the private network should support “gratuitous arp” based IP-to-MAC discovery. This is required in order to allow the cluster IP address to migrate between the primary Controller host and the Shadow Controller host by sending a gratuitous arp for each new IP to MAC binding.
- If you installed the Network Manager service while installing the base operating system on the nodes, EPIC will stop this service because it conflicts with the High Availability monitoring services. Any network interface configured to use this service will be configured to not use it. EPIC will also configure the service to not restart when the node reboots.

1.3.6 - Browser Requirements

The EPIC self-service portal is accessible via HTML (http://) using the following browsers:

- Internet Explorer (10.0 or later)
- Firefox (38.0.5 or later)
- Chrome
- Safari (desktop and mobile)

1.3.7 - Restricted Sudo Privileges

If installing EPIC as a non-root user, that user must have sudo permissions to execute each of the following binaries without restrictions on all hosts in the EPIC platform:

```
arping
blockdev
ccs
chcon
chgrp
chkconfig
chmod
chown
cp
dmsetup
docker
echo
/etc/init.d/bds_gmetad-controller
/etc/init.d/bds_gmond-11638_1474931031.72
/etc/init.d/bds_gmond-25419_1474931007.56
/etc/init.d/bds_gmond-3190_1474930566.03
/etc/init.d/bds_gmond-3192_1474930559.36
/etc/init.d/bds_gmond-3607_1474929894.94
/etc/init.d/bds_gmond-8776_1474931016.11
/etc/init.d/nagios
/etc/init.d/pacemaker
find
grep
hadoop
hostname
ip
kadmin.local
kdb5_util
killall
kinit
klist
kprop
ln
ls
lvchange
lvconvert
lvcreate
lvremove
mkdir
mkfs.ext4
mount
mv
ntpd
/opt/bluedata/common-install/bd_mgmt/bin/
bd_mgmt
parted
partprobe
pcs
pvcreate
restorecon
rm
/sbin/ifconfig
/sbin/initctl
/sbin/iptables
/sbin/start
```

```
/sbin/stop
sed
semanage
semodule
service
set
setsebool
su
sysctl
tar
touch
useradd
usermod
/usr/bin/ovs-ofctl
/usr/bin/ovs-vsctl
/usr/sbin/arping
/usr/sbin/dnsmasq
/usr/sbin/pcs
vgcreate
vgdisplay
wget
yum
```

1.4 - BlueData EPIC Architecture

This section describes the EPIC architecture, user hierarchy, DataTaps, and other important EPIC concepts.

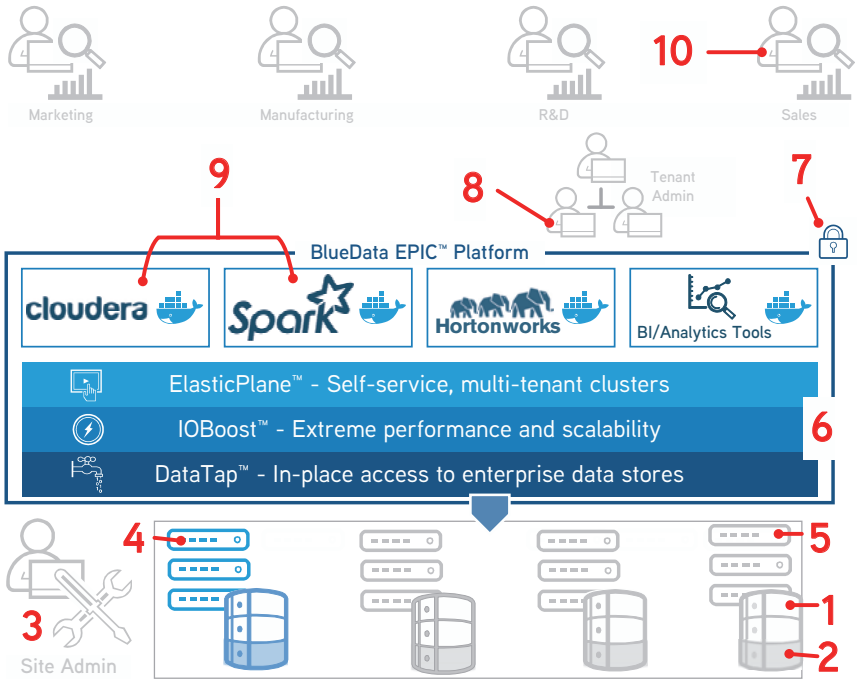

Figure 1.1: EPIC architecture

1.4.1 - BlueData EPIC Software Components

BlueData EPIC is an enterprise-grade software platform that forms a layer between the underlying infrastructure and Big Data applications, transforming that infrastructure into an agile and flexible platform for virtual clusters running on Docker containers.

EPIC consists of three key capabilities:

- **ElasticPlane**™ is a self-service web portal interface that spins up virtual Hadoop or Spark clusters on demand in a secure, multi-tenant environment.
- **IOBoost**™ provides application-aware data caching and tiering to ensure high performance for virtual clusters running Big Data workloads.
- **DataTap**™ accelerates time-to-value for Big Data by allowing in-place access to any storage environment, thereby eliminating time-consuming data movement.

The high-level EPIC architecture is as follows (numbers correspond to the callouts in Figure 1.1):

- **Data Source (1):** This is where EPIC reads and writes job data and temporary files required by the tenants and virtual clusters. The cluster file system that is locally hosted in the node storage space of the EPIC platform can be used for this purpose;

however, EPIC also allows you to create DataTaps, which are shortcuts to existing data storage locations on your network. This reduces or even eliminates the need to copy large volumes of data to and from the virtual clusters before and after running jobs, thus saving time and reducing network traffic. Please see *"Storage" on page 22* for more about how EPIC handles data storage.

- **Unique file directories for each tenant (2):** EPIC automatically creates a sandboxed shared-storage area for each tenant within the tenant storage space of the EPIC platform. This per-tenant storage can be used to isolate data that should be accessible by only one tenant. Optionally, it can also be used to enforce a quota on the tenant's use of that space.
- **Site Administrator (3):** One or more Site Administrator(s) handle overall EPIC administration, including managing hosts and creating tenants.
- **Controller host (4):** The Controller host is the host where you initially install EPIC. This host controls the rest of the hosts in the EPIC platform.
- **Worker hosts (5):** Worker hosts are under the direct control of the Controller host. EPIC dynamically allocates the resources on these hosts to the virtual clusters and jobs within each tenant as needed, based on user settings and resource availability. This dynamic resource allocation means that EPIC achieves a much higher host utilization rate than traditional Hadoop and Spark deployments. If you have High Availability enabled, then two of these Worker hosts will have additional roles, as described in *"High Availability" on page 29*.
- **EPIC Platform (6):** The EPIC platform consists of the EPIC installations on each of the hosts. EPIC handles all of the back-end virtual cluster management for you, thereby eliminating the need for complex, time-consuming IT support. Site and Tenant Administrator users can perform all of these tasks in moments using the EPIC web portal.
- **Role-based security (7):** EPIC includes three user roles (Site Administrator, Tenant Administrator, and Member) that allow you to control who can see and perform specific functions. Roles are granted on a per-tenant basis, meaning that you can either restrict users to a single tenant or grant access to multiple tenants. Each user may have one role per tenant.
- **Tenant Administrators (8):** A Tenant Administrator manages the resources assigned to that tenant. Each tenant must have at least one user with the Tenant Administrator role.
- **Tenants (9):** Tenants allow you to restrict EPIC access as needed, such as by department. Each tenant has its own unique sets of authorized users, DataTaps, applications, and virtual clusters that are never shared with any other tenant. Users with access to one tenant cannot access or modify any aspect of another tenant unless they have an assigned role (Tenant Administrator or Member) on that tenant.
- **End Users/Members (10):** A typical enterprise will create one tenant for each department that needs to run Big Data jobs, such as Manufacturing, Marketing, Research & Development, or Sales. These departments are the end users for EPIC. Individuals within each department who have a Member role for the tenant belonging to that department can access EPIC to run jobs.

1.4.2 - Software Hierarchy

EPIC runs on either the Red Hat Enterprise Linux or CentOS operating system, version 6.7 (minimum) or 6.8 (recommended). You must have the operating system installed on all of the nodes that you will be using for EPIC before beginning the installation process (see *"High Availability" on page 29*). BlueData also provides an *Installation Guide* to customers that contains step-by-step instructions for installing the BlueData EPIC software platform.

1.4.3 - Virtual Cores and RAM

Each node that makes up a persistent cluster or transient job consumes system CPU and memory resources, according to the virtual CPU (VCPU) core count and amount of RAM specified for that node. The EPIC platform provides a total amount of available virtual CPU cores and RAM. Each tenant may also be assigned a quota that limits the total number of virtual CPU cores and/or amount of RAM that are available to the clusters and jobs within that tenant.

EPIC grants VCPU cores and RAM to clusters and jobs on a first-come, first-served basis. Each cluster or job requires CPU and RAM resources in order to run, based on the number and size of its component nodes. Cluster or job creation can only proceed if the total resources assigned to that cluster or job will not exceed the tenant quota and if a corresponding amount of resources are free in the system.

EPIC models virtual CPU cores as follows:

- The number of available virtual CPU cores is the number of physical CPU cores multiplied by the CPU allocation ratio specified by the Site Administrator. For example, if the hosts have 40 physical CPU cores and the Site Administrator specifies a CPU allocation ratio of 3, then EPIC will display a total of 120 available cores.
- EPIC allows an unlimited number of virtual CPU cores to be allocated to each tenant. The collective core usage for all nodes within a tenant will be constrained by either the tenant's assigned quota or the available cores in the system, whichever limit is reached first. The tenant quotas and the CPU allocation ratio act together to prevent tenant members from overloading the system's CPU resources.
- When two nodes are assigned to the same host and contend for the same physical CPU cores, EPIC allocates resources to those nodes in a ratio determined by their virtual CPU core count. For example, a node with 8 cores will receive twice as much CPU time as a node with 4 cores.
- The Site Administrator can also specify a Quality of Service (QOS) multiplier for each tenant. In the case of CPU resource contention, the node core count is multiplied by the tenant QOS multiplier when determining the CPU time it will be granted. For example, a node with 8 cores in a tenant with a QOS multiplier of 1 will receive the same CPU time as a node with 4 cores in a tenant with a QOS multiplier of 2. The QOS multiplier is used to describe relative tenant priorities when CPU resource contention occurs; it does not affect the overall cap on CPU load established by the CPU allocation ratio and tenant quotas.

EPIC models RAM as follows:

- The total amount of available RAM is equal to the amount of unreserved RAM in the EPIC platform. Unreserved RAM is the amount of RAM remaining after reserving some memory in each host for EPIC services. For example, if your EPIC platform consists of four hosts that each have 128GB of physical RAM with 110GB of unreserved RAM, the total amount of RAM available to share among EPIC tenants will be 440GB.
- EPIC allows an unlimited amount of RAM to be allocated to each tenant. The collective RAM usage for all nodes within a tenant will be constrained by either the tenant's assigned quota or the available RAM in the system, whichever limit is reached first.

During tenant creation, EPIC will suggest some default values in the **Maximum Cores** and **Maximum Memory** quota fields. These default values will be 25% of the total system virtual CPU cores or RAM, respectively. The total available amount of that resource is displayed for comparison below each field. You may edit these quota values or delete a value and leave the field blank to indicate that the tenant does not have a quota defined for that resource.

Assigning a quota of virtual CPU cores and/or RAM to a tenant does not reserve those resources for that tenant when that tenant is idle (not running one or more jobs or clusters). This means that a tenant may not actually be able to acquire system resources up to its configured maximum CPU cores and RAM.

You may assign a quota for any amount of virtual CPU cores and/or GB of RAM to any tenant(s) regardless of the actual number of available system resources. A configuration where total allowed tenant resources exceeds the current amount of system resources is called *over-provisioning*. Over-provisioning occurs when one or more of the following conditions are met:

- You only have one tenant which has quotas that either exceed the system resources or are undefined quotas. This tenant will only be able to use the resources that are actually available to the EPIC platform; this arrangement is just a convenience to make sure that the one tenant is always able to fully utilize the platform, even if you add more hosts in the future.
- You have multiple tenants where none have overly large or undefined quotas, but where the sum of their quotas exceeds the resources available to the EPIC platform. In this case, you are not expecting all tenants to attempt to use all their allocated resources simultaneously. Still, you have given each tenant the ability to claim more than its “fair share” of the EPIC platform's resources when these extra resources are available. In this case, you must balance the need for occasional bursts of usage against the need to restrict how much a “greedy” tenant can consume. A larger quota gives more freedom for burst consumption of unused resources while also expanding the potential for one tenant to prevent other tenants from fully utilizing their quotas.
- You have multiple tenants where one or more has overly large and/or undefined quotas. Such tenants are trusted or prioritized to be able to claim any free resources; however, they cannot consume resources being used by other tenants.

Note: Over-provisioning is useful in certain situations; however, avoiding over-provisioning prevents potential resource conflicts by ensuring that all tenants are guaranteed the maximum number of allocated virtual CPU cores and RAM.

1.4.4 - Virtual Node Flavors

A virtual node flavor defines the number of virtual CPU cores and RAM used by a virtual node. For example, if the flavor "small" specifies a single virtual CPU core and 3GB of RAM, then all virtual nodes created with the "small" flavor will have those specifications, subject to the rules described in *"Virtual Cores and RAM" on page 19*.

The Site Administrator should create flavors with virtual hardware specifications appropriate to the jobs and clusters that tenant members will create. Application characteristics will guide these choices, particularly the minimum virtual hardware requirements per node. Using nodes with excessively large specifications will waste resources (and count toward a tenant's quota). It is therefore important to define a range of flavor choices that closely match user requirements.

EPIC creates a default set of flavors (such as **Small**, **Medium**, and **Large**) during installation. The Site Administrator may freely edit or delete these flavors. When editing or deleting a flavor:

- If you edit or delete an existing flavor, then all jobs and/or virtual nodes using that flavor will continue using the flavor as specified before the change or deletion. EPIC displays the flavor definition being used by transient and persistent clusters.
- You may delete all of the flavors defined within your EPIC installation; however, you will be unable to create any persistent clusters or transient jobs if you do this, until you create at least one new flavor.
- You may specify a root disk size when creating or editing a flavor. This size overrides the image size. Specifying a root disk size that is smaller than the image size will prevent you from being able to install that image on a cluster that uses that flavor. Creating a larger root disk size will slow down cluster creation; however, this may be necessary if you are using the cluster to run an application that uses a local file system.

Note: Consider using DataTaps (see "Storage" on page 22) where possible for optimal performance.

1.5 - Storage

This section describes how EPIC uses DataTaps, tenant storage, and node storage.

1.5.1 - DataTaps

DataTaps expand access to shared data by specifying a named path to a specified storage resource. Big Data jobs within EPIC virtual clusters can then access paths within that resource using that name. This allows you to run jobs using your existing data systems without the need to make time-consuming copies or transfers of your data. Tenant Administrator users can quickly and easily build, edit, and remove DataTaps using the **DataTaps** screen, as described in the *User/Administrator Guide*. Tenant Member users can use DataTaps by name.

Each DataTap consists of some of the following properties depending on its type (NFS, HDFS, or HDFS with Kerberos):

- **Name:** Unique name for each DataTap. This name may contain letters (A-Z or a-z), digits (0-9), and hyphens (-), but may not contain spaces.
- **Description:** Brief description of the DataTap, such as the type of data or the purpose of the DataTap.
- **Type:** Type of file system used by the shared storage resource associated with the DataTap (HDFS, or NFS). This is completely transparent to the end job or other process using the DataTap.
- **Host:** DNS name or address of the service providing access to the storage resource. For example, this could be the namenode of an HDFS cluster.
- **Share:** For NFS DataTaps, this is the exported share on the selected host.
- **Port:** For HDFS DataTaps, this is the port on the host used to access the data.
- **Path:** Complete path to the directory containing the data within the specified NFS share or HDFS file system. You can leave this field blank if you intend the DataTap to point the root of the specified share/volume/file system.
- **Standby namenode:** DNS name or IP address of a standby namenode that an HDFS DataTap will try to reach if it cannot contact the primary host. This field is optional; when used, it provides high-availability access to the specified HFDS DataTap.
- **Kerberos parameters:** If the HDFS DataTap has Kerberos enabled, then you will need to specify additional parameters.

The storage pointed to by a BlueData DataTap can be accessed by a Map/Reduce job (or by any other Hadoop-or Spark-based activity in an EPIC virtual node) by using a URI that includes the name of the DataTap.

A DataTap points at the top of some directory hierarchy in the storage container. A URI of the following form can be used to access the root of that hierarchy:

```
dtap://data_connector_name/
```

In this example, `data_connector_name` is the name of the DataTap that you wish to use. You can access files and directories further in the hierarchy by appending path components to the URI:

```
dtap://datatap_name/some_subdirectory/
another_subdirectory/some_file
```

For example, the URI `dtap://mydataconnector/home/mydirectory` means that the data is located within the `/home/mydirectory` directory in the storage that the DataTap named `mydataconnector` points to.

DataTaps exist on a per-tenant basis. This means that a DataTap created for Tenant A cannot be used by Tenant B. You may, however, create a DataTap for Tenant B with the exact same properties as its counterpart for Tenant A, thus allowing both tenants to use the same shared network resource.

Users who have a Tenant Administrator role may view and modify detailed DataTap information. Members may only view general DataTap information and are unable to create, edit, or remove a DataTap.

CAUTION: DATA CONFLICTS MAY OCCUR IF MORE THAN ONE DATATAP POINTS TO A LOCATION BEING USED BY MULTIPLE JOBS AT ONCE.

1.5.2 - Tenant Storage

Tenant storage is a storage location that is shared by all nodes within a given tenant. The Site Administrator configures this service while installing EPIC and can change it at any time thereafter. This storage service can use a local HDFS installation or remote HDFS or NFS system.

Note: If all tenants are created using the same tenant storage service settings, then no tenant can access the storage space of any other tenant.

When a new tenant is created, that tenant automatically receives a DataTap called `TenantStorage` that points at a location within the tenant storage space. This DataTap can be used in the same manner as other DataTaps, but it cannot be edited or deleted.

The `TenantStorage` DataTap points at the top-level directory that a tenant can access within the tenant storage service. The Tenant Administrator can create or edit additional DataTaps that point at or below that directory; however, one cannot create or edit a DataTap that points outside the tenant storage on that particular storage service. (It is of course possible to create and edit DataTaps that point to external services).

If the tenant storage is based on a local HDFS, then the Site Administrator can specify a storage quota for each tenant. EPIC uses the HDFS back-end to enforce this quota, meaning that the quota applies to storage operations that originate from both the EPIC DataTap browser or the nodes within that tenant.

1.5.3 - Node Storage

Node storage is based on each host in the EPIC platform and is used for the volumes that back the root filesystems of virtual nodes. A tenant can optionally be assigned a quota for how much storage the nodes in that tenant can consume.

1.5.4 - Application Path Inputs

Applications running on EPIC virtual clusters will typically accept input arguments that specify one or more storage paths that identify files or directories that either currently exist or are intended to be created by the application. Each path can be specified in one of two ways:

- You can use a UNIX-style file path, such as `/home/directory`. This path refers to a location within the cluster file system. Remember that the cluster file system and all data stored therein will be deleted when the cluster is deleted.
- You can use a DataTap URI, such as `dtap://mydatatap/home/mydirectory`. This path refers to a location within the storage system pointed to by the named DataTap within the same tenant. A Hadoop or Spark application will "mount" a given DataTap before using any paths within that DataTap. If the DataTap changes or is deleted, a running application will not see the effects until the next time it attempts to mount that DataTap.

1.6 - Tenants

Tenants are created by the Site Administrator after installing BlueData EPIC on the cluster platform. The resources available to an EPIC platform are split among the tenants on the platform. Each tenant is allocated a set of resources and restricts access to a set of data to only those users authorized to access the tenant. Resources used by one tenant cannot be used by another tenant. All users who are members of a tenant can access the resources and data objects available to that tenant.

You will need to decide how to create tenants to best suit your organizational needs, such as by:

- **Office Location:** If your organization has multiple office locations, you could choose to create one or more tenants per location. For example, you could create a tenant for the San Francisco office and one for the New York office. EPIC does not take location into account; this is just an example of how you could use a tenant.
- **Department:** You could choose to create one or more tenants for each department, For example, you could create one tenant each for the Manufacturing, Marketing, Research & Development, and Sales departments.
- **Combination:** You could choose to create one tenant by department for each location. For example, you could create a tenant for the Marketing department in San Francisco and another tenant for the Marketing department in New York.

Some of the factors to consider when planning how to create tenants may include:

- **Structure of your organization:** This may include such considerations as the department(s), team(s), and/or function(s) that need to be able to run jobs.
- **Seasonal needs:** Some parts of your organization may have varying needs depending on the time of year. For example, your Accounting department may need to run jobs between January 1 and April 15 each year but have little to no needs at other times of the year.
- **Amount and location(s) of hosts:** The number and location(s) of the hosts that you will use to create an EPIC platform may also be a factor. If your hosts are physically distant from the users who need to run jobs, then network bandwidth may become an important factor as well.
- **Personnel who need EPIC access:** The locations, titles, and job functions of the people who will need to be able to access EPIC at any level (Site Administrator, Tenant Administrator, or Member) may influence how you plan and create tenants.
- **IT policies:** Your organization's IT policies may play a role in determining how you create tenants and who may access them.

- **Regulatory needs:** If your organization deals with regulated products or services (such as pharmaceuticals or financial products), then you may need to create additional tenants to safeguard regulated data and keep it separate from non-regulated data.

These are just a few of the possible criteria you must evaluate when planning how to create tenants. EPIC has the power and flexibility to support the tenants you create regardless of the schema you use. You may create, edit, and delete tenants at any time. However, careful planning for how you will use your EPIC platform that includes the specific tenant(s) your organization will need now and in the future will help you better plan your entire EPIC installation from the number and type of hosts to the tenants you create once EPIC is installed on those nodes.

1.6.1 - Users

A user consists of the following components:

- Login credentials (username and password)
- Role assigned to those credentials

Some of the user-related things you must consider when planning and maintaining your EPIC installation include:

- **Tenants:** The number of tenants and the function(s) each tenant performs will play a direct role in determining how many Tenant Administrator users you will need and, by extension, the number of Member users you will need for each tenant. The reverse is also true, because the number and functions of users needing to run jobs can influence how you create tenants. For example, different levels of confidentiality might require separate tenants.
- **Job functions:** The specific work performed by each user will directly impact the EPIC role they receive. For example, a small organization may designate a single user as the Tenant Administrator for multiple tenants, while a large organization may designate multiple Tenant Administrators per tenant.
- **Security clearances:** You may need to restrict access to information based on each user's security clearance. This can impact both the tenant(s) a user has access to and the role that user has within the tenant(s).

Each user may have a maximum of one role per tenant. For example, if your EPIC installation consists of 20 tenants, then each user may have up to 20 separate roles. A user with more than one role may be a Member of some tenants and a Tenant Administrator of other tenants.

1.6.2 - User Roles

The table on the following page lists the specific functions that can be performed within EPIC and the role(s) that can perform each of those actions.

In the following table:

- **Permission** stands for the right to perform a given action. Users with specific roles receive specific permissions within EPIC.
- **SA** stands for the Site Administrator role.
- **TA** stands for the Tenant Administrator role.

- **M** stands for the Member (non-administrative) role.
- An **X** in a column means that a user with the indicated role can perform the indicated action.
- A blank entry means that a user with the indicated role cannot perform the indicated action.

Permission	SA	TA	M
View a tenant	X	X	
Create a tenant	X		
Edit a tenant	X		
Delete a tenant	X		
Add an EPIC user	X		
Remove an EPIC user	X		
Grant a user site role	X		
Revoke a user site role	X		
Grant a user tenant role	X	X	
Revoke a user tenant role	X	X	
View detailed host info	X		
Manage user authentication	X		
View job information	X	X	X
Enter/exit Lockdown mode	X		
Add a job		X	X
Edit a job		X	X
Delete a job		X	X
View virtual cluster information	X	X	X
Add a virtual cluster		X	X
Edit a virtual cluster		X	X
Delete a virtual cluster		X	X
View detailed DataTap info	X	X	
Add a DataTap		X	
Edit a DataTap		X	
Remove a DataTap		X	
View summary DataTap info		X	X
View virtual node information		X	X
Manage EPIC platform configuration	X		
Create/edit/delete flavor definitions	X		
Install/uninstall/upgrade **App Store** images	X		
Add and manage EPIC Worker hosts	X		
View global usage/health/metrics	X		
View tenant resource usage	X	X	

1.6.3 - User Authentication

Each user has a unique username and password that they must provide in order to login to BlueData EPIC. Authentication is the process by which EPIC matches the user-supplied username and password against the list of authorized users and determines both

- whether to grant access (stored either in the local user database server or in the remote LDAP/Active Directory server), and
- what exact access to allow, in terms of the specific role(s) granted to that user (stored on the EPIC Controller node).

User authentication information is stored on a secure server. EPIC can use either its own internal user database or your existing LDAP or Active Directory server. In either case, the authentication process is the same:

1. A user accesses the EPIC **Login** screen using a Web browser pointed to the IP address of the Controller host.
2. The user enters their username and password in the appropriate fields and attempts to login.
3. EPIC passes the user-supplied username and password to the authentication server.
4. The authentication returns a response that indicates either a valid (allow user to login) or invalid (prevent user from logging in) login attempt.
5. If the login attempt is valid, EPIC will match the user with the role(s) granted to that user and allow the proper access.

Using the internal user database included with EPIC is fast and convenient from an IT perspective. However, it may complicate user administration for various reasons, such as:

- The user may be required to change their password on the rest of the network but this change will not apply to EPIC.
- A user who is removed from the network (such as when they leave the organization) must be removed from EPIC separately.

Connecting EPIC to your existing user authentication server requires you to supply some information about that server when installing EPIC. Contact your user administrator for the following information:

- **LDAP:** LDAP Host, User Attribute, User Subtree DN
- **Active Directory:** AD Host, User Attribute, User Subtree DN

1.7 - High Availability

EPIC supports two levels of High Availability protection:

- **BlueData EPIC High Availability:** See below.
- **Virtual Cluster High Availability:** See *"Virtual Cluster High Availability" on page 31*.

1.7.1 - BlueData EPIC High Availability

EPIC supports High Availability functionality that protects your EPIC platform against the failure of the Controller host. Your EPIC platform must conform to all of the requirements listed in *"High Availability Requirements" on page 14* in order to support this feature.

High Availability requires designating two Worker hosts as the Shadow Controller and Arbiter, respectively. If the Controller host fails, then EPIC will failover to the Shadow Controller host within approximately two or three minutes, and a warning will appear at the top of the EPIC screens. You may need to log back in to EPIC if this occurs.

Each host in the EPIC platform has its own IP address. If the Controller host fails, then attempting to access the Shadow Controller host using the same IP address will fail. Similarly, accessing the Shadow Controller host using that node's IP address will fail once the Controller host recovers. To avoid this problem, you must specify a cluster IP address that is bonded to the node acting as the Controller host, and then log into EPIC using that cluster IP address. EPIC will automatically connect you to the Controller host (if the EPIC platform is running normally) or to the Shadow Controller host with a warning message (if the Controller host has failed and triggered the High Availability protection).

EPIC High Availability protects against the failure of any one of the three hosts being used to provide this protection. The warning message will therefore appear if either the Shadow Controller or Arbiter host fails, even if the Controller host is functioning properly.

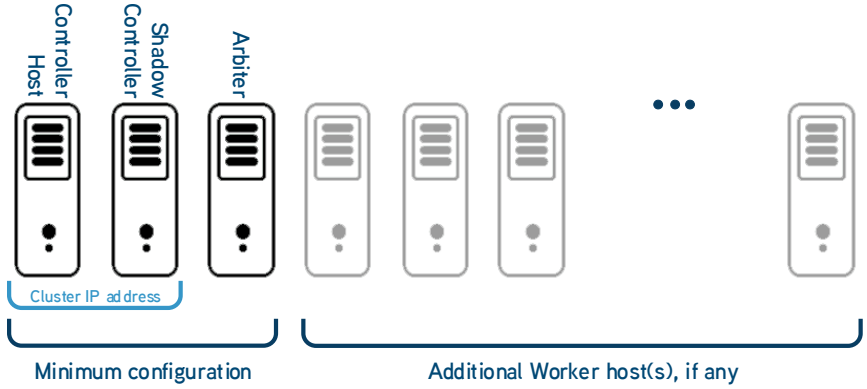

Figure 1.2: BlueData EPIC platform configured for High Availability

When High Availability is enabled:

- The Controller host manages the EPIC platform, and the Shadow Controller and Arbiter hosts function as Worker hosts.

- If the Controller host fails, then the Arbiter host switches management of the EPIC Platform to the Standby Controller host, and the EPIC platform is no longer protected against any failure of the Shadow Controller host(s).
- If the Arbiter host fails, then the Controller host continues working, and the EPIC platform is not protected against any further failure of the Controller or Shadow Controller host(s).

When a failure of a High Availability host occurs, EPIC takes the following actions:

- If the Controller host has failed, then EPIC fails over to the Standby Controller host and begins running in a degraded state. This process usually takes 2-3 minutes, during which you will not be able to log in to EPIC.
- If the Shadow Controller or Arbiter host fails, then EPIC keeps running on the Controller host in a degraded state.
- A message appears in the upper right corner of the EPIC interface warning you that the system is running in a degraded state. Use the **Service Status** tab of the Site Administrator **Dashboard** (see the *User/Administrator Guide*) to see which host has failed and which services are down.
- EPIC analyzes the root cause of the host failure and attempts to recover the failed host automatically. If recovery is possible, then the failed host will come back up and EPIC will resume normal operation.
- If EPIC cannot resolve the problem, then the affected host will be left in an error state and you will need to manually diagnose and repair the problem (if possible) and then reboot that host. If rebooting solves the problem, then the failed host will come back up and EPIC will resume normal operation. If this does not solve the problem, then you will need to contact BlueData Technical Support for assistance.

Enabling High Availability protection in EPIC is a two-stage process: First, you must designate one Worker host as the Shadow Controller host in the **Installation** tab of the **Cluster Installation** screen. This is a one-time assignment; you cannot transfer the Shadow Controller role to another Worker host. Second, you must enable High Availability protection and then assign the Arbiter role to a third Worker host in the **HA Settings** tab of the **Settings** screen. Please see the *EPIC Installation Guide* and the *User/Administrator Guide* for more information.

EPIC does not support enabling High Availability if any virtual clusters already exist. If you create one or more virtual clusters before deciding to enable High Availability, then you should delete those clusters before proceeding with the High Availability. In general, you should implement High Availability when first installing EPIC as described in the *EPIC Installation Guide* and the *User/Administrator Guide*.

1.7.2 - Virtual Cluster High Availability

Some Hadoop distributions and MR types allow you to create a transient or persistent cluster with High Availability protection. This is separate and distinct from the EPIC platform High Availability described above, as follows:

- A cluster with High Availability enabled for that virtual cluster is still dependent on the EPIC platform. If the Controller host on an EPIC platform without High Availability fails, then the virtual cluster will also fail.
- If the EPIC platform has High Availability enabled and the Master node of a virtual cluster fails, then that virtual cluster will fail if High Availability for that virtual cluster was not enabled when that virtual cluster was created.

The following table displays the relationship between virtual cluster and EPIC platform High Availability protection under a variety of scenarios:

Failure Type	No HA	EPIC HA only	Cluster HA only	EPIC & Cluster HA
EPIC Controller host down; virtual cluster Master node up.	X	**protected**	X	**protected**
EPIC Controller host up; virtual cluster Master down.	X	X	**protected**	**protected**
EPIC Controller host up; Other virtual cluster node down.	**protected**	**protected**	**protected**	**protected**

1.8 - About This Manual

This section describes the formatting conventions and information contained in this manual.

1.8.1 - Organization

This manual introduces EPIC at a high level, including key benefits, definitions, architecture, and requirements. This chapter also describes how this manual is formatted and organized.

1.8.2 - Formatting Conventions

This manual uses several formatting conventions to present information of special importance.

Lists of items, points to consider, or procedures that do not need to be performed in a specific order appear in bullet format:

- Item 1
- Item 2

Procedures that must be followed in a specific order appear in numbered steps:

1. Perform this step first.
2. Perform this step second.

Specific keyboard keys are depicted in square brackets and are capitalized, for example: [ESC]. If more than one key should be pressed simultaneously, the notation will appear as [KEY1]+[KEY 2], for example [ALT]+[F4].

Interface elements such as document titles, fields, windows, tabs, buttons, commands, options, and icons appear in **bold** text.

Specific commands appear in standard `Courier` font. Sequences of commands appear in the order in which you should execute them and include horizontal or vertical spaces between commands. Plain-text responses from the system appear in bold **`Courier`** font.

This manual also contains important safety information and instructions in specially formatted callouts with accompanying graphic symbols. These callouts and their symbols appear as follows throughout the manual:

CAUTION: CAUTIONS ALERT YOU TO THE POSSIBILITY OF A SERIOUS ERROR, DATA LOSS, OR OTHER ADVERSE CONDITION.

Note: Notes provide helpful information.

The **Note** and **Caution** icons are blue in the main chapter, and gray in the appendices.

1.9 - Additional Information

This section lists related documentation and provides information on contacting BlueData, Inc.

1.9.1 - Related Documentation

Please refer to the following documents for additional information:

- **EPIC Lite Installation Guide:** This guide helps you install EPIC Lite, the free demonstration version of EPIC, on a single host.
- **EPIC Installation Guide:** This guide contains instructions for installing the full version of EPIC on your network.
- **User/Administrator Guide:** This guide describes the EPIC interface for Site Administrator, Tenant Administrator, and Member users.
- **Running Applications in EPIC:** This guide provides a brief overview of how to input data, run jobs, and access job output within EPIC.
- **Deployment Guide:** Certain platforms have additional requirements and/or procedures for installing and running EPIC.
- **App Store Image Authoring Guide:** Describes how Site Administrators can author new images and make them available in their local instance of the EPIC **App Store**.

1.9.2 - Contact Information

You may contact BlueData Software, Inc. at the following addresses:

BlueData Software, Inc.
3979 Freedom Circle, Suite 850
Santa Clara, California 95054
Email: info@bluedata.com
Website: www.bluedata.com

1.9.3 - End User License Agreement

Please review the EPIC End User License Agreement (EULA). See *"End User License Agreement" on page 35*.

This page intentionally left blank.

2 - End User License Agreement

BLUEDATA SOFTWARE INC. END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE INSTALLING OR OTHERWISE USING EPIC OR EPIC Lite SOFTWARE ("SOFTWARE" OR "EVALUATION SOFTWARE") AS PROVIDED HEREWITH BY BLUEDATA SOFTWARE INC. BY INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS DOCUMENT, YOU ARE NOT AUTHORIZED TO INSTALL OR USE THIS SOFTWARE. IF YOU WISH TO USE THE SOFTWARE AS AN EMPLOYEE, CONTRACTOR, OR AGENT OF A CORPORATION, PARTNERSHIP OR SIMILAR ENTITY, THEN YOU MUST BE AUTHORIZED TO SIGN FOR AND BIND THE ENTITY IN ORDER TO ACCEPT THE TERMS OF THIS AGREEMENT.

This EULA is entered into immediately by and between BlueData Software, Inc. ("Company"), and the customer (individual or entity) that has downloaded or otherwise procured the licensed Software for use as an end user ("you" or "Evaluator") with respect to the Company Software that Company provides to Evaluator under this EULA Agreement. This Agreement covers any Software and Documentation.

1. **Limited License:** Subject to the terms and conditions of this EULA, Company grants you a limited, non-exclusive, non-transferable, personal license during the Evaluation Period to install and internally use the Software solely for testing purposes to determine the compatibility and interoperability of the Software with your hardware and software and for no other purpose. You must limit access to and use of the Software by only your employees with the need to use the Software for the foregoing purpose ("Authorized Users").

2. **Proprietary Rights; Restrictions on Use:** The Software is licensed (not sold) to you by Company. You acknowledge and agree that the Software is copyrighted and contains materials that are protected by copyright, trade secret and other laws and international treaty provisions relating to proprietary rights. You may not remove, deface, or obscure any of Company's or its suppliers' proprietary rights notices on or in the Software or on output generated by the Software. You may not, nor may you permit, any third party to: (a) decompile, reverse engineer, disassemble, or otherwise attempt to derive the source code, algorithms or underlying ideas, design, or architecture of the Software; (b) modify, translate, or create derivative works of the Software; or (c) rent, lease, loan, distribute, transmit, assign, or transfer the Software to any third party, or provide access to or use of the Software by any third party, including any agent of yours other than Authorized Users. Without Company's prior written consent, you shall not disclose any information relating to features, performance, or operation of the Software (including any benchmarking or other testing results) to any third party, nor use any of such information other than for purposes permitted under Section 1, above.

   You acknowledge and agree that any unauthorized use, transfer, sublicensing, or disclosure of the Software, or other violation of this License, would cause irreparable injury to Company, and under such circumstances, Company shall be entitled to equitable relief, without posting bond or other security, including but not limited to, preliminary and permanent injunctive relief.

All rights, title, and interest in and to the Evaluation Software, the Feedback, accompanying materials, and all proprietary information contained therein, are owned by Company and are protected by copyright, trademark, patent and trade secret law, and international treaties. Evaluator will transfer and assign, and hereby does irrevocably transfer and assign, to Company all right, title, and interest, including all intellectual property rights, that Evaluator may have or acquire in the Feedback, and Evaluator will provide reasonable assistance to Company to effect such assignment. All rights not specifically granted in this Agreement are reserved by Company.

3. **Consent to Use of Data:** Evaluator agrees that BlueData may collect and use technical data and related information, including but not limited to technical information about your computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to Evaluator (if any) related to the Licensed Application. BlueData may use this information, as long as it is in a form that does not personally identify Evaluator, to improve its products or to provide services or technologies.

4. **Termination:** This Agreement shall be effective immediately and shall expire at the end of the Evaluation Period limited to 90 days, unless earlier terminated. Your rights under this EULA will terminate automatically without notice from Company if you fail to comply with any term(s) of this EULA. In addition, Company may terminate this Agreement at any time upon notice to you. Immediately upon any termination, (a) the license granted under Section 1 above terminates, and (b) you must destroy the Software, including all copies and portions thereof, in your possession or under your control. You must certify such destruction in writing to Company within 5 days of termination. If you choose to purchase Company's Products, you shall notify Company on the date of expiration or termination of this EULA and such purchase shall be pursuant to Company's then-current terms and conditions for the purchase of Company's products. However, the Company assumes no obligation under this EULA to introduce the Software as a commercial product.

5. **Indemnification:** You shall indemnify, defend and hold harmless Company from any and all damages, liabilities, costs and expenses (including but not limited to reasonable attorneys' fees) incurred by Company arising from or related to your use of Company's products, including without limitation the Evaluation Software.

6. **Disclaimer; Limitation of Liability:** YOUR USE OF THE SOFTWARE IS AT YOUR SOLE RISK. THE SOFTWARE IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND AND COMPANY AND COMPANY'S LICENSOR(S) EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE, NOR DOES THE COMPANY PROVIDE ANY WARRANTY OR INDEMNIFICATION WITH RESPECT TO VIOLATION OF THE RIGHTS OF THIRD PARTIES. IN ADDITION, COMPANY DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE,

SHALL COMPANY BE LIABLE FOR ANY DIRECT, INCIDENTAL, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUD¬ING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS), OR FOR THE COST OF PROCURING OTHER SOFTWARE PRODUCTS OR SERVICES, ARISING OUT OF OR RELATING TO THIS EULA, EVEN IF COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL COMPANY BE LIABLE FOR CUMULATIVE DAMAGES OF ANY KIND IN EXCESS OF FIVE HUNDRED DOLLARS ($500).

7. **Miscellaneous:** This EULA is governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles. Any controversy or claim arising out of or relating to this EULA, or the breach thereof, shall be determined by arbitration administered by the International Centre for Dispute Resolution in accordance with its International Arbitration Rules, conducted in Santa Clara Country, California, U.S.A. There shall be one arbitrator, and the language of the arbitration shall be in English. If any provision of this EULA is held to be invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this EULA will remain in full force. Failure of a party to enforce any provision of this EULA shall not constitute and shall not be construed as a waiver of such provision or of the right to enforce such provision. Company reserves the right, and you agree that Company may, by itself or through its authorized representatives, inspect your systems, networks, hardware, books, and other records in any form to verify your compliance with this EULA, upon reasonable prior notice to you. This EULA sets forth the entire agreement between the parties with respect to your use of the Software and supersedes all prior or contemporaneous representations or understandings regarding such subject matter. No modification or amendment of this EULA will be binding unless accepted and agreed by an authorized representative of Company.

3 - Third Party Licenses

EPIC includes the following open-source components that are distributed according to the terms of the licenses:

- **erlang-uuid:** Copyright 2008 by Travis Vachon and licensed under the BSD 3-Clause License, which is available from *http://opensource.org/licenses/BSD-3-Clause*
- **mochiweb:** Copyright 2007 by Mochi Media, Inc. and licensed under the MIT License, which is available from *http://opensource.org/licenses/MIT*
- **sgte:** Copyright 2007 by Filippo Pacini and licensed under the Mozilla Public License 1.1, which is available from *http://opensource.org/licenses/MPL-1.1*

This page intentionally left blank.

About EPIC Guide, version 2.4 (10/2016)

Contact Information:

BlueData Software, Inc.
3979 Freedom Circle, Suite 850
Santa Clara, California 95054

Email: info@bluedata.com
Website: www.bluedata.com