DigitalEdge™

Getting Started

on a Private Cloud

Version 1.3

September 2014

leidos

DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY

The Software accompanying this Documentation is provided with the Limited Warranty contained in the License Agreement for that Software. Leidos, its affiliates and suppliers, disclaim all warranties that the Software will perform as expected or desired on any machine or in any environment. Leidos, its affiliates and suppliers, further disclaim any warranties that this Documentation is complete, accurate, or error-free. Both the Software and the Documentation are subject to updates or changes at Leidos' sole discretion. LEIDOS, ITS LICENSORS AND SUPPLIERS MAKE NO OTHER WARRANTIES, WRITTEN OR ORAL, EXPRESS OR IMPLIED RELATING TO THE PRODUCTS, SOFTWARE, AND DOCUMENTATION. LEIDOS, ITS LICENSORS AND SUPPLIERS DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, USE, TITLE, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. In no event shall Leidos, its affiliates or suppliers, be liable to the End User for any consequential, incidental, indirect, exemplary, punitive, or special damages (including lost profits, lost data, or cost of substitute goods or services) related to or arising out of the use of this Software and Documentation however caused and whether such damages are based in tort (including negligence), contract, or otherwise, and regardless of whether Leidos, its affiliates or suppliers, has been advised of the possibility of such damages in advance. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS, END USER ACKNOWLEDGES AND AGREES THAT LEIDOS AND ITS AFFILIATES AND SUPPLIERS IN NO EVENT SHALL BE RESPONSIBLE OR LIABLE TO THE END USER FOR ANY AMOUNTS IN EXCESS OF THE FEES PAID BY THE END USER TO LEIDOS. LEIDOS SHALL NOT BE RESPONSIBLE FOR ANY MATTER BEYOND ITS REASONABLE CONTROL.

LEIDOS PROPRIETARY INFORMATION

This document contains Leidos Proprietary Information. It may be used by recipient only for the purpose for which it was transmitted and will be returned or destroyed upon request or when no longer needed by recipient. It may not be copied or communicated without the advance written consent of Leidos. This document contains trade secrets and commercial or financial information which are privileged and confidential and exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552.

TRADEMARKS AND ACKNOWLEDGMENTS

Private installations of DigitalEdge are powered by Eucalyptus®.

Public cloud installations of DigitalEdge are powered by Amazon Web Services™.

The following list includes all trademarks that are referenced throughout the DigitalEdge documentation suite.

Adobe, Flash, PDF, and Shockwave are either registered trademarks or trademarks of Adobe Systems Incorporate in the United States and/or other countries.

Amazon Web Services, AWS, Amazon Elastic Compute Cloud, Amazon EC2, EC2, Amazon Simple Storage Service, Amazon S3, Amazon VPC, Amazon DynamoDB, Amazon Route 53, the "Powered by Amazon Web Services" logo, are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

Apache, Archiva, Cassandra, Hadoop, Hive, HBase, Hue, Lucene, Maven, Apache Phoenix, Solr, Zoie, ActiveMQ are all trademarks of The Apache Software Foundation.

ArcSight is a registered trademark of ArcSight, Inc.

CAS is copyright 2007, JA-SIG, Inc.

CentOS is a trademark of the CentOS Project.

Cloudera is a registered trademark of Cloudera, Inc.

CloudShield is a registered trademark of CloudShield Technologies, Inc. in the U.S. and/or other countries.

CTools are open-source tools produced and managed by Webdetails Consulting Company in Portugal.

Drupal is a registered trademark of Dries Buytaert.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.

Eucalyptus and Walrus are registered trademarks of Eucalyptus Systems, Inc.

CONTACT INFORMATION

Leidos Franklin Center
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Email: DigitalEdgeSupport@Leidos.com

DigitalEdge Technical Support: 443-367-7770

DigitalEdge Sales Support: 443-367-7800

To submit ideas or feedback: https://www9.v1ideas.com/digitaledge/welcome

Contents

Chapter 1: Introduction **1**

DigitalEdge Platform 1

Product documentation 2

Typographical conventions 2

Chapter 2: DigitalEdge Architecture **4**

Tenant Management System (TMS) 5

Chapter 3: Prerequisites **7**

Hardware components 7

Software components 8

DNS requirements 8

Chapter 4: Installation Roadmap **11**

Platform architecture 12

Chapter 5: Installing CentOS **13**

Chapter 6: Installing Eucalyptus **16**

Installing Eucalyptus on the Cloud Controller 17

Registering the Cloud Controller 19

Installing Eucalyptus on the Cluster Controller 19

Configuring the Cluster Controller 20

Registering the Cluster Controller 21

Installing Eucalyptus on a Node Controller 22

Configuring a Node Controller 23

Registering a Node Controller 25

Preparing for the DigitalEdge installation 25

Chapter 7: Installing DigitalEdge on Eucalyptus **27**

Logging on to DigitalEdge 31

Chapter 8: Using the Management Console as a TMS Administrator **32**

Logging in ... 32
Managing tenants ... 34
Creating user logins and credentials for TMS ... 36
Allocating tenant space in the Master Repository ... 36
Creating a tenant gateway node ... 37
Creating DNS entries ... 37
Creating security rules at the TMS level ... 38
Synchronizing the system ... 39
Logging out ... 39
Chapter 9: Creating Tenant Accounts ... 41
Chapter 10: Creating a New EMI ... 45
Chapter 11: Installing a Software Upgrade ... 49
Chapter 12: Restarting the Gateway ... 53
Appendix A: Terminology ... 58
Appendix B: What Each Node Does ... 61
Appendix C: Alternative to DNS Forwarding ... 64
Appendix D: What a Full Installation Does ... 66
Appendix E: What the Tenant Installer Does ... 68
Appendix F: What the EMI Installer Does ... 69
Appendix G: What the Software Upgrade Installer Does ... 70
Appendix H: What the Gateway Restart Install Option Does ... 71
Appendix I: Install Hybridfox ... 72
Appendix J: Create PuTTY PPK ... 73
Appendix K: Create Environment for Euca2ools ... 74
Index ... 75

Chapter 1: Introduction

DigitalEdge is a highly configurable software platform providing real-time analytics of big data in motion for cyber-security. This *Getting Started Guide* helps you with:

- Understanding the high level platform architecture
- Installing the operating system and cloud software
- Setting up DigitalEdge
- Working with tenant accounts

Before plunging in, be sure to read the *Overview Guide*; it describes the DigitalEdge architecture, concepts, and terminology. These instructions assume you are familiar with those concepts.

This *Getting Started Guide* helps you configure the servers and network interfaces required for the DigitalEdge platform.

Once you have the platform set up and installed, use the *Configuration Guide* to plan, configure, and build the DigitalEdge data models, work flow, and plug-in components. Then, use the *Operations Guide* to manage and maintain DigitalEdge.

DigitalEdge Platform

DigitalEdge is an advanced, customizable software platform that enables a full lifecycle from data discovery to actionable intelligence. It provides enhanced ingestion of structured and unstructured data into customized work flows for real-time situational awareness. The processing pipeline can be built with custom plug-ins to transport source data, parse and enrich data, and load data into big data repositories or enterprise systems. Data can be queried, analyzed, or reported in near real-time. In short, DigitalEdge integrates ETL (extract, transform, and load) real-time stream processing, and big data NoSQL ("Not Only SQL") stores into a high performance analytic system. Instead of waiting hours for actionable data and reports, analysts can now achieve near real-time situational awareness. DigitalEdge provides a rapid response to changing environments.

DigitalEdge is Java based and provides an extensible architecture, APIs, and development kits. The platform provides plug-in architecture for sharing components in a problem domain. DigitalEdge can be provisioned as a fully integrated solution on x86 hardware, or off-premise on a public cloud. DigitalEdge runs as a platform-as-a-service (PaaS) in:

- The Amazon AWS™ public Elastic Compute Cloud™ (EC2), using the Virtual Private Cloud™ (VPC™) environment for security
- A private cloud using Eucalyptus® in your own data center

Cloud computing provides on-demand network access to a shared pool of configurable resources such as servers, storage, applications, and services. Resources are automatically provisioned with minimal intervention, scaling up during peak times and scaling back as needs decrease.

Product documentation

DigitalEdge is a complex big data platform. The system comes with a complete set of documentation in PDF and HTML5 formats to help you master DigitalEdge:

Document	Use	Audience
Overview Guide	Basic information about the DigitalEdge platform, including architecture, concepts, and terminology; a must-read before working with any aspect of DigitalEdge	Anyone working with DigitalEdge in any capacity
Configuration Guide	Instructions for defining data models and building processing pipelines	Data Specialists, DigitalEdge Administrators
Operations Guide	Daily administration information, covering monitoring, managing, and modifying the platform	DigitalEdge Administrators
Cookbook	Guidelines and procedures for many common tasks in a DigitalEdge system	DigitalEdge Administrators
DigitalEdge SDK Guide	Reference for building custom plug-in components	Developers
Alerts API Guide	Reference for specifying data triggers and notifications for an alerting capability	Developers
Search API Guide	Reference for providing search services on a Lucene data sink node	Developers

Typographical conventions

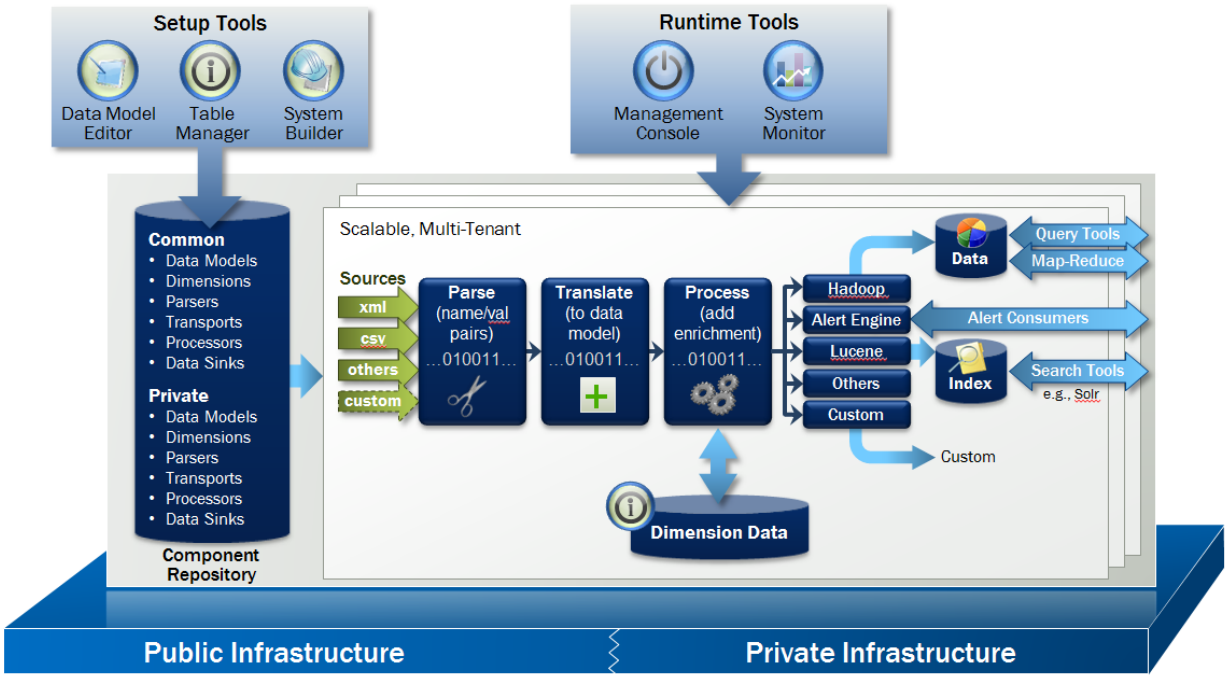
The following style conventions are used throughout this documentation:

Type of Information	Style in Documentation
Code, commands, filenames	`code`
Cross references	Click to see this topic
Emphasis	*important point*
Hyperlinks	Click to go to this site
Notes, warnings, tips	
References to other documents	*Document Title*
Sample code blocks	`code`

Type of Information	Style in Documentation
Troubleshooting issue or problem	
Troubleshooting solution	
User input	*Italics*
User interface labels and controls	**Bold**
Variables	<*change-this-name*>

Chapter 2: DigitalEdge Architecture

DigitalEdge is highly configurable, with a plug-in architecture that lets you swap components in and out. Plug-in components are stored in the Component Repository. The DigitalEdge system architecture is designed as follows:



Data moves through system processors which are configured and customized with the DigitalEdge Setup Tools. System Builder builds and assembles the components into a processing pipeline. The processing pipeline is completely configurable with the Setup Tools.The data flow includes these steps:

1. Transports grab data from data sources and feed the data into DigitalEdge.
2. Data is extracted by parsers.
3. The fusion engine translates and normalizes the data to the DigitalEdge input model.
4. The enrichment engine adds dimensional data and algorithmic enrichments to provide context and meaning to data, resulting in all relevant data being integrated into one record
5. Data is processed and stored in persistent data sinks managed by DigitalEdge (Hadoop, Hive, HBase, MongoDB, etc.) or sent to other data sinks for post-processing (indexing, alerting, etc.). Data can also be sent to systems outside of DigitalEdge.
6. Various web apps makes the data accessible in several ways:
    - Indexed data is searchable through the Search API or the Search app.
    - Configurable situational information is sent to users by the alerting engine.
    - Data can be viewed in dashboards or other external applications.

Tenant Management System (TMS)

The Tenant Management System is the DigitalEdge application for creating and managing tenant accounts.

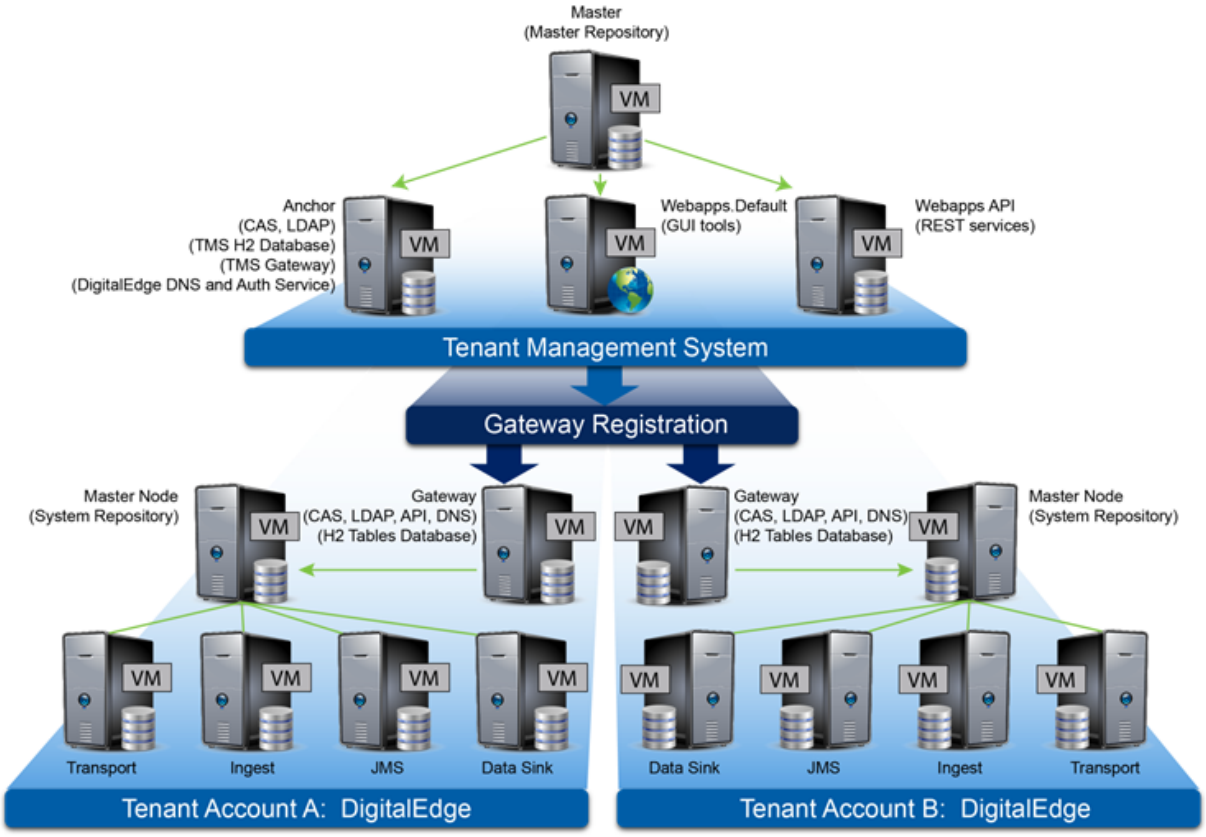
The DigitalEdge TMS is set up at your organization and controlled by a TMS Administrator. A *tenant account* can represent a department, a project, or an organizational group that matches your business needs. Tenants can create independent systems or integrate systems between tenant accounts. They can share plug-in components, and can create private plug-in components as needed.

A *primary tenant* is the first tenant (usually the DigitalEdge Administrator) created in an account. The primary tenant owns all the resources: the system repository, LDAP, the tenant database, etc. One or more *secondary tenants* may be created in an account. All secondary tenants share the account resources that are owned by their primary tenant (system repository, LDAP, etc.), share and see all systems created under an account, and have the same privileges as the primary tenant. But secondary tenants have different logon credentials for security purposes.

Logically, TMS is above the tenant accounts. TMS provides administrative services at an oversight level through the Management Console to:

- Create new tenant accounts
- Manage, set up, and start tenant applications
- Manage user identities
- Store and manage the DigitalEdge private components
- Navigate to other DigitalEdge tools
- View system logs
- Provide an additional level of security

From a high level perspective, TMS and tenant accounts interact as follows:



- The DigitalEdge installer launches TMS at the Eucalyptus cloud level.
- The TMS Master node sets up and launches all the TMS nodes.
- The TMS Administrator creates new tenant accounts and the DigitalEdge Installer creates the Gateway node.
- The DigitalEdge Administrator builds and starts up and DigitalEdge systems.
- The tenant's DigitalEdge Gateway node spawns the tenant's Master node for new systems.
- The tenant's Master node launches and manages all other nodes for DigitalEdge systems in the tenant account.

This diagram represents the initialization of a basic DigitalEdge system. Depending on the needs of a tenant's system, during DigitalEdge configuration, the DigitalEdge Administrator may also configure and start up:

- Multiple instances of transport, ingest, JMS, or data sink nodes
- Alerting node(s)
- Search node(s)
- User applications

Chapter 3: Prerequisites

The following components are required before you start to install the system and DigitalEdge. Check with Leidos for any items that you do not have in hand.

Hardware components

DigitalEdge is designed to run on a Eucalyptus infrastructure-as-a-service (IaaS) platform, which can run on any AMD or Intel x86 hardware. For installations on VMware, please contact your DigitalEdge Deployment Engineer.Leidos recommends the following for a minimum Eucalyptus hardware base:

- Two controller servers with at least eight cores, 2.4GHz, 32GB RAM, 500GB disk
- At least one node server with at least eight cores, 2.4GHz, 128 GB, 300GB disk
- Windows client PC to run and to access DigitalEdge

Additional hardware is required for high availability, redundant isolated front end controllers, redundant network switches, SAN, etc. Also, node servers must be sized to data rates. Hardware components should meet the following specifications:

- Physical machines, not virtual machines, for all Eucalyptus components (Cloud Controller, Walrus, Cluster Controller, Storage Controller, Node Controller, and nodes)
    - Running an Intel or AMD CPU with a minimum of two 2 GHz cores
    - Minimum of 30 GB storage
    - Minimum of 100 GB for Walrus and the Storage Controller
    - 50-100 GB per Node Controller
    - Minimum of 4 GB RAM per machine
    - Minimum of 1 Network Interface Card per component (the Cluster Controller should have 2)
    - Internal gigabit connectivity between servers in rack or on the local network
- As of DigitalEdge 1.2, separate SAN or network attached storage is supported. Contact your DigitalEdge Deployment Engineer for details.
- CentOS 6.4+ operating system and Eucalyptus 3.2.2+ installed and configured the on all servers, with synchronized clocks, and running Hypervisor
- Internet connectivity to access the Eucalyptus installer package, or Eucalyptus installer on a CD
- DNS forwarder for DigitalEdge. If you are not using a forwarder, you will need to know the third IP address in the public address range assigned in the Eucalyptus configuration file (see your Eucalyptus administrator). The third IP address defaults to use as the DNS resolver.

Contact Technical Support at DigitalEdgeSupport@Leidos.com for custom hardware recommendations based on system sizing.

Software components

Before getting started, you will need the following software:

- Eucalyptus® 3.2.2+ (open source or Enterprise edition)
- CentOS 6.4+
- Java 1.6
- Hypervisor: KVM (Kernel-Based Virtual Machine)
- Web browser recommendations: the latest version of Firefox (minimally, Extended Support Release version 17 or 24) or Chrome (minimally, version 21)
- Shockwave® (Flash®) Player: for DigitalEdge web applications
- PuTTY: or a similar a tool to manage SSH connections
- Hybridfox 1.7+: An optional Firefox extension to launch new instances, mount volumes, manage images and security groups, and map IP addresses in either the Amazon AWS™ or Eucalyptus® environments (See "Install Hybridfox" on page 72)
- dos2unix utility: for the DigitalEdge installer
- A user account other than root with sudo access for installing DigitalEdge

You should have the following files from Leidos:

- <de_installer>.exe: The DigitalEdge installation program
- *<de_sw_version_#>*.tar.gz: DigitalEdge software; the file is named with the version number of the DigitalEdge software
- A link to an Amazon Machine Image (AMI) for DigitalEdge: a pre-configured system image and virtual application from which a Eucalyptus Machine Image (EMI) will be constructed

DNS requirements

DigitalEdge should have DNS set up as follows to support domain name resolution.

Each Eucalyptus implementation should have a subdomain created off your internal namespace for DigitalEdge. You should configure a Forwarder for your corporate DNS server to send all queries for this subdomain to a fixed IP address that resides within the DigitalEdge environment, allowing users on the network to resolve any of the DigitalEdge application servers. This configuration lets you create systems within your DigitalEdge environment that are immediately accessible by name.

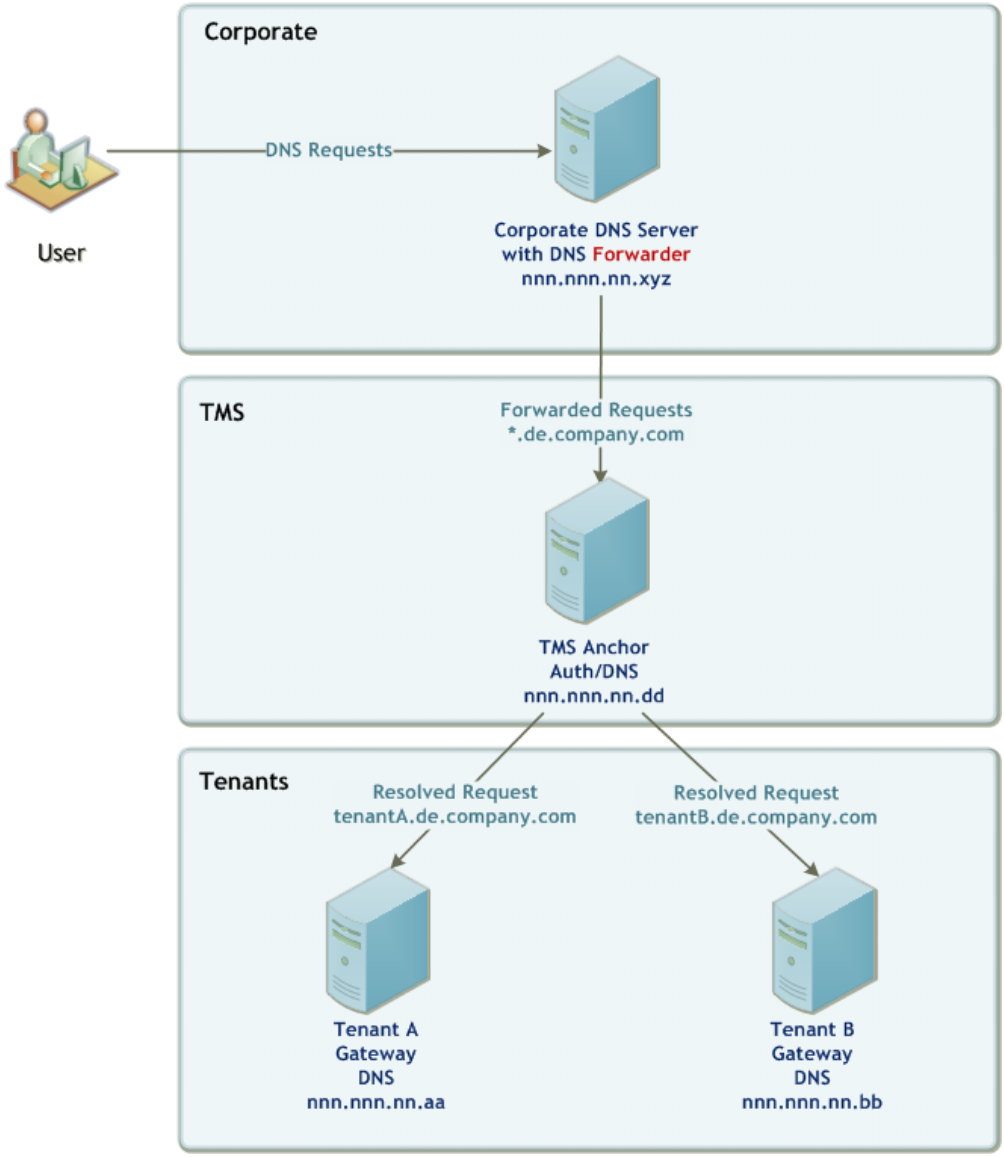
A DNS Forwarder is recommended by DigitalEdge for several reasons:

- To implement security using SSL based on DNS
- To create all certificates with just one domain name (using SSL or a certificate authority of

your choice)

- To implement SSL everywhere within DigitalEdge with just one domain name

By implementing a Forwarder, you will simply be forwarding all DigitalEdge requests to one unique domain name. You will never have to change the domain name in the Forwarder because DigitalEdge resolves the requests and assigns elastic IP addresses at the TMS DNS level.



All DigitalEdge instances that are publicly facing have interfaces that use SSL. This includes:

- Webapps
- JMS external instance

- Data sinks
- Transports

Each instance or process is bound to a DNS suffix. So the completely resolved DNS name consists of the instance name + tenant name + TMS domain name. For example:

instance.name.tenant.de.company.com

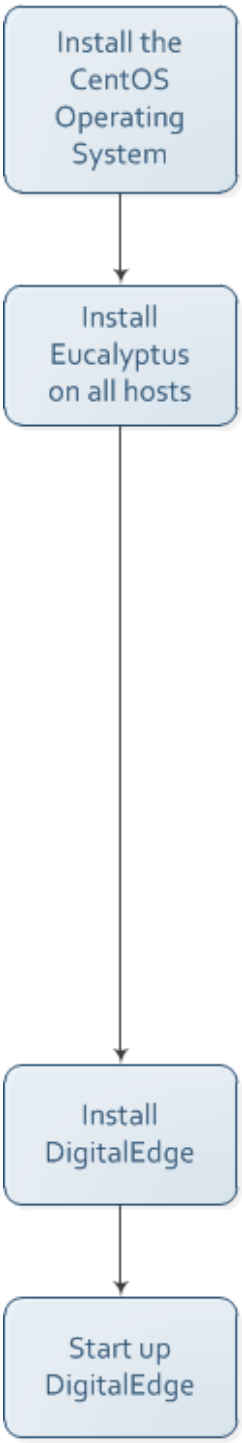
webapp.tenantA.de.company.com

jms-ext-node.tenantB.de.company.com

If your organization is not able to create a DNS forwarder for the DigitalEdge subdomain on Eucalyptus, after you have installed and configured DigitalEdge, you can assign an elastic IP using the DigitalEdge **System Builder**. In this case, DigitalEdge will use IP addresses instead of DNS to access all its applications. Note that this solution may not be ideal for end users who prefer entering a name rather than remembering IP numbers. See "Alternative to DNS Forwarding" on page 64

Chapter 4: Installation Roadmap

Getting started with DigitalEdge on a private cloud involves the installation and setup of several components:



See "Installing CentOS" on page 13

See "Installing Eucalyptus" on page 16

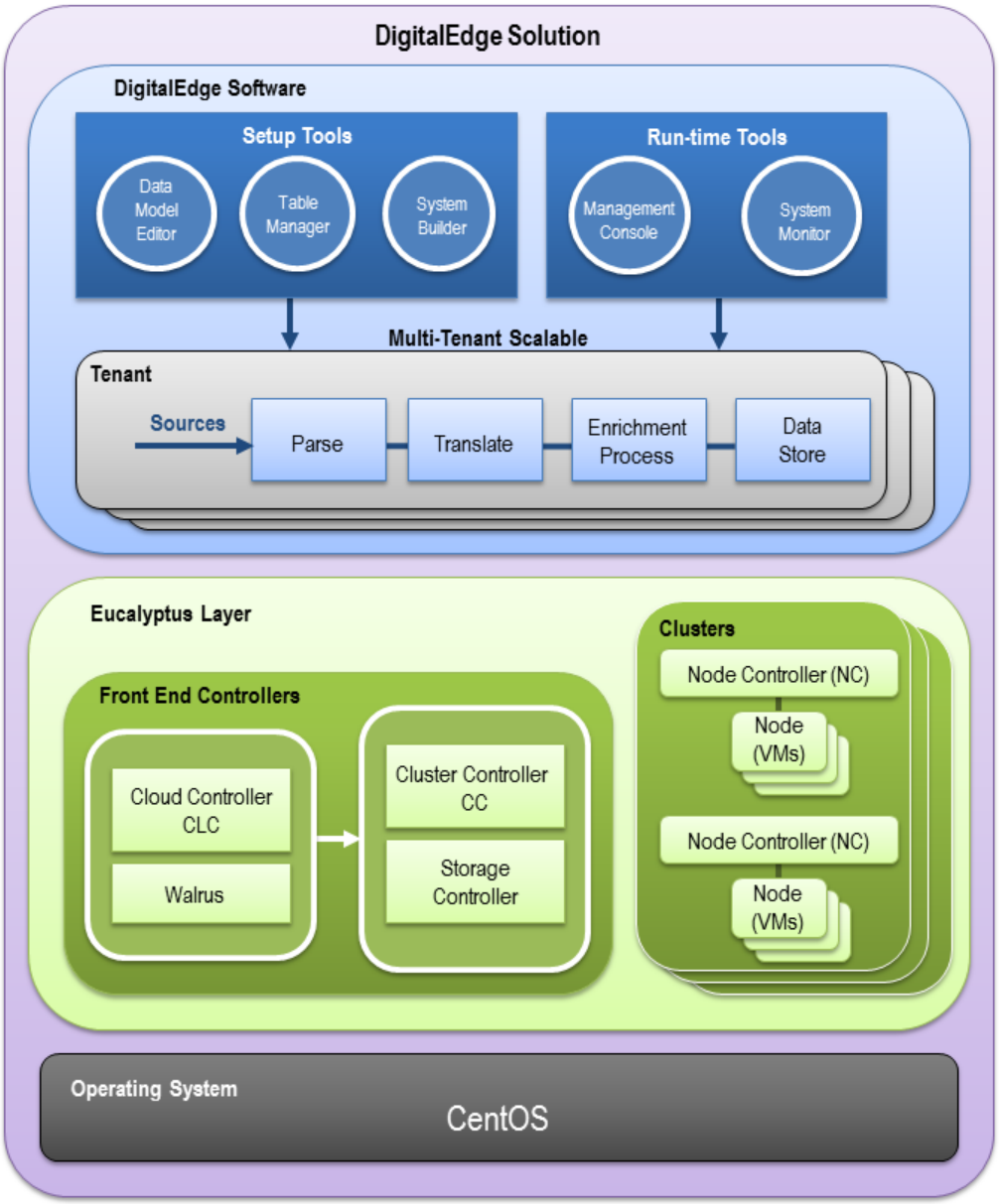
- See "Installing Eucalyptus on the Cloud Controller" on page 17
- See "Registering the Cloud Controller" on page 19
- See "Installing Eucalyptus on the Cluster Controller" on page 19
- See "Configuring the Cluster Controller" on page 20
- See "Registering the Cluster Controller" on page 21
- See "Installing Eucalyptus on a Node Controller" on page 22
- See "Configuring a Node Controller" on page 23
- See "Registering a Node Controller" on page 25
- See "Preparing for the DigitalEdge installation" on page 25

See "Installing DigitalEdge on Eucalyptus" on page 27

See "Logging on to DigitalEdge" on page 31

Platform architecture

DigitalEdge runs as a platform-as-a-service (PaaS) on the Eucalyptus cloud software and the CentOS operating system. The basic configuration can be depicted as follows:



Chapter 5: Installing CentOS

The DigitalEdge platform runs on the CentOS operating system, a free Linux distribution for web server-based systems, and Eucalyptus, the open-source software platform that implements private cloud computing.

To prepare the platform, first install the minimum CentOS on all DigitalEdge servers. Minimally, this would involve two servers:

- One for the Eucalyptus Cloud Controller (including Walrus) and the Cluster Controller (including the Storage Controller)
- One for a Eucalyptus Node Controller

Optimally, the smallest system would involve 3 machines:

- One for the Cloud Controller (including Walrus)
- One for the Cluster Controller (including the Storage Controller)
- At least one Node Controller

Consult a DigitalEdge Deployment Engineer for sizing advice.

DigitalEdge uses CentOS 6.4+.

- Download the operating system from https://www.centos.org/
- CentOS release notes are at http://wiki.centos.org/Manuals/ReleaseNotes/CentOS6.4
- Complete installation instructions are at http://www.centos.org/docs/5/html/Installation_Guide-en-US/

The CentOS installation and configuration procedure requires under 1 hour of your time.

Install the minimum CentOS on every server that will be running Eucalyptus and DigitalEdge.

1. Install the base CentOS:
   a. Boot from an installation disk or an image on a local hard drive. The **Welcome to CentOS** screen appears. (Click **OK** to continue through the installation process.)
   b. Select **Install or upgrade an existing system**. Press the **Tab** key to stay in text mode. Progress information scrolls as the hardware is initialized.
   c. Make a **Language Selection**.
   d. Make a **Keyboard Selection**.
   e. Select the **Basic Storage Devices**.
   f. Make a **Time Zone Selection**.
   g. Enter a **Root Password** for the operating system. The installer will warn you if you use invalid characters or if the password is weak.

h. For a **Partitioning Type**, select **Use entire drive**. Select the specific drive to use for installation.

i. The **Formatting ...** message appears and progress information is reported during the **Package Installation** as the required software packages are installed.

j. The CentOS installer reports **Complete** when finished.

2. Next, configure the server that will be running the Eucalytpus front-end controllers (Cloud Controller, Cluster Controller, and Node Controller). On the server hosting the Eucalyptus Cloud Controller, edit the networking interface configuration file to assign an IP address and host name to the machine.

   a. At the Cloud Controller's **localhost login** prompt, logon as `root`.

   b. Enter your new root password.

   c. Edit the networking interface file `vi \etc\sysconfig\network-scripts\ifcfg-<interface_name>`. Uncomment and change the following lines to:

      ```
      ONBOOT=yes

      BOOTPROTO=static

      NM_CONTROLLED=no
      ```

   d. Add the following new lines, substituting the IP address of the Eucalyptus Cloud Controller for `<ip_address_number>`:

      ```
      IPADDR=<ip_address_number>

      NETMASK=<ip_address_number>
      ```

3. Configure the host name for the Cloud Controller server by editing the `sysconfig` network file: `vi \etc\sysconfig\network\sysconfig`

   a. Change the host name in the `sysconfig` network file to the desired Cloud Controller hostname:

      ```
      HOSTNAME=test-cloud1
      ```

   b. and add the line:

      ```
      GATEWAY=<ip_address_for_network_gateway>
      ```

4. Reboot to start CentOS and to pick up the new host name and interface changes.

5. Repeat steps 2-4 on physical machine hosting a Eucalyptus Controller, substituting that machine's IP address for `<ip_address_number>`, essentially telling the machine it's own IP address and netmask so that it will function successfully on the network.

6. Install and configure the Network Time Protocol. DigitalEdge uses GMT. Obtain the NTP server used by your network for configuration.

   a. Point to a nameserver in `/etc/resolve.conf`.

   b. Run the following commands:

      ```
      yum -y install ntp
      ```

```
vi /etc/ntp.conf
```

c. Edit the nameserver in the `ntp.conf` file to be the IP address of the NTP server. Choose a local server, and another one as a backup NTP server. Save the `ntp.conf` file.

d. Enable and configure NTP to run at reboot:

```
chkconfig ntpd on
```

e. Start the NTP service:

```
service ntpd start
```

```
ntpdate -u <ip_address or ntp_server_hostname>
```

f. Synchronize the server to use GMT:

```
ls /etc/localtime
```

g. Remove the current configuration/symbolic link:

```
rm -f /etc/localtime
```

h. Link localtime to GMT to set NTP:

```
cd /etc
```

```
ln -s /usr/share/zoneinfo/GMT /etc/localtime
```

CentOS will report:

```
success: lrwxrwxrwx.1 root toot <date_time> /etc/localtime
```

7. Eucalyptus must have the Security-Enhanced Linux (SELinux) module disabled.

a. Edit `/etc/sysconfig/selinux` to change the following line to:

```
SELINUX=disabled
```

b. Reboot to reread and disable the file.

c. You can check that SELinux was successfully disabled:

```
sestatus
```

8. If you have a hardening script, run it now.
9. Repartition the drive. You will need a minimum of 60 GB for Walrus, Eucalyptus' object-based storage system.
10. Repeat these steps on all DigitalEdge servers.

Chapter 6: Installing Eucalyptus

The DigitalEdge platform runs on the CentOS operating system and Eucalyptus, the open-source software platform that implements private cloud computing.

DigitalEdge uses Eucalyptus 3.2.2+.

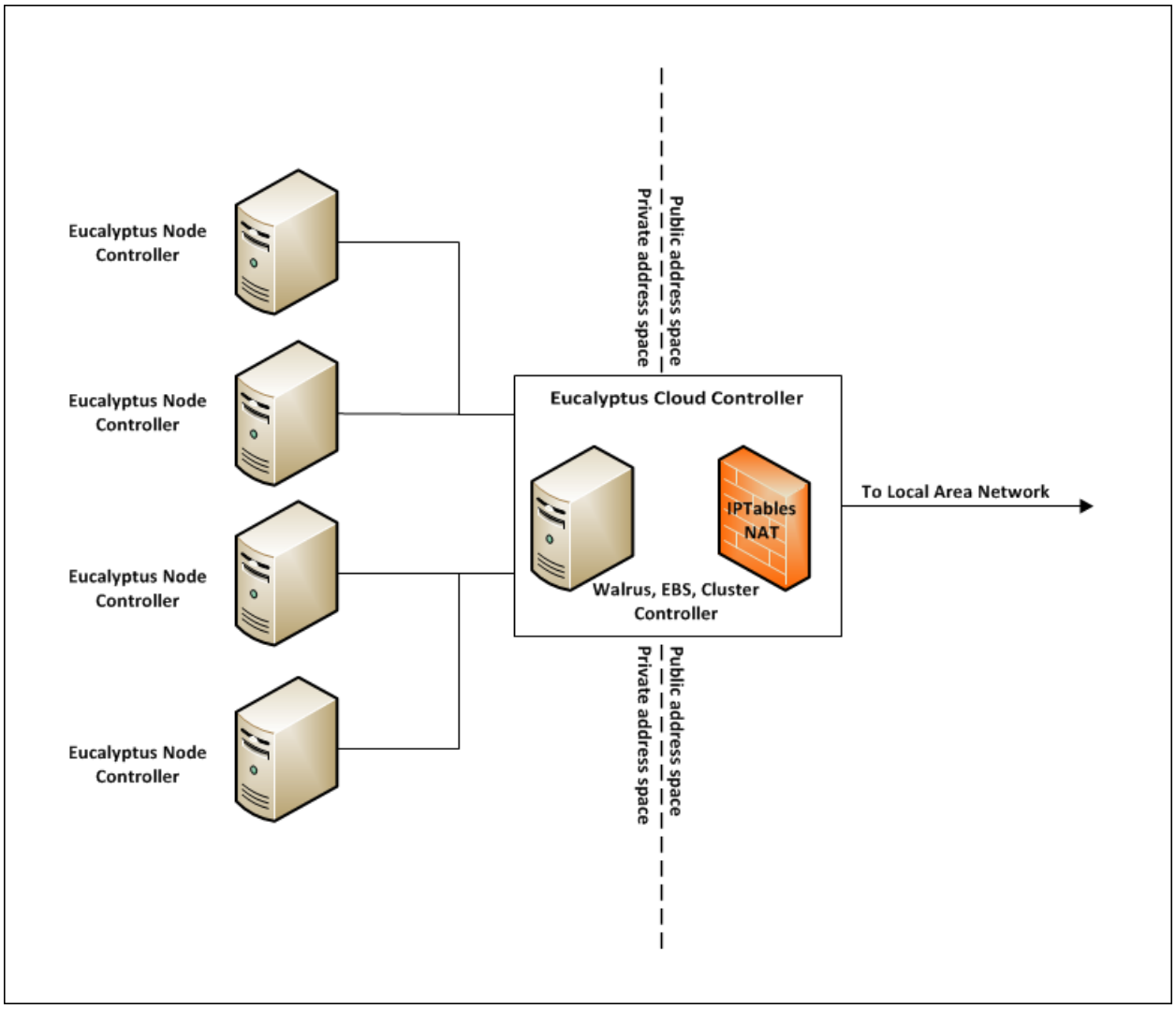
- Download Eucalyptus from http://www.eucalyptus.com/download/eucalyptus. The licensed version of Eucalyptus is preferred over the open source version because the licensed version includes technical support.
- Consult the CentOS instructions at http://www.eucalyptus.com/download/eucalyptus
- Get the complete *Eucalypus Installation Guide* from http://www.eucalyptus.com/eucalyptus-cloud/documentation. The *Eucalyptus Installation Guide* provides excellent guidance on disk space requirements, hardware planning, and component placement. It also explains each Eucalyptus installation step in more detail to supplement the following instructions.

The Eucalyptus installation and configuration procedures require approximately 2 hours.

You must install Eucalyptus on every CentOS host, including the following components (each of which is a web service):

- Cloud Controller: The cloud entry point for administrators and users, providing services such as:
    - Scheduling
    - Requests to the cluster controller
    - An interface to the management component, the Eucalyptus Administrator Console
    - Managing virtualized resources
    - Housing Walrus, which stores virtual machine images and user data
- Cluster Controller: Manages all IP addresses
    - Includes connectivity to both the Cloud Controller and the Node Controllers
    - Manages virtual machine networks
    - Runs the Eucalyptus EC2 services and Walrus S3 services
    - On the same machine as the Storage Controller
- Node Controller: Manages the virtual network endpoint
    - On each machine that hosts virtual machine instances
    - Controls VM activity

The basic Eucalyptus architecture is configured as:



The smallest DigitalEdge system would have the Cloud Controller and the Cluster Controller on one host, and the Node Controller on a second host. Optimally, each controller should be on its own host. Each component requires a slightly different installation and configuration. Larger systems will have multiple Node Controllers.

Installing Eucalyptus on the Cloud Controller

First, install Eucalyptus on the Cloud Controller. The Cloud Controller is the cloud entry point for all administrators and users. It routes all scheduling requests to the Cluster Controller, manages virtualized resources, hosts Walrus, and interfaces to the management console.

Steps 1-4 install Eucalyptus repositories, which must be on the physical machine that runs the Cloud Controller. Step 5 installs the components that make up the Eucalyptus Cloud Controller software package.

1. Install the Eucalyptus repository.

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
centos/6/x86_64/eucalyptus-release-3.2.noarch.rpm
```

2. Install the Euca2ools package repository.

```
yum install http://downloads.eucalyptus.com/software/euca2ools/2.1/
centos/6/x86_64/euca2ools-release-2/1.noarch.rpm
```

3. Install the EPEL repository.

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
centos/6/x86_64/epel-release-6.noarch.rpm
```

4. Install the ELRepo repository on the host running Walrus.

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
centos/6/x86_64/elrepo-release-6.noarch.rpm
```

5. Install the Cloud Controller software.

```
yum -y groupinstall eucalyptus-cloud-controller
```

   Note that this command will fail on the dependencies if you do not have Internet connectivity.

   This step requires approximately 5-10 minutes.

6. Install Walrus, Eucalyptus' object-based storage system. DigitalEdge stores all machine images and system configuration files in Walrus.

```
yum -y install eucalyptus-walrus
```

7. Initialize the database while Eucalyptus is not yet running.

   
   Note that this step must be executed from the Cloud Controller first, before starting Walrus, the Cluster Controller, and the Storage Controller if all those components are installed on the same machine.

```
euca_conf --initialize
```

   This command takes several minutes.

   a. When the initialization succeeds, start the cloud service:

```
service eucalyptus-cloud start
```

   b. Wait a minute to have all the services come up, then do a status check on the services:

```
euca-describe-services
```

   or, for more descriptive information:

```
euca-describe-services -e
```

8. Get the file that contains all the credentials for running the remaining commands from the root user. This file provides the administrative credentials needed to generate certificates and to run

the services.

```
mkdir.euca

cd .euca/

/usr/sbin/euca_conf --get-credentials admin.zip

unzip admin.zip

source eucarc
```

Registering the Cloud Controller

After you have installed Eucalyptus on the Cloud Controller, register and restart the services.

1. Starting and synching all services may take a few minutes. Confirm that all base services are enabled and functioning in the cloud service:

   ```
   euca-describe-services
   ```

   If you receive a warning that Walrus is not configured, ignore the warning and continue.

2. Register Walrus:

   ```
   /usr/sbin/euca_conf --register-walrus --partition walrus
   --host <ip_address> --component <component_name>
   ```

   where `partition walrus` MUST be named `walrus`, `host` can be any IP address (or hostname), and `<component_name>` is a name of your choosing.

   a. Provide your CentOS root password.

   b. After a minute, the Walrus `component_name` will appear as `ENABLED` in the services list.

3. Install dos2unix for the DigitalEdge installation program.

   ```
   yum install dos2unix
   ```

4. Reboot.

Installing Eucalyptus on the Cluster Controller

The Cluster Controller manages all public addresses for virtual instances (e.g., a DigitalEdge webapp). It must be set up with two interfaces to route traffic to all the instances, one on the public network, and one on the private network.

Steps 1-3 install Eucalyptus repositories, which must be on the physical machine that runs the Cluster Controller. Step 4 installs the components that make up the Eucalyptus Cluster Controller and Storage Controller software packages.

1. Configure the Eucalyptus repository.

   ```
   yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
   centos/6/x86_64/eucalyptus-release-3.2.noarch.rpm
   ```

2. Configure the Euca2ools package repository.

```
yum install http://downloads.eucalyptus.com/software/euca2ools/2.1/
centos/6/x86_64/euca2ools-release-2/1.noarch.rpm
```

3. Configure the EPEL repository.

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
centos/6/x86_64/epel-release-6.noarch.rpm
```

4. Install the Cluster Controller and the Storage Controller. These components are always installed on the same machine for a DigitalEdge deployment.

```
yum install -y eucalyptus-cc eucalyptus-sc
```

   This command takes several minutes to execute.

5. Install dos2unix for the DigitalEdge installation program.

```
yum install ldos2unix
```

6. Reboot.

Configuring the Cluster Controller

After you install Eucalyptus on the Cluster Controller, configure the controller with these procedures.

1. Edit the Eucalyptus configuration file that controls both the Cluster Controller and the Storage Controller.

```
vi /etc/eucalyptus/eucalyptus.conf
```

2. Uncomment and edit the following lines in the `eucalyptus.conf` file:
   a. The following parameter increases the number of loop devices to prevent running out of them. The more loop devices you have, the more robust the system is. A large number of loop devices allows the system to expand the Storage and Node Controller resources during high demand periods (elastic scaling).

```
CREATE_SC_LOOP_DEVICES=1024
```

   b. The following parameter increases the heap to improve performance:

```
CLOUD_OPTS="-Xmx6g"
```

3. Under the `NETWORKING CONFIGURATION` section in the `eucalyptus.conf` file:
   a. Edit the following parameter:

```
VNET_MODE='"MANAGED-NOVLAN"
```

   b. The following parameter creates the private interface, where `<private_name>` is the private network interface name associated with the private IP address on the same netwrok as the Node Controllers (for example, eth0).

```
VNET_PRIVINTERFACE="<private_name>"
```

c. The following parameter creates the public interface.

```
VNET_PUBINTERFACE="<public_name>"
```

d. Next, list your elastic IPs, depending on the network space that you have assigned. You can provide a public IP range, individual non-contiguous IP addresses separated by single spaces, or a combination of a range and individual IPs.

```
VNET_PUBLICIPS="<free-public-ip-1> <free-public-ip-2> …"
```

e. The following parameter assigns a private, non-routable IP address (`<ip_address>`) to the instances.

```
VNET_SUBNET="<ip_address>"
```

f. The following parameter identifies the network from which to pull the IP addresses (both the IP and a block of addresses), preferably Class B. You should also provide a Class B Netmask for the range of IP addressess than can be used by the virtual network supporting the instances.

```
VNET_NETMASK="<ip_address>"
```

g. This parameter determines how big your network blocks should be by setting the number of simultaneous instances each security group can use.

```
VNET_ADDRSPERNET="512"
```

h. Eucalyptus will insert an IP in all instances so that they can communicate with your network. Here, provide the IP address of the DNS server to use (external to the Cloud Controller and the Node Controllers). This DNS is required by Eucalyptus, but DigitalEdge does not use it.

```
VNET_DNS=""your-dns-server-ip"
```

3. Restart the Eucalyptus service on the Cluster Controller with its new networking configurations:

```
service eucalyptus-cc restart
```

4. Repeat these steps on each Cluster Controller in your system.

Registering the Cluster Controller

Complete the Eucalyptus installation on the Cluster Controller by registering and restarting its services.

1. Start the Eucalyptus services on the Cloud Controller.

```
service eucalyptus-cloud start
```

2. Register the Eucalyptus Cluster and Storage Controller services with the following commands:

```
/usr/sbin/euca_conf --register-cluster --partition <partition_name>
--host <ip_address> --components <cluster_controller_name>
```

where `<partition_name>` is a name of your choosing to identify the Cluster/Storage partition. For DigitalEdge, the Cluster and Storage partition will be the same.The `<ip_address>` should

be the IP address of the physical machine hosting the Cluster Controller, even though the command is run from the Cloud Controller.

```
/usr/sbin/euca_conf --register-sc --partition <partition_name>
--host <ip_address> --components <storage_controller_name>
```

where `<partition_name>` is identical to the previous command, `<storage_controller_name>` is a name of your choosing, and `<ip_address>` is the address for the Cluster Controller machine that you are connecting to.

Provide your CentOS root password.

3. Specify a storage backend:
   ```
   euca-modify-property -p <partition_name>.storage.blockstoragemanager
   =overlay
   ```
   a. **TIP:** If this command is not successful, restart the services on both the Cloud and Cluster Controllers:
      ```
      service iptables stop

      chkconfig iptables off

      service eucalyptus-cloud restart
      ```
   b. When all services are listed as ENABLED, rerun:
      ```
      euca-modify-property -p <partition_
      name>.storage.blockstoragemanager=overlay
      ```
4. Restart both the Eucalyptus Cloud and Cluster Controller services.
   ```
   service eucalyptus-cc restart

   service eucalyptus-cloud restart
   ```
5. Reboot.

Installing Eucalyptus on a Node Controller

Each Node Controller manages the virtual machine activity on a machine that hosts VM instances. You must install CentOS and Eucalyptus on each node.

Follow these instructions to set up a Node Controller. Consult the instructions in the *Installation Guide* at http://www.eucalyptus.com/eucalyptus-cloud/documentation while building the controller node for more detailed information.

Steps 1-3 install Eucalyptus repositories, which must be on the physical machine that runs the Node Controller. Steps 4-5 install the network interface and bridge utilities that must be on the Node Controller.

1. Configure the Eucalyptus repository.
   ```
   yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
   centos/6/x86_64/eucalyptus-release-3.2.noarch.rpm
   ```

2. Configure the Euca2ools package repository.

   ```
   yum install http://downloads.eucalyptus.com/software/euca2ools/2.1/
   centos/6/x86_64/euca2ools-release-2/1.noarch.rpm
   ```

3. Configure the EPEL repository.

   ```
   yum install http://downloads.eucalyptus.com/software/eucalyptus/3.2/
   centos/6/x86_64/epel-release-6.noarch.rpm
   ```

4. Install the network interface on a Node Controller.

   ```
   yum install -y eucalyptus-nc
   ```

5. Install the bridge utilities.

   ```
   yum install bridge-utils
   ```

6. Make sure that KVM (Kernel-based Virtual Machine) has the proper permissions, that is will run as user `root` and group `kvm`.

   ```
   ls -l /dev/kvm
   ```

   The output should look similar to:

   ```
   crw-rw-rw- 1 root kvm 10, 232 Nov 30 10:27 /dev/kvm
   ```

   If KVM does not have the correct permissions and the output lists `root root` instead of `root kvm`, be sure to reboot to assign the appropriate permissions.

7. Install dos2unix for the DigitalEdge installation program.

   ```
   yum install dos2unix
   ```

8. Reboot.

Configuring a Node Controller

After you install Eucalyptus on a Node Controller, follow these configuration steps.

1. Create a bridge interface from the Cloud Controller to the Node Controller. Choose an IP address to assign to the `br0` interface.
   a. Edit the empty bridge interface file:

      ```
      vi /etc/sysconfig/network-scripts/ifcfg-br0
      ```

   b. Include the following parameters:

      ```
      DEVICE="br0"

      TYPE="Bridge"

      BOOTPROTO="static"

      IPADDR="<ip_address>"
      ```

```
NETMASK="<ip_address>"

GATEWAY="<ip_address>"

ONBOOT="yes"
```

The private <ip_address> is found in the private network interface file.

2. Complete the bridge by mapping the physical interface file to br0 in the private network interface file.
   a. Edit the physical network interface file. For example:

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth1
   ```

   b. Add the following parameters:

   ```
   BRIDGE="br0"

   DEVICE="eth1"

   ONBOOT="yes"

   NM_CONTROLLED="no"
   ```

3. Set the number of cores and loop devices to use in the Node Controller.

   ```
   vi etc/eucalyptus/eucalyptus.conf
   ```

   a. Uncomment and edit the following parameters:

   ```
   MAX_CORES="36"
   ```

   Note: To use all cores, set this parameter to 0. A value of 36 is a starting point for this parameter; the actual number should be 1.5 times the number of CPU cores you have in your hardware setup.

   b. Each instance occupies a certain amount of disk space. The following parameters specify the maximum size available for an instance, recorded in megabytes. Set these parameters to the appropriate sizes for your system.

   ```
   NC_WORK_SIZE="300000"

   NC_CACHE_SIZE="150000
   ```

   c. The following parameter must match the number of loop devices you configured in `eucalyptus.conf` on the physical machine supporting the Storage Controller (for DigitalEdge, this is the same machine supporting the Cluster Controller).

   ```
   CREATE_NC_LOOP_DEVICES=1024
   ```

   d. Edit the following parameter:

   ```
   VNET_BRIDGE="br0"
   ```

4. Copy the Node Controller `eucalyptus.conf` file to all other Node Controllers.

Registering a Node Controller

Complete the Eucalyptus installation on a Node Controller by registering the node with the Cluster Controller.

1. Start the Node Controller.

   ```
   service eucalyptus-nc start
   ```

2. Reboot to register the nodes with the Cluster Controller.
3. Check the disk space partition:

   ```
   df -h
   ```

   Make sure that the partition's group and user groups are owned as `root kvm` and not `root root` by listing the directory.

Preparing for the DigitalEdge installation

1. Check the resources and services to confirm that everything is installed properly. From the Cloud Controller:

   ```
   euca-describe-availability-zones verbose
   ```

2. Log files are created and stored on each controller. Check the log files on the Cloud Controller to verify that installation is successful.

   ```
   varlogs/eucalyptus
   ```

3. Check the NTP synchronization from the Cloud Controller.

   ```
   ntpstat -q
   ```

4. Register each Node Controller from the Cluster Controller.

   ```
   /usr/sbin/euca-conf --register-nodes "<ip_address>"
   ```

   where <ip_address> is one or more Node Controller private IP addresses, separated by spaces.

   It will take a few minutes for the nodes to appear as available on the Cloud Controller.

5. Make sure that all the available disk space has been allocated to the partitions on the Node Controllers.
6. The DigitalEdge installer requires a user account (other than root) with sudo access and with the password prompt turned off. This procedure establishes two user group simultaneously: a Eucalyptus group and an admin group.

   Add the user to the `eucalyptus` group.

   Add group read permissions for:

   ```
   /var/lib/eucalyptus/keys/cloud-pk.pem
   ```

   ```
   /var/lib/eucalytpus/keys/
   ```

7. Log onto the Eucalyptus Console webapp from the Cloud Controller and configure several components for DigitalEdge.
   a. `https://<cloud controller ip>:8443`
   b. The **User** name and **Password** are both `admin`. At your first logon, Eucalyptus will ask you to change the password.
   c. In the **Eucalyptus Console**, under the **Service Components** section, make sure that the **walrus** component is set to:

      Maximum bucket size (MB) 51200

      Space reserved for unbundling images (MB) 51200
   d. Under the **Service Components** section, make sure the **storage controller** is configured as:

      Max volume size 100 (GB)

      Disk space reserved for volumes 500 (GB) or higher
   e. In the **VmTypes** section, make sure the Eucalyptus VM types match these DigitalEdge specifications:

VM Type	CPUs	Memory (MB)	Disk (GB)
m1.small	1	1700	10
c1.medium	1	3750	10
m1.large	2	7500	10
m1.xlarge	4	15000	10
c1.xlarge	4	15000	10

Chapter 7: Installing DigitalEdge on Eucalyptus

Once you have CentOS and Eucalyptus installed and the Node Controller built, you are ready to install the DigitalEdge software and set up your Tenant Management System (TMS).

Prerequisites

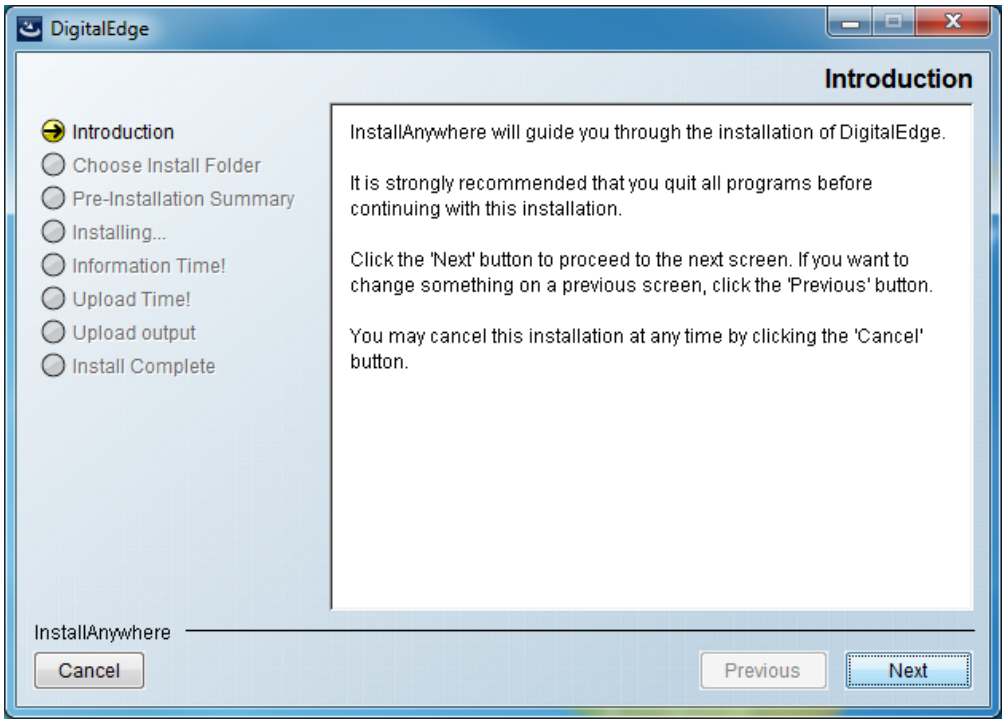
- The Systems Administrator has installed and configured CentOS and Eucalyptus
- You can log on to the Node Controller
- You can log on to the Eucalyptus Console webapp
- You have an installer from Leidos
- You have gathered parameter values for the installer from Eucalyptus and your Eucalyptus Administrator (specific parameters are requested in the Installer dialog)

With Eucalyptus up and running, you can now do a full installation of DigitalEdge. This involves setting up a Tenant Management System, creating at least one tenant account, installing the DigitalEdge software, and accessing the DigitalEdge Setup Tools. These processes are all accomplished using the **Full Install** option in the installation EXE. Installation requires at least 1 hour.

Follow these steps to do a **Full Install** of DigitalEdge:

1. Copy `<de_installer>.exe` to a local drive.
2. Run `<de_installer>.exe`. The installer expands and creates a log file. The log file is located in the same directory selected as the installation path. The log file is a text file that should be refreshed to view installation progress updates.

3. Choose **English** as the language and click **OK**. The **Introduction** screen lists the steps that the installer will accomplish:

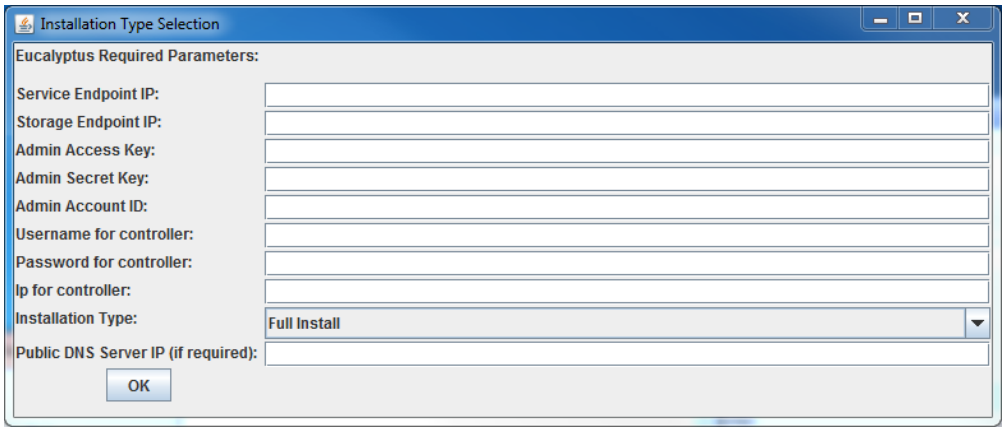


Click **Next** to proceed to each installation step.

4. On the **Choose Install Folder** screen, select a location for the DigitalEdge software.
5. The **Pre-Installation Summary** lists file locations.
6. The **Installing...** screen displays information as the installer moves files.
7. When prompted, **Have you downloaded an AMI already?**:
   - If you have an AMI, click **Yes** to continue with step 8.
   - If you do not have an AMI, and you are connected to the Internet, click **No**. The **DigitalEdge Amazon Machine Image (AMI) Application** download page appears. Click **Create**.

     Select the AMI **Name** of BaseImage and click Create. Select and refresh the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Continue with step 8.
   - If you do not have an AMI and you are not connected to the Internet, click **Yes** and pause in the installation process. Go to a PC that is connected to the Internet and access the **DigitalEdge Amazon Machine Image (AMI) Application** download page at https://default.tms-dev.deleidos.com/amife. Click **Create**. Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Copy the AMI over to your Eucalyptus client and continue with this installation.

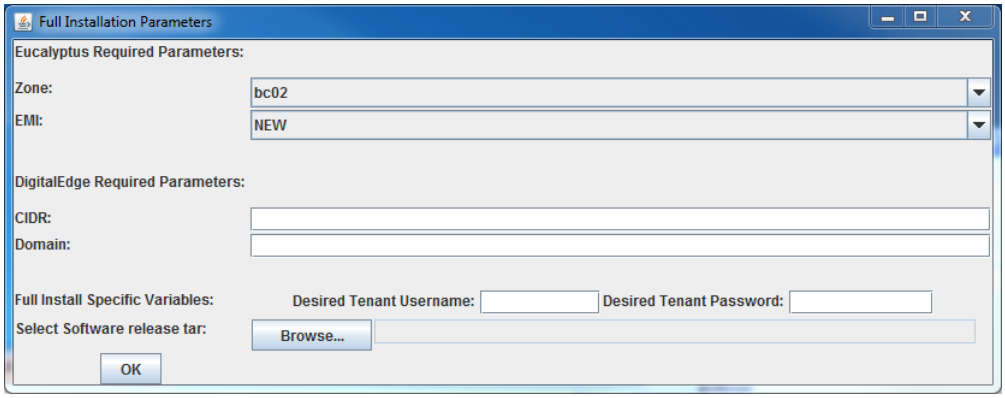
8. Next, verify the AMI that you have:
   a. **Browse** to the AMI location and select the AMI file.
   b. Click **Verify**. The installer will open the AMI file and validate it.
   c. Verification will take a few minutes. Click **OK** on this informative message.
   d. When verification is complete, click **OK**. If the AMI file failed verification, return to step 7 to get another AMI.
9. The **Information Time** screen requests input of **Eucalyptus Required Parameters** in the **Installation Type Selection** dialog box:



- **Service Endpoint IP**: The IP address where your services (such as the Eucalyptus Console) are running, typically the Eucalyptus Cloud Controller IP address.
- **Storage Endpoint IP**: The IP address where Walrus is located. The **Storage Endpoint** can be the same as the **Service Endpoint**.
- **Admin Access Key**: The access key for Eucalyptus; listed in the **Eucalyptus Console** > **Keys** > **Eucalyptus**
- **Admin Secret Key**: The secret key for Eucalyptus; listed in the **Eucalyptus Console** > **Keys** > **Eucalyptus**
- **Admin Account ID**: The Eucalyptus account ID, identified as a 12 digit IAAS service number in the Eucalyptus Console under > **Identity Management** > **Accounts** > **ID**
- **Username for controller**: Logon credentials for the Eucalyptus Node Controller. Ask your Eucalyptus Administrator for the username, which is the same username that was configured during the installation and configuration of the Eucalyptus Node Controller.
- **Password for controller**: Logon credentials for the Eucalyptus Node Controller. Ask your Eucalyptus Administrator for the password, which is the same password that was configured during the installation and configuration of the Eucalyptus Node Controller.
- **IP for controller**: The IP address for the Eucalyptus Node Controller; ask your Eucalyptus Administrator for the IP address
- **Installation Type**: Select **Full Install** for a first-time DigitalEdge installation.

- **Public DNS Server IP (if required)**: If you did not create a DNS forwarder, Eucalyptus will use this DNS server/public IP address to resolve node lookups and to access the Internet. Check with your Eucalyptus administrator for details.

10. Click **OK**. A second list of parameters appears in the **Full Installation Parameters** dialog box:



- **Zone**: Select the Service Zone for your cloud system
- **EMI**: For a first installation, there will be no EMI available; select **NEW**
- **CIDR**: The IPv4 submask address for your local network, representing the IP block that the console will be accessing for TMS and the DigitalEdge webapps, such as `192.168.0.0/16`
- **Domain**: A system domain name for DigitalEdge; the domain name must match your DNS forwarder name, and it must forward to the third IP address in the forwarder's configuration file.
- **Desired Tenant Username**: The tenant account name and the logon name of the primary tenant in your DigitalEdge tenant account
- **Desired Tenant Password**: The logon password of the primary tenant in your DigitalEdge tenant account
- **Select Software release tar**: Browse to locate the DigitalEdge software file provided by Leidos that you copied to the local drive

11. Click **OK** and **Next**. The **Upload Time** screen appears
12. Click **Next** to view progress as Eucalyptus uploads all the files you need for DigitalEdge and installs the software.

    A log file named installer.log is created in the selected **Install Folder** (step 4). Check this file as installation proceeds; installation can take 1 hour or more. For example, the log file will be similar to:

```
INFO - Attempting to connect to controller and ping for data.

INFO - Attempting to connect to controller and ping for data.

INFO - Attempting to find IP addresses:
```

```
INFO - Master IP Address: 192.168.30.179

INFO - Auth IP Address: 192.168.30.180

INFO - API IP Address: 192.168.30.184

INFO - Default IP Address: 192.168.30.185
```

13. The installer displays the **Upload Output**.
14. You can now log on to DigitalEdge.

Logging on to DigitalEdge

Use this procedure to log on to the DigitalEdge **Management Console** as a tenant. Substitute your newly chosen **Domain** name for <*domain-name*> and your specified **Desired Tenant Username** for <*tenant-name*> (from the **Full Installation Parameters**):

1. Navigate to `https://default.<domain-name>/tenantconsole/`. The `<domain-name>` is the name chosen for running DigitalEdge.
2. Log on as `<tenant-name>`.
3. Check the DigitalEdge Management Console to make sure that the DigitalEdge Gateway to the Tenant Management System is green. Consult the DigitalEdge *Operations Guide* for detailed information about using the Management Console.

Chapter 8: Using the Management Console as a TMS Administrator

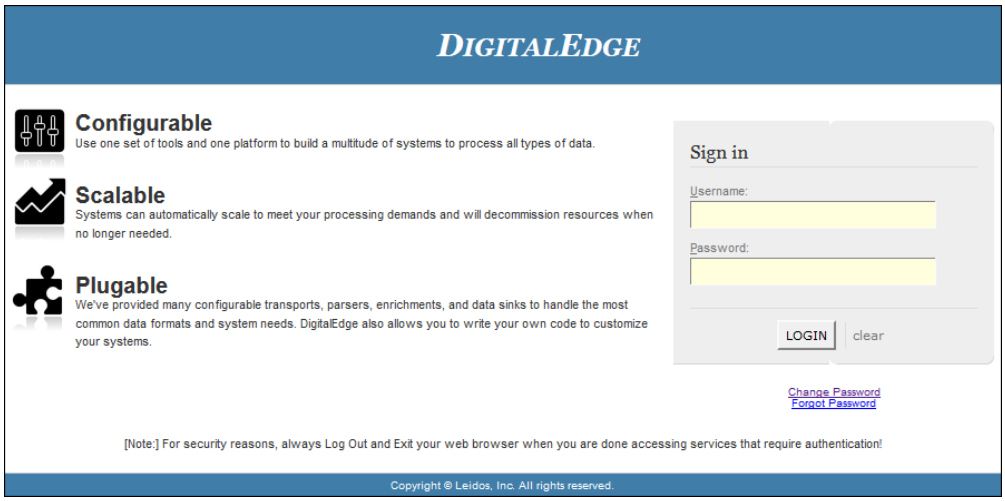
When running on a private Eucalyptus cloud system, there are several tasks that you can only accomplish when logged in to the Management Console as a TMS Administrator. These functions are used infrequently.

- **Create tenant accounts and primary tenants**: A tenant account can include primary and secondary tenants. A primary tenant is the first tenant created (during installation) in an account and owns all the resources (such as the system repository, LDAP, the tenant database, etc.). See "Creating Tenant Accounts" on page 41
- **Create secondary tenants**: A tenant account can also include secondary tenants. All secondary tenants share the account resources that are owned by their primary tenant, share and see all systems created under an account, and have access to the same DigitalEdge functionality as the primary tenant. But secondary tenants have different logon credentials for security purposes. See "Managing tenants" on page 34
- **Create user logins and credentials for TMS**: A tenant account can also have other users defined to access webapps. See "Creating user logins and credentials for TMS" on page 36
- **Allocate tenant account space on the Master Repository**: The TMS Master Repository stores both common and private plug-in components. For each tenant account, DigitalEdge designates space in the Master Repository for storing custom-created private components, and stores tenant IDs in the Master Repository. See "Allocating tenant space in the Master Repository" on page 36
- **Create a tenant gateway node**: The Gateway node starts and stops systems, creates and deletes systems and security groups, and synchronizes components. It also hosts CAS for single sign on permissions, LDAP for user account credentials, and the tenant database. See "Creating a tenant gateway node" on page 37
- **Create DNS entries**: You must create DNS entries before a tenant can create data models, configure DigitalEdge, and launch and access webapps. See "Creating DNS entries" on page 37
- **Create or remove security rules that apply to the TMS level**: A security group controls incoming communications to a server or process by implementing a set of firewall rules. DigitalEdge security groups are modeled on EC2™ security groups, which restrict communications based on protocol (TCP, UDP, etc.), IP address, and port. See "Creating security rules at the TMS level" on page 38
- **Synchronizing services with S3 or Walrus**: When you start up a DigitalEdge system, it automatically syncs the tenant's System Repository with the TMS Master Repository, sharing common components. You can also manually sync the repositories in the Management Console. See "Synchronizing the system" on page 39

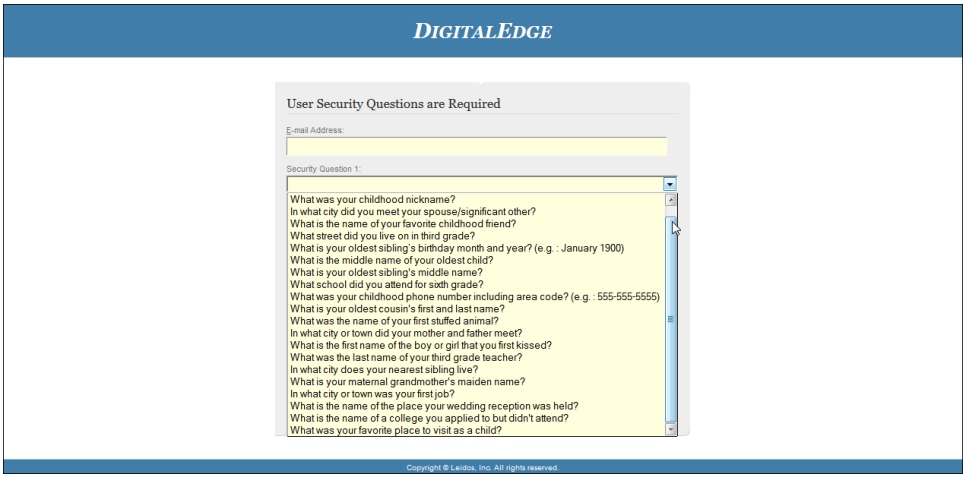
Logging in

Use this procedure to log on to the DigitalEdge **Management Console**.

1. In a web browser, go to `https://default.<system_domain_name>/tenantconsole`
2. Enter your **Username** and **Password**.
3. Click **LOGIN**.



4. The first time you log on to DigitalEdge, you must complete your registration:
   a. Supply your email address, and three security questions and answers to be used when confirming your identity:



   b. Click **Continue**.
   c. Read the DigitalEdge **License and Support Agreement** and click **ACCEPT**.
5. You can access all the DigitalEdge Setup and Runtime tools from the **Management Console**.

You cannot access the **Management Console** with an expired DigitalEdge license; contact Support for a new license.

Managing tenants

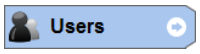
DigitalEdge includes a tenant account for each project /department using DigitalEdge on a private Eucalyptus cloud. Each tenant account runs its own secure applications and does not share data with other accounts.

A tenant account can include primary and secondary tenants. A primary tenant, created during installation, is the first tenant created in an account. The primary tenant owns all the resources (such as the system repository, LDAP, the tenant database, etc.).

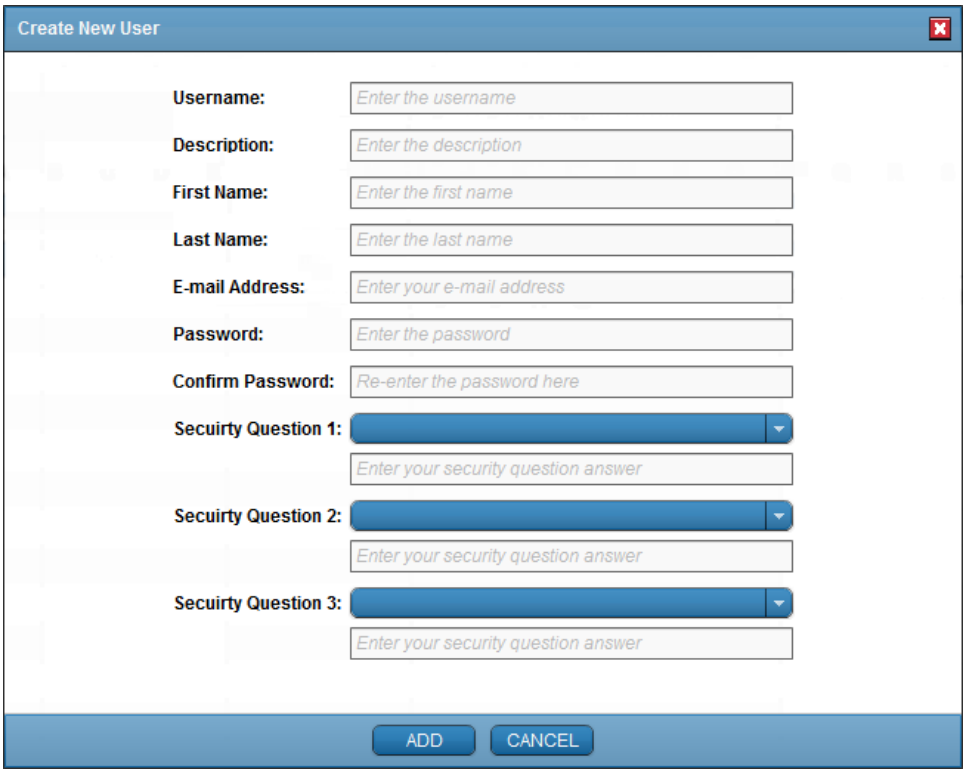
As a TMS Administrator, you can also create one or more secondary tenants in a tenant account. A secondary tenant is created in the **Management Console**. All secondary tenants share the account resources that are owned by their primary tenant, share and see all systems created under an account, and have access to the same DigitalEdge functionality as the primary tenant. But secondary tenants have different logon credentials for security purposes.

Add a secondary tenant

This procedure creates a secondary tenant in the DigitalEdge Management Console.

1. Open the **Management Console** as a TMS Administrator.
2. First, create a new user. This user will be tagged as a secondary tenant in the next step.
   a. Click the **Users** option. 

The Users workspace appears.
   b. Click **Add User**.  The **Create New User** dialog box appears.



c. Create and enter a **Username** (anything but "admin").

d. Enter a **Description** of this user.

e. Enter the user's **First Name**.

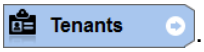
f. Enter the user's **Last Name**.

g. Enter a security **Password** (there are currently no rules for constructing passwords).

h. Re-enter the password for confirmation.

i. Click **ADD**.

3. Next, assign secondary tenant privileges to the new user.

a. Click the **Tenants** option 

. The Tenants workspace appears.

b. Click **Refresh**. 

c. Click **Add Account**.  The **Create New Account** dialog box appears.

d. Provide the following information:

- **Tenant Id**: Use the drop-down menu selection to choose the new user that you created in the previous step. This user will now be granted secondary tenant privileges.
- **Link Id**: Use the drop-down menu selector to choose the primary tenant. The new secondary tenant will share the resources (system repository, LDAP, dimension tables database, etc.) owned by this primary tenant.

e. Click **ADD**. The **Add Account** box confirms that you have successfully linked a secondary tenant to a primary tenant. Click **OK**.

Edit a tenant

1. From the **Tenant ID** list, highlight a tenant that you want to change and click **Edit**  . The **Update Account** dialog box appears.
2. You can edit any field that is not grayed out.
3. Click **UPDATE**.

Delete a tenant

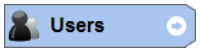
1. From the **Tenant ID** list, highlight a tenant that you want to remove and click **Delete**  .
2. In the **Confirmation** dialog box, click **Yes** to delete the tenant.

When you delete a secondary tenant, the user name that you created for that secondary tenant is *not* deleted. You must use the **Users/Delete** function to remove that user.

When you delete a primary tenant, all secondary tenants linked to that primary tenant are *also* unlinked and deleted.

Creating user logins and credentials for TMS

Follow these steps to create users who have access to TMS, not just a tenant account. *TMS users* are added to the TMS anchor node (LDAP); *tenant users* are added to the tenant gateway node (LDAP).

1. Open the **Management Console** as a TMS Administrator.
2. Click the **Users** option. 

The Users workspace appears.
3. Click **Add User**.  The **Create New User** dialog box appears.
4. Enter a **Username**, **Description**, **First Name**, **Last Name**, and **Password** (there are currently no rules for constructing passwords).
5. Click **ADD**.

Edit a user

When you need to edit users, you can scroll through the list if it is short. If you have a long list of users to maintain, you can jump to an alphabetical starting point in the list by clicking on a **First Letter**. Or, you can search for a user with the search box in the upper right corner and the **Filter** button.

1. From the user list, click **Edit**  to the right of the user you want to change. The **Update User** dialog box appears.
2. You can edit any field except the **Username**.
3. Click **UPDATE**.

Delete a user

1. From the user list, click **Delete**  to the right of the user you want to remove.
2. In the **Confirmation** dialog box, click **Yes** to delete the user.

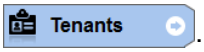
Allocating tenant space in the Master Repository

For each tenant account, DigitalEdge designates space in the TMS Master Repository for storing custom-created private components. The **Repository Space** option reserves enough repository space for this tenant account, you do not have to calculate space requirements.

Repository space is allocated when a new tenant account is created. In Amazon implementations, this occurs during the DigitalEdge Registration process. In Eucalyptus implementations, it occurs when you create a new tenant account.

As a TMS administrator, you can check that space has been allocated by accessing: **Management Console** > **Tenants** > **Account Detail** > **Account Support** > **Repository Space**.

If an error occurred when the tenant account was being created, you can allocate Repository space as follows:

1. Open the **Management Console** as a TMS Administrator.
2. Click the **Tenants** option  . The Tenants workspace appears.
3. On the **Tenant ID** list, highlight the account that you want to configure.
4. In the **Account Detail** panel, under **Account Support,** double-click the **Repository Space** option if it is listed as not set. A **Confirmation** message appears.
5. Click **Yes** to create space in the Master Repository to store this account's private plug-in components. The **Repository Space** status changes to set.

Creating a tenant gateway node

DigitalEdge creates a gateway node in each new tenant account. The gateway node starts and stops systems, creates and deletes systems and security groups, and synchronizes components. In Amazon implementations, this occurs during the DigitalEdge Registration process. In Eucalyptus implementations, it occurs when you create a new tenant account.

As a TMS administrator, you can check that a gateway node has been created by accessing: **Management Console** > **Tenants** > **Account Detail** > **Account Support** > **Gateway Instance**.

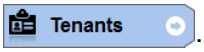
Creating DNS entries

You must create DNS entries to allow a tenant to create data models, configure DigitalEdge, and launch systems.

The **DNS Forwarder** option adds a forwarder entry to TMS which points to the tenant gateway node for the correct tenant domain name. The **DNS Zone** option creates DNS zones and entries for the master instance services, essentially building bridges to allow the internal and external IPs to communicate. Enabling either one of these DNS options activates both DNS options.

You must enable both DNS options for the new tenant account, otherwise users will not be able to access webapps such as Alert Controller and Search.

The Gateway must be up to activate these DNS options.

1. Open the **Management Console** as a TMS Administrator.
2. Click the **Tenants** option  . The Tenants workspace appears.
3. On the **Tenant ID** list, highlight the account that you want to configure.
4. In the **Account Detail** panel, under **Account Support,** double-click either the **DNS Forwarder** option or the **DNS Zone** option if it is listed as not set. A **Confirmation** message appears.
5. Click **Yes**. The status of both the **DNS Forwarder** and the **DNS Zone** changes to set.

Creating security rules at the TMS level

A security group controls incoming communications to a server or process by implementing a set of firewall rules. DigitalEdge security groups are modeled on Amazon EC2™ security groups, which restrict communications based on protocol (TCP, UDP, etc.), IP address, and port. A security group authorizes work with a process group, provides the ability to open a port for use, and specifies what outside networks can communicate with a process group.

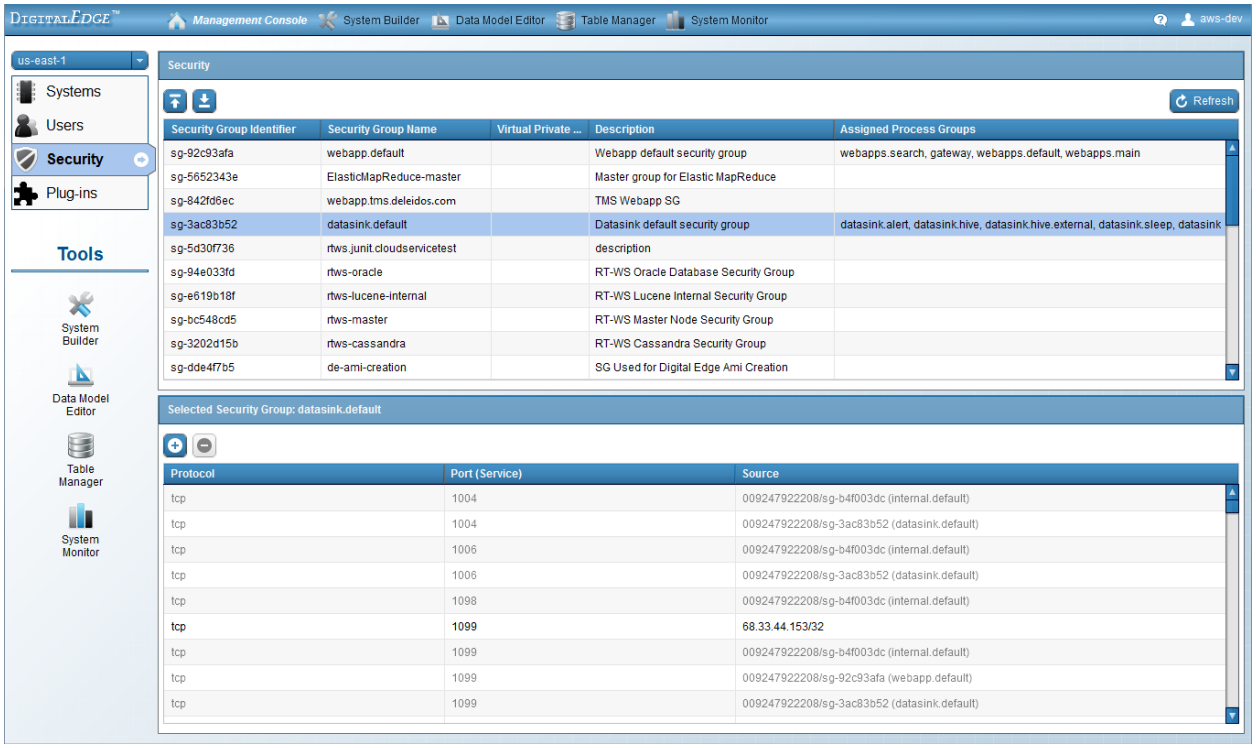
Security group parameters are specified in security rules. A security rule is a permission or a firewall ACCEPT rule. Each rule specifies a communications protocol, a port, and a source (either IP addresses or another security group that can talk to a process). Use the Management Console's **Security** section to work with security rules and to:

- Define a security rule for a security group
- Determine who can connect to a process
- Check an instance that is associated with a security group
- Open a port for a newly added instance/component (added in **System Builder**).

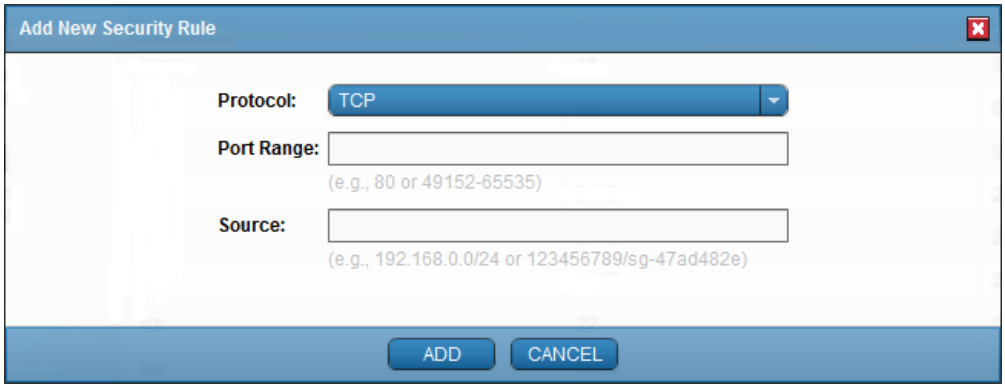
Add a security rule to a security group

1. Open the **Management Console**.
2. Click the **Security** option. 

3. From the **Security** list, click the row of a security group you want to work with. The list of security rules appears in the bottom panel.



4. Click the **Add** button. The **Add New Security Rule** dialog box appears.



5. Select a **Protocol** from the drop-down menu (TCP, UDP, or ICMP).
6. Enter a **Port Range** (one port number or a range of ports).
7. Enter a communications **Source**. A source can be an IP address, a range of IP addresses, or another security group that can talk with the assigned process groups.
8. Click **ADD**.

You cannot edit a security rule. To change a rule, **Delete** it and **Add** it again with revised parameters.

Rules which specify standard ports cannot be deleted. These rules are grayed out in the Security Rule List.

Synchronizing the system

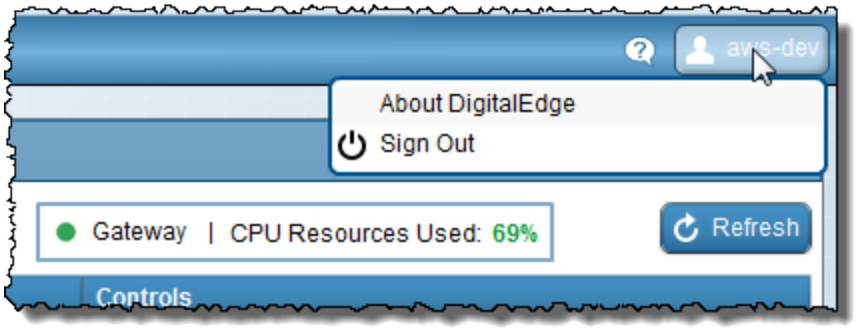
The Master Repository on TMS stores all common plug-in components and scripts as well as the private components and scripts for each tenant account.

You may want to upgrade a DigitalEdge system periodically. To sync your system to the latest DigitalEdge repository components, use the Management Console **Update System** icon on the **Systems** screen. The **Update System** function works in the background of a running system. It downloads the components and scripts from the Master Repository, restarts the ingest node processes, and updates your System Repository. There is no need to stop or restart a system when syncing with the latest components. A progress bar indicates the length and status of the update operation.

Logging out

Use this procedure to log out of DigitalEdge.

1. Go to the **Management Console**.
2. Click the user icon in the upper right corner and select **Sign Out**.



Use the same procedure to log out of any Setup or Runtime UI tool.

When you **Sign Out** of one tool, all open tools are automatically signed out.

Chapter 9: Creating Tenant Accounts

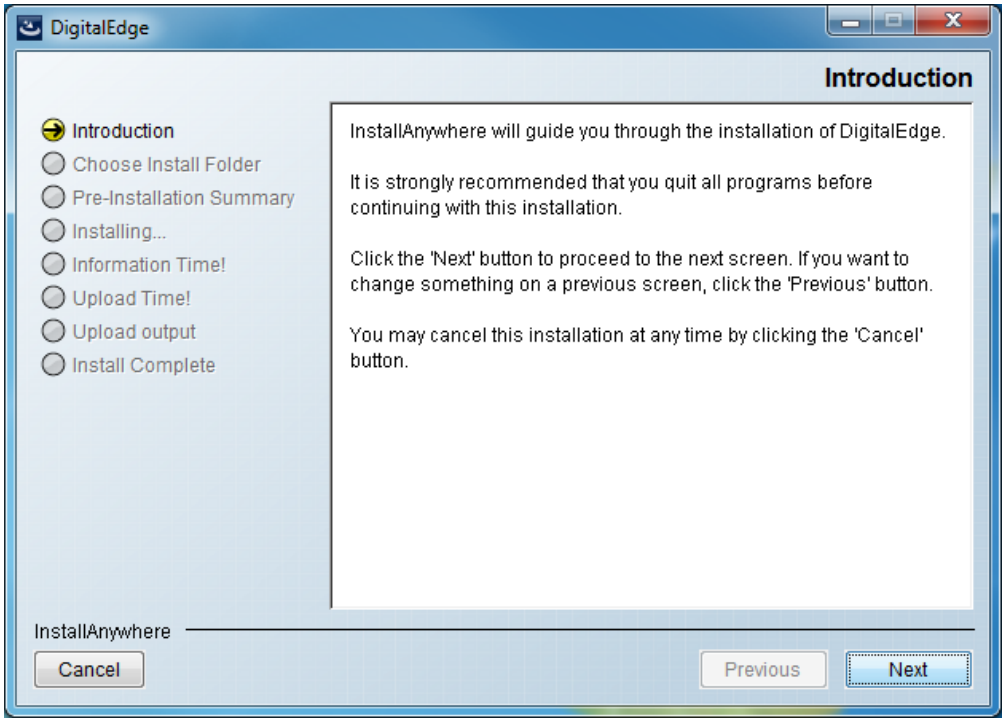
As TMS Administrator, you must create and set up a tenant account for each project /department using DigitalEdge on Eucalyptus. Each account runs its own secure applications and does not share data with other accounts. This procedure creates a tenant account in Eucalyptus, creates the account in DigitalEdge (for access to the DigitalEdge Management Console), defines the primary tenant, and launches the account. You will use the DigitalEdge Installation program to create accounts and the first primary tenant in each account.

Prerequisites

- DigitalEdge is installed (in a **Full Install**)
- The first tenant account has been created (in a **Full Install**)
- TMS is up
- You have an installer from Leidos

Follow these steps to install a tenant account:

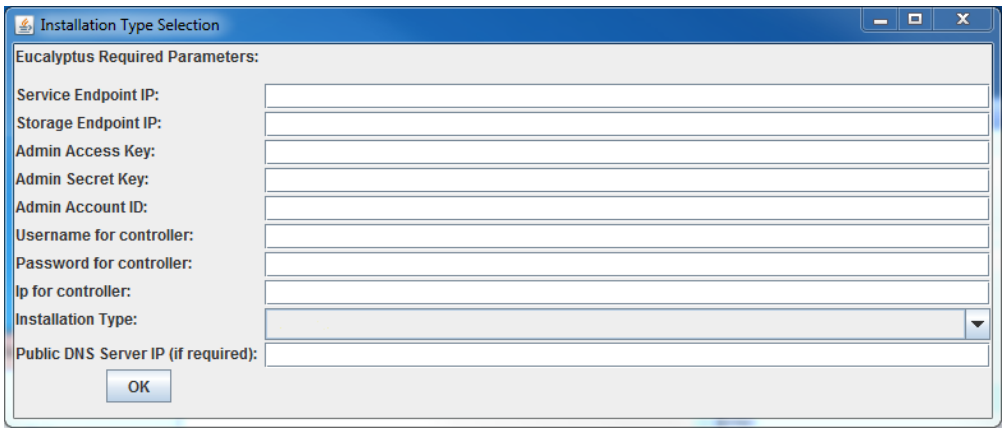
1. Copy `<de_installer>.exe` to a local drive.
2. Run `<de_installer>.exe`.
3. Choose **English** as the language and click **OK**. The **Introduction** screen lists the steps that the installer will accomplish:



Click **Next** to proceed to each installation step.

4. On the **Choose Install Folder** screen, select a location for the DigitalEdge software.
5. The **Pre-Installation Summary** lists file locations.
6. The **Installing...** screen displays information as the installer moves files.
7. When prompted, **Have you downloaded an AMI already?**:
   - If you have an AMI, click **Yes** to continue with step 8.
   - If you do not have an AMI, and you are connected to the Internet, click **No**. The **DigitalEdge Amazon Machine Image (AMI) Application** download page appears. Click **Create**.

     Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Continue with step 8.
   - If you do not have an AMI and you are not connected to the Internet, click **Yes** and pause in the installation process. Go to a PC that is connected to the Internet and access the **DigitalEdge Amazon Machine Image (AMI) Application** download page at https://default.tms-dev.deleidos.com/amife. Click **Create**. Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Copy the AMI over to your Eucalyptus client and continue with this installation.
8. Next, verify the AMI that you have:
   a. **Browse** to the AMI location and select the AMI file.
   b. Click **Verify**. The installer will open the AMI file and validate it.
   c. Verification will take a few minutes. Click **OK** on this informative message.
   d. When verification is complete, click **OK**. If the AMI file failed verification, return to step 7 to get another AMI.
9. The **Information Time** screen requests input of **Eucalyptus Required Parameters** in the **Installation Type Selection** dialog box:

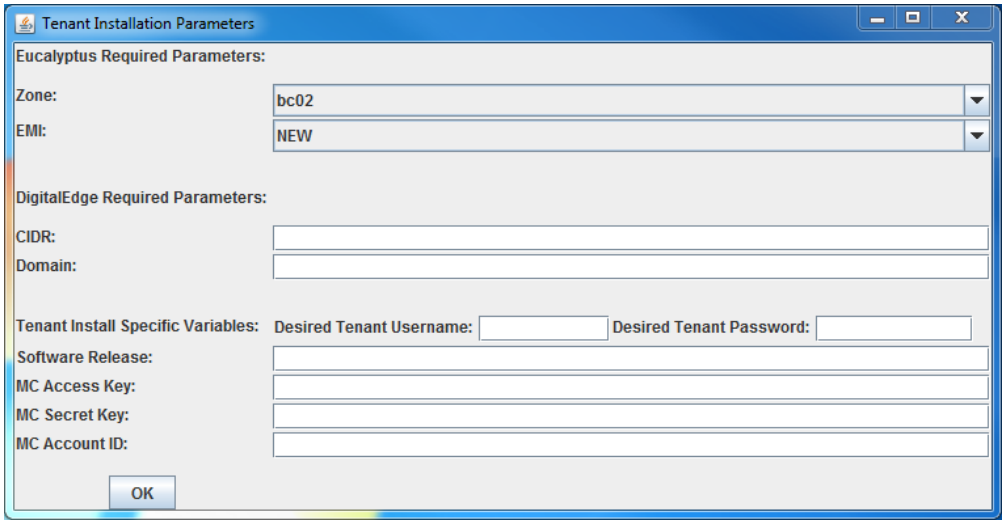


All of the following parameters should match the values that you entered when you did a **Full Install**:

- **Service Endpoint IP**
- **Storage Endpoint IP**
- **Admin Access Key**
- **Admin Secret Key**
- **Admin Account ID**
- **Username for controller**
- **Password for controller**
- **IP for controller**
- **Public DNS Server IP (if required)**

For an **Installation Type**, select **Tenant Install**.

10. Click **OK**. A second list of parameters appears in the **Tenant Installation Parameters** dialog box:



The following parameters should match the values that you entered when you did a **Full Install**:

- **Zone**
- **EMI**
- **CIDR**
- **Domain**

Create a new tenant account with the following parameters:

- **Desired Tenant Username**: The tenant account name and the logon name of the primary tenant in your DigitalEdge tenant account


A tenant name cannot include any capital letters.

- **Desired Tenant Password**: The logon password of the new tenant account
- **Software Release**: The DigitalEdge software version number, found as the name of the `.tar.gz` file provided by Leidos
- **MC Access Key**: In the Eucalyptus console, **Keys** tab, copy the **ID (Access Key)** property. The keys will be listed under the **tms** account (the only other account besides **eucalyptus** and any tenants you have created).
- **MC Secret Key**: In the Eucalyptus console, **Keys** tab, copy the **Secret Key** property. The keys will be listed under the **tms** account (the only other account besides **eucalyptus** and any tenants you have created).
- **MC Account ID**: In the Eucalyptus console, identified as a 12 digit IAAS service number under **Identity Management** > **Accounts** > **ID**
- **MC KeyPair**: This key pair is used to launch instances in the tenant account. You may have just one key pair in the drop-down menu to select. If the menu includes multiple key pairs, select the most recent one.

11. Click **OK** and **Next**. The **Upload Time** screen appears
12. As DigitalEdge changes ACLs for the new tenant account, it checks for previous values and overwrites older values.
13. Click **Next** to view progress as Eucalyptus uploads all the files you need. A log file named installer.log is created in the selected **Install Folder** (step 4).
14. The installer displays the **Upload Output**.

Chapter 10: Creating a New EMI

As a TMS Administrator, you can create and install a new EMI when needed. This procedure uses the DigitalEdge Installation program and creates a revised EMI to use with the latest release of DigitalEdge.

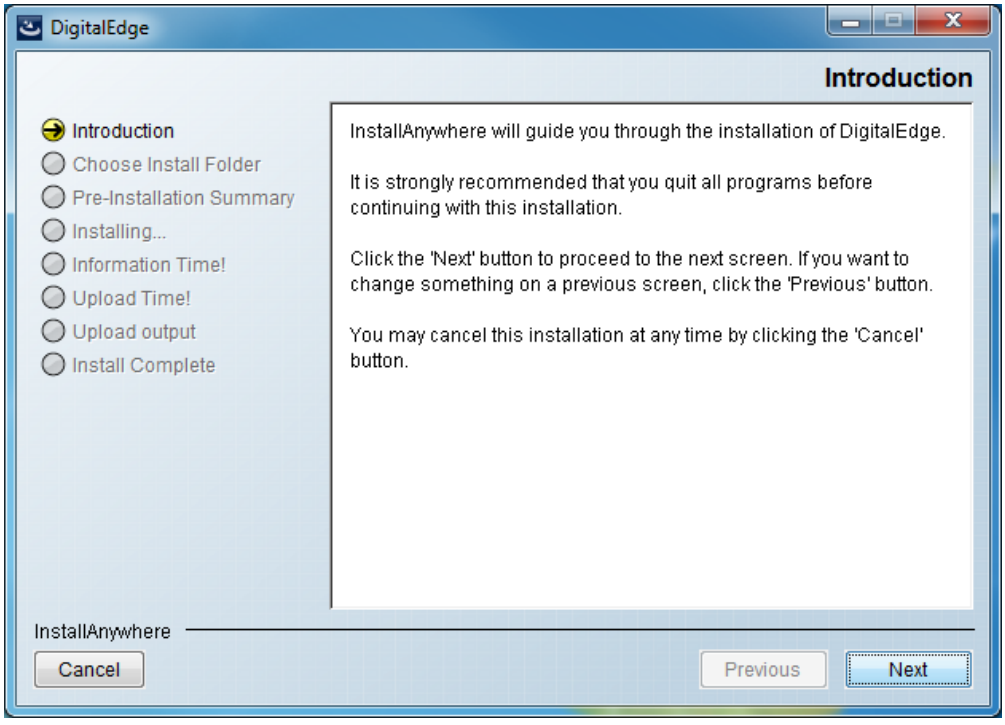
If Leidos requires a new EMI for your installation, the following process must be implemented *before* you do a **Software Upgrade** installation type.

Prerequisites

- DigitalEdge is installed (in a **Full Install**)
- You have an installer and a link to an AMI file. The AMI will be converted to an EMI in this process.
- TMS can be running or down

Follow these steps to install a new EMI:

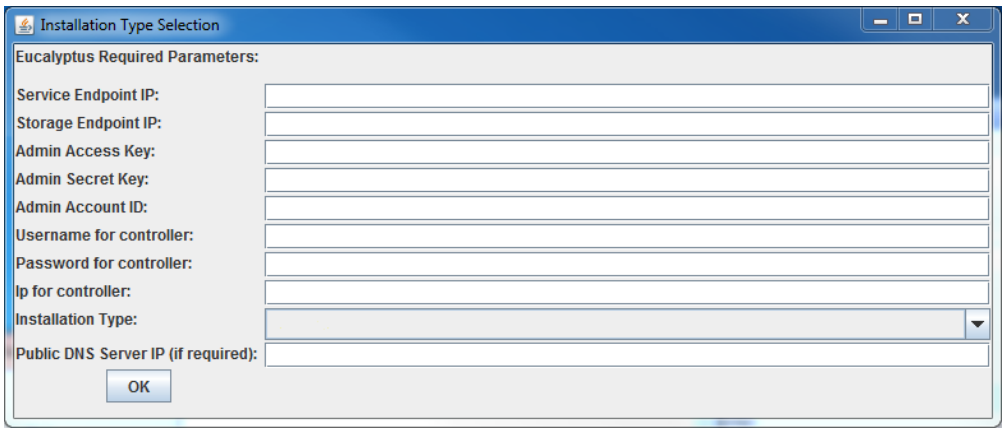
1. Copy `<de_installer>.exe` to a local drive.
2. Run `<de_installer>.exe`.
3. Choose **English** as the language and click **OK**. The **Introduction** screen lists the steps that the installer will accomplish:



Click **Next** to proceed to each installation step.

4. On the **Choose Install Folder** screen, select a location for the DigitalEdge software.
5. The **Pre-Installation Summary** lists file locations.
6. The **Installing...** screen displays information as the installer moves files.
7. When prompted, **Have you downloaded an AMI already?**:
   - If you have an AMI, click **Yes** to continue with step 8.
   - If you do not have an AMI, and you are connected to the Internet, click **No**. The **DigitalEdge Amazon Machine Image (AMI) Application** download page appears. Click **Create**.

     Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Continue with step 8.
   - If you do not have an AMI and you are not connected to the Internet, click **Yes** and pause in the installation process. Go to a PC that is connected to the Internet and access the **DigitalEdge Amazon Machine Image (AMI) Application** download page at https://default.tms-dev.deleidos.com/amife. Click **Create**. Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Copy the AMI over to your Eucalyptus client and continue with this installation.
8. Next, verify the AMI that you have:
   a. **Browse** to the AMI location and select the AMI file.
   b. Click **Verify**. The installer will open the AMI file and validate it.
   c. Verification will take a few minutes. Click **OK** on this informative message.
   d. When verification is complete, click **OK**. If the AMI file failed verification, return to step 7 to get another AMI.
9. The **Information Time** screen requests input of **Eucalyptus Required Parameters** in the **Installation Type Selection** dialog box:

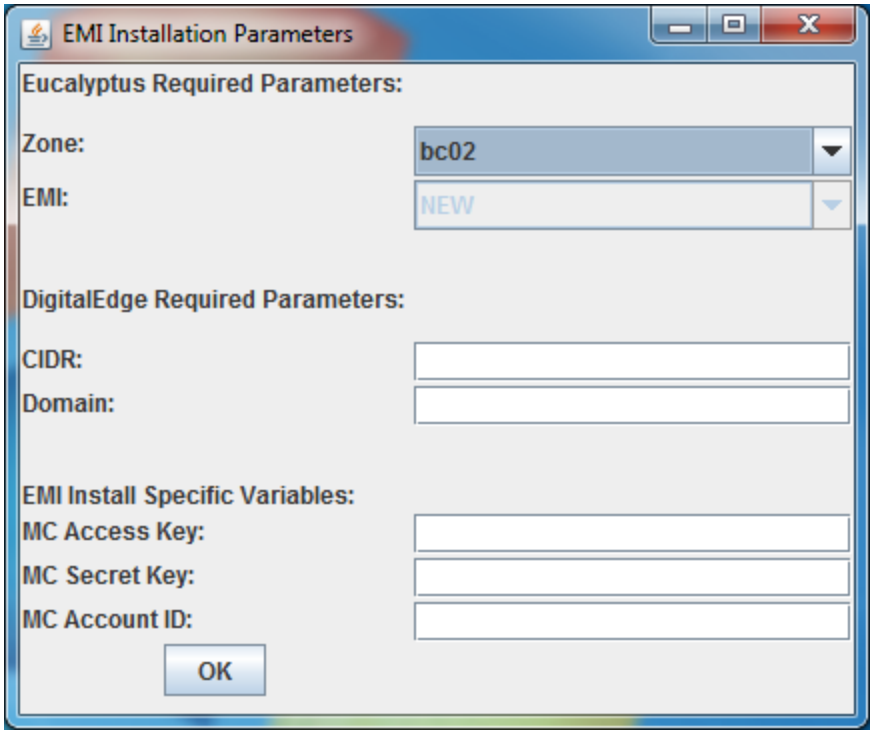


All of the following parameters should match the values that you entered when you did a **Full Install**:

- **Service Endpoint IP**
- **Storage Endpoint IP**
- **Admin Access Key**
- **Admin Secret Key**
- **Admin Account ID**
- **Username for controller**
- **Password for controller**
- **IP for controller**
- **Public DNS Server IP (if required)**

For an **Installation Type**, select **EMI Iinstall**.

10. Click **OK**. A second list of parameters appears in the **EMI Installation Parameters** dialog box:



The following parameters should match the values that you entered when you did a **Full Install**:

- **Zone**
- **EMI**
- **CIDR**
- **Domain**

Create a new EMI with the following parameters:

- **MC Access Key**: In the Eucalyptus console, **Keys** tab, copy the TMS access key (created during a full installation)
- **MC Secret Key**: In the Eucalyptus console, **Keys** tab, copy theTMS secret key (created during a full installation)
- **MC Account ID**: In the Eucalyptus console, copy the 12 digit IAAS service number under **Identity Management** > **Accounts** > **ID**

11. Click **OK** and **Next**. The **Upload Time** screen appears
12. Click **Next** to view progress as Eucalyptus uploads all the files you need for DigitalEdge and installs the software. A log file named installer.log is created in the selected **Install Folder** (step 4).
13. The installer displays the **Upload Output**.
14. You can now do a **Software Upgrade** installation with the new EMI.

Chapter 11: Installing a Software Upgrade

As a TMS Administrator, you can install a new version of DigitalEdge when needed. This process can be used to install a major release, minor release, or patches.

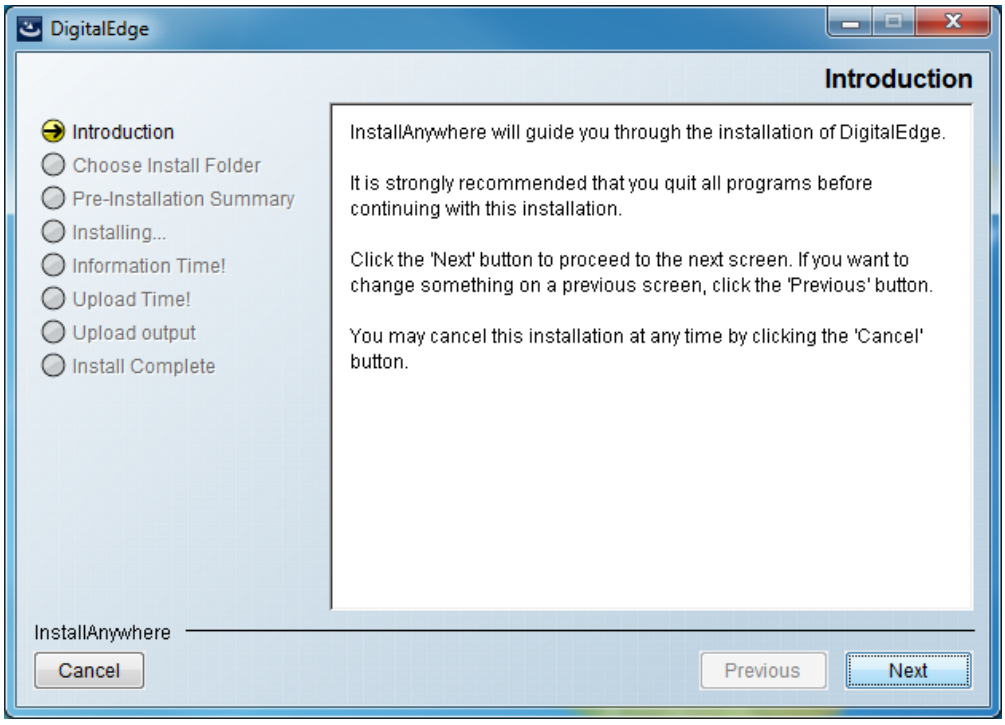
You may need to do an **EMI Install** (to create the latest EMI) before you do a **Software Upgrade** installation type. When in doubt, contact Leidos.

Prerequisites

- DigitalEdge is installed (in a **Full Install**)
- You have done an EMI Install
- You have an installer received from Leidos
- TMS can be running or down

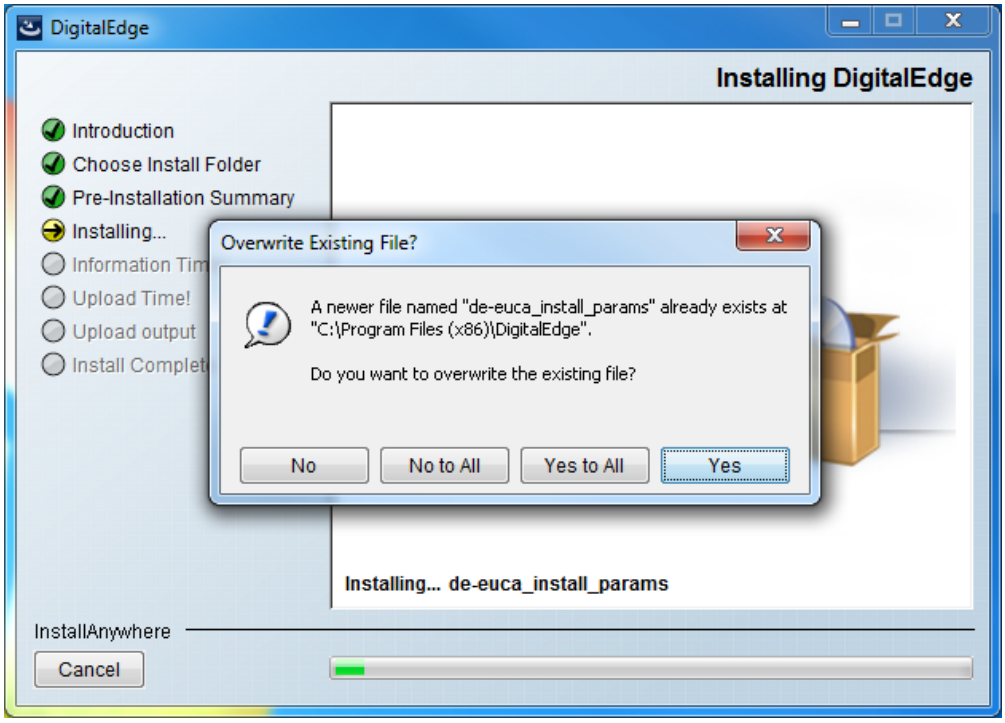
Follow these steps to install a DigitalEdge upgrade:

1. Copy `<de_installer>.exe` to a local drive (if you haven't already done so in a previous step).
2. Run `<de_installer>.exe`.
3. Choose **English** as the language and click **OK**. The **Introduction** screen lists the steps that the installer will accomplish:



Click **Next** to proceed to each installation step.

4. On the **Choose Install Folder** screen, select a location for the DigitalEdge software.
5. The **Pre-Installation Summary** lists file locations.
6. The **Installing...** screen displays information, and a request to overwrite files if a previous version is found:

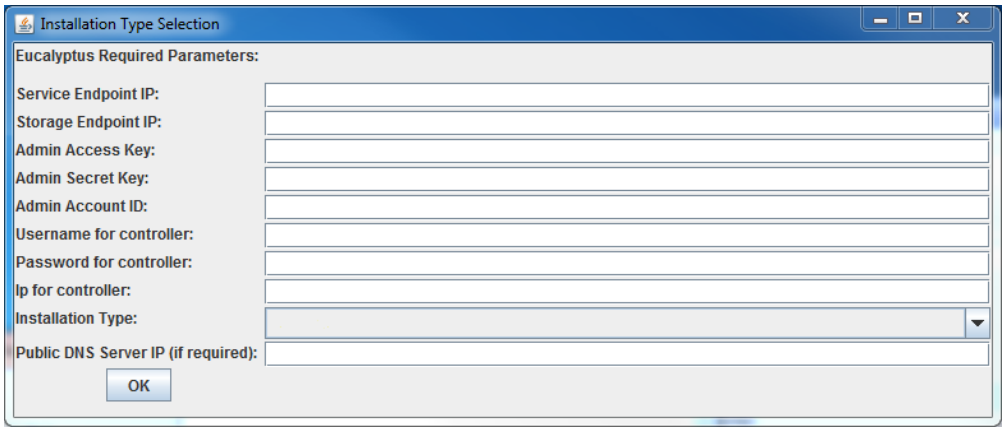


   You should overwrite the file when doing a software upgrade.

7. When prompted, **Have you downloaded an AMI already?**:
   - If you have an AMI, click **Yes** to continue with step 8.
   - If you do not have an AMI, and you are connected to the Internet, click **No**. The **DigitalEdge Amazon Machine Image (AMI) Application** download page appears. Click **Create**.

     Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Continue with step 8.
   - If you do not have an AMI and you are not connected to the Internet, click **Yes** and pause in the installation process. Go to a PC that is connected to the Internet and access the **DigitalEdge Amazon Machine Image (AMI) Application** download page at https://default.tms-dev.deleidos.com/amife. Click **Create**. Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Copy the AMI over to your Eucalyptus client and continue with this installation.

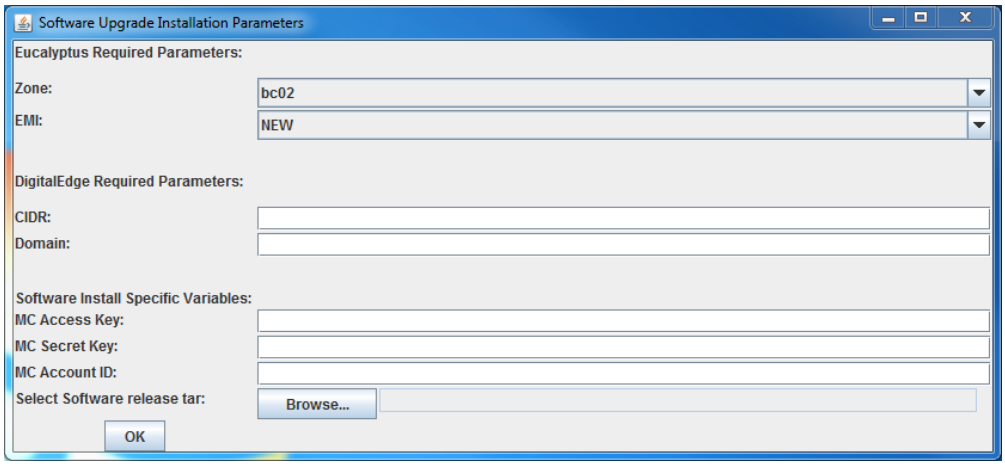
8. Next, verify the AMI that you have:
   a. **Browse** to the AMI location and select the AMI file.
   b. Click **Verify**. The installer will open the AMI file and validate it.
   c. Verification will take a few minutes. Click **OK** on this informative message.
   d. When verification is complete, click **OK**. If the AMI file failed verification, return to step 7 to get another AMI.
9. The **Information Time** screen requests input of **Eucalyptus Required Parameters** in the **Installation Type Selection** dialog box:



   All of the following parameters should match the values that you entered when you did a **Full Install**:

   - **Service Endpoint IP**
   - **Storage Endpoint IP**
   - **Admin Access Key**
   - **Admin Secret Key**
   - **Admin Account ID**
   - **Username for controller**
   - **Password for controller**
   - **IP for controller**
   - **Public DNS Server IP (if required)**

   For an **Installation Type**, select **Software Upgrade**.
10. Click **OK**. A second list of parameters appears in the **Full Installation Parameters** dialog box:



The following parameters should match the values that you entered when you did a **Full Install**:

- **Zone**
- **EMI**
- **CIDR**
- **Domain**

Install the latest release with the following parameters:

- **MC Access Key**: In the Eucalyptus console, **Keys** tab, copy the TMS access key
- **MC Secret Key**: In the Eucalyptus console, **Keys** tab, copy the TMS secret key
- **MC Account ID**: In the Eucalyptus console, copy the 12 digit IAAS service number under **Identity Management** > **Accounts** > **ID**
- **Select Software Release tar**: Browse to locate the DigitalEdge software file provided by Leidos that you copied to the local drive

11. Click **OK** and **Next**. The **Upload Time** screen appears.
12. Click **Next** to view progress as Eucalyptus uploads all the files you need for DigitalEdge and installs the software. A log file named installer.log is created in the selected **Install Folder** (step 4).
13. The installer displays the **Upload Output**.
14. Rerun the installer and select **Gateway Restart** to complete the upgrade.

Chapter 12: Restarting the Gateway

As the final step in a software upgrade installation, you must rerun the installer to have DigitalEdge shut down the previous gateway and launch the new gateway with the latest code release.

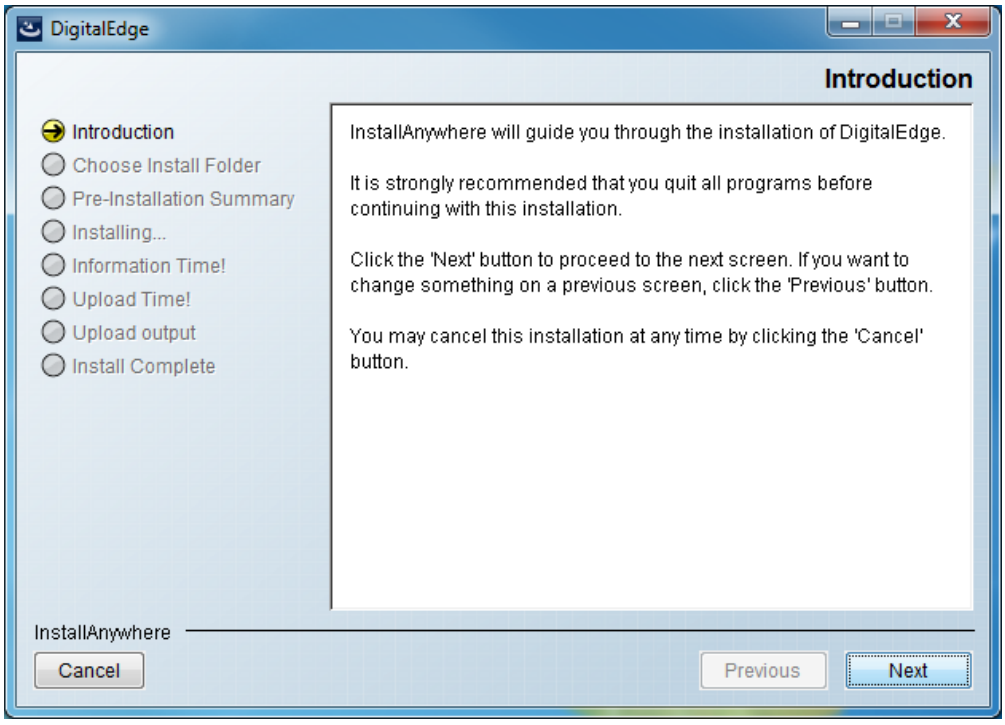
A software upgrade installation will not work until you complete a gateway restart.

Prerequisites

- DigitalEdge is installed (in a **Software Upgrade**)
- TMS *must* be running

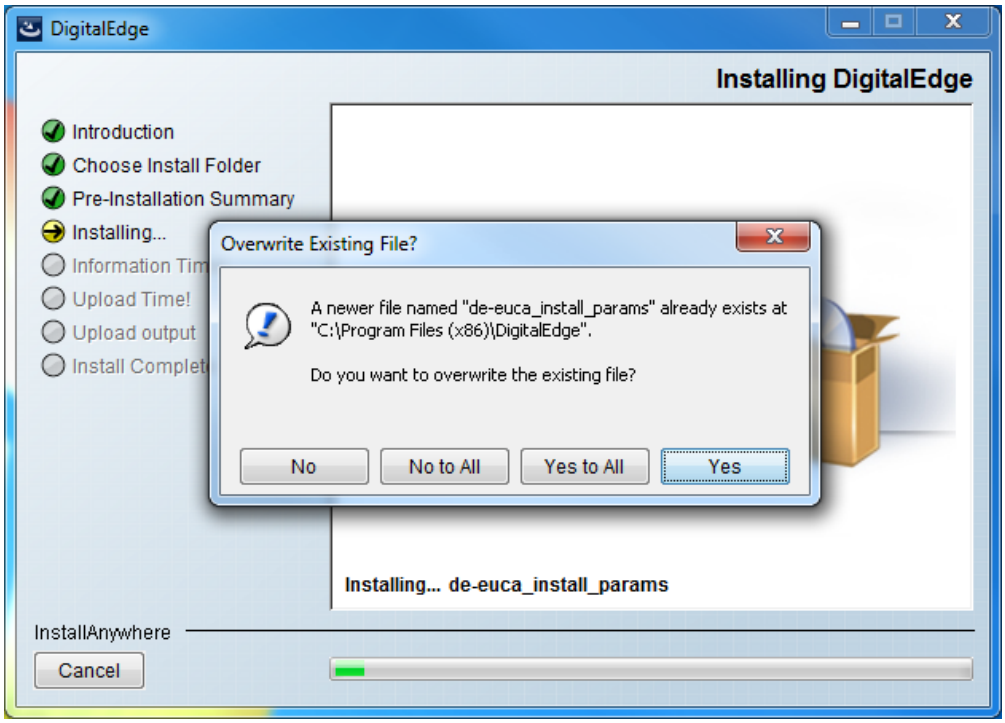
Follow these steps to complete the installation of a DigitalEdge upgrade and to restart the gateway:

1. Run `<de_installer>.exe`.
2. Choose **English** as the language and click **OK**. The **Introduction** screen lists the steps that the installer will accomplish:



Click **Next** to proceed to each installation step.

3. On the **Choose Install Folder** screen, select the location for the DigitalEdge software upgrade.
4. The **Pre-Installation Summary** lists file locations.
5. The **Installing...** screen displays information, and a request to overwrite files if a previous version is found:

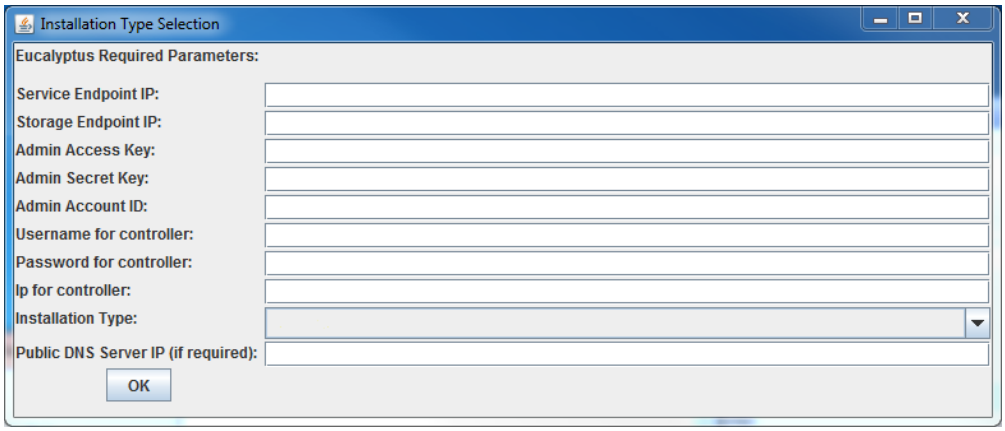


Do *not* overwrite the file when doing a gateway restart.

6. When prompted, **Have you downloaded an AMI already?**:
   - If you have an AMI, click **Yes** to continue with step 8.
   - If you do not have an AMI, and you are connected to the Internet, click **No**. The **DigitalEdge Amazon Machine Image (AMI) Application** download page appears. Click **Create**.

     Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Continue with step 8.
   - If you do not have an AMI and you are not connected to the Internet, click **Yes** and pause in the installation process. Go to a PC that is connected to the Internet and access the **DigitalEdge Amazon Machine Image (AMI) Application** download page at https://default.tms-dev.deleidos.com/amife. Click **Create**. Select the AMI **Name** of BaseImage and click Create. Select the **Status** page to check on the build progress. Click **Download** when the AMI is ready. Copy the AMI over to your Eucalyptus client and continue with this installation.
7. Next, verify the AMI that you have:
   a. **Browse** to the AMI location and select the AMI file.
   b. Click **Verify**. The installer will open the AMI file and validate it.
   c. Verification will take a few minutes. Click **OK** on this informative message.
   d. When verification is complete, click **OK**. If the AMI file failed verification, return to step 7 to get another AMI.

8. The **Information Time** screen requests input of **Eucalyptus Required Parameters** in the **Installation Type Selection** dialog box:

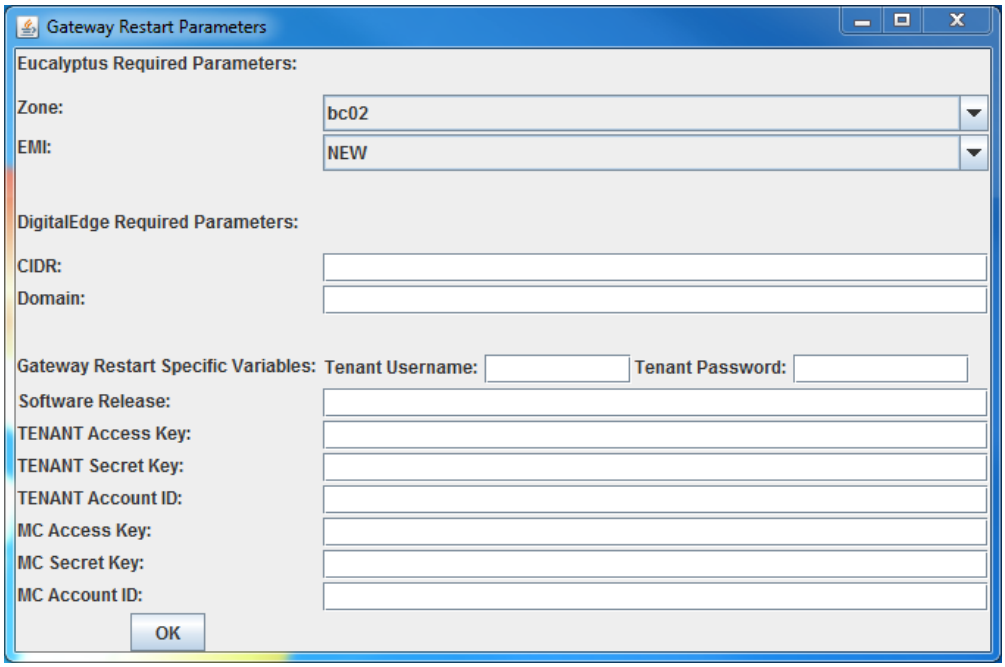


   All of the following parameters should match the values that you entered when you did a **Software Upgrade**:

   - **Service Endpoint IP**
   - **Storage Endpoint IP**
   - **Admin Access Key**
   - **Admin Secret Key** supply
   - **Admin Account ID**
   - **Username for controller**
   - **Password for controller** supply
   - **IP for controller**
   - **Public DNS Server IP (if required)**

   For an **Installation Type**, select **Gateway Restart**.

9. Click **OK**. A second list of parameters appears in the **Full Installation Parameters** dialog box:



The following parameters should match the values that you entered for the **Software Upgrade**:

- **Zone**
- **EMI**
- **CIDR**
- **Domain**

Finish installation with the following parameters:

- **Tenant Username**: The logon name of your DigitalEdge tenant account
- **Tenant Password**: The logon password of your DigitalEdge tenant account
- **Software Release**: The DigitalEdge software version number, found as the name of the `.tar.gz` file provided by Leidos
- **TENANT Access Key**: In the Eucalyptus console, **Keys** tab, copy the access key created for your DigitalEdge tenant username
- **TENANT Secret Key**: In the Eucalyptus console, **Keys** tab, copy the secret key created for your DigitalEdge tenant username
- **TENANT Account ID**: In the Eucalyptus console, copy the 12 digit IAAS service number under **Identity Management** > **Accounts** > **ID** created for your DigitalEdge tenant username
- **MC KeyPair**: You may have just one key pair in the drop-down menu to select. If the menu includes multiple key pairs, select the most recent one.
- **MC Access Key**: In the Eucalyptus console, **Keys** tab, copy the TMS access key
- **MC Secret Key**: In the Eucalyptus console, **Keys** tab, copy theTMS secret key

- **MC Account ID**: In the Eucalyptus console, copy the 12 digit IAAS service number under **Identity Management** > **Accounts** > **ID**

10. Click **OK** and **Next**. The **Upload Time** screen appears
11. Click **Next** to view progress as Eucalyptus finishes the software installation. A log file named installer.log is created in the selected **Install Folder** (step 4).
12. The installer displays the **Upload Output**.
13. You can now log on to DigitalEdge.

Installing a Software Upgrade

Appendix A: Terminology

Term	Definition
Alert	Email notification to a user that a potential fraud has been detected by DigitalEdge
AMI (Amazon Machine Image)	A bootable server that is a special type of pre-configured virtual machine in the cloud; AMIs serve as basic units of service deployment
Anchor node	In TMS, the anchor node hosts CAS, LDAP, and the TMS database
AWS™ (Amazon Web Services™)	Remote web services that comprise the cloud computing platform offered by Amazon and implemented in the Eucalyptus platform
Data sink	A queue, server, or database that can receive pipeline-processed JSON data to store or post-process for other uses
Dead letter queue	If an incoming record cannot be parsed for any reason, rather than ignoring it and dropping it out of the system, DigitalEdge saves the record in the dead letter queue where you can examine it and correct it.
EC2™ (Amazon Elastic Compute Cloud™)	A key part of Amazon's AWS™ public cloud computing platform, providing users the ability to create, launch, and end virtual server instances in a scalable deployment of applications
Elastic IP	A static IP address designed for cloud computing, associated with your Amazon account, not an instance; EC2 lets you mask problems by remapping an elastic IP address to a replacement instance
EMI (Eucalyptus Machine Image)	A pre-configured virtual machine, including the operating system and virtual application software, that can be used to create an instance in a Eucalyptus environment
Gateway node	A node in a tenant system that hosts CAS for single sign on permissions and LDAP for user account credentials. The Gateway node starts and stops systems, creates and deletes systems and security groups, and synchronizes components.
Hybridfox	An optional Firefox add-on that provides an interface to cloud accounts, including AWS and Eucalyptus, to help you manage images, instances, security groups, key pairs, elastic IPs, and storage.

Term	Definition
IAAS	The Infrastructure As a Service (IAAS) number is a tenant ID assigned by the facility providing your cloud services (e.g., Amazon or Eucalyptus). In the Eucalyptus Console, it is identified under **Identity Management** > **Accounts** > **ID#**. It is always a 12 digit number. In the DigitalEdge Management Console, it is listed as the account ID.
Master node	A VM (virtual machine) that launches all other nodes in a system. The master node handles auto-scaling, internal monitoring, starting and stopping for all instances. In TMS, the master node includes the Master Repository. In a tenant account, the master node includes the System Repository.
Master Repository	The Master Repository resides in TMS. It is the storage location for all common plug-in components provided with DigitalEdge, and private plug-in components used by each tenant account.
NAT (Network Address Translation)	An instance which is configured to perform network address translation and to serve as a firewall into the private Amazon VPC subnet
POC	Point of Contact information
Private IP	An internal RFC 1918 address that is only routable within the EC2 Cloud; traffic outside your EC2 network cannot access this IP
Public IP	An Internet routable IP address assigned by the system for all instances; Traffic routed to a public IP is translated via NAT and forwarded to an instance's private IP address
Repository	The storage location for all the plug-in components; the System Repository stores private components used in a tenant's DigitalEdge account, the Master Repository resides at the TMS level and stores all common and private components
S3™ (Amazon Simple Storage Service™)	The online storage web service provided with AWS™ and used as a data source for public cloud instantiations
Splitter	Each transport works with a specific incoming record type (JSON, XML, PCAP, etc.); the tranport's record-format parameter uses a splitter to define record boundaries when the input data includes multiple records
Tenant account	A tenant is an account on a cloud platform. In the public cloud, a tenant account typically represents an organization that is building an AWS application. On a private cloud,

Term	Definition
Primary tenant Secondary tenant	internal to an organization, a tenant account is usually a project or a department that runs its own secure applications. A *primary* tenant is the first tenant created in a DigitalEdge account (via the Installation program on a Eucalyptus system, via Registration on AWS systems). The primary tenant owns all the DigitalEdge resources: the system repository, LDAP, the tenant database, etc. and does not share data with other tenants. One or more *secondary* tenants may be created in an account. A secondary tenant is created by a TMS Administrator in the Management Console. All secondary tenants share the account resources that are owned by their primary tenant (system repository, LDAP, etc.), share and see all systems created under an account, and have the same privileges as the primary tenant. But secondary tenants have different logon credentials for security purposes.
TMS (Tenant Management System)	The Tenant Management System is a behind-the-scenes infrastructure for DigitalEdge to create and manage tenant accounts. TMS provides services to create new accounts, to monitor tenant applications, to calculate tenant usage activity and charges, to manage user identities and permissions, to manage the DigitalEdge GUI tools and plug-in components, and to provide security.
VPC™ (Amazon Virtual Private Cloud™)	An isolated environment within the AWS cloud where you can launch applications in a more secure, virtual network

Appendix B: What Each Node Does

Each node in DigitalEdge is a virtual machine and an instance of a process group, most of which are auto-scaling. To help size a system, the following table provides details about what each node does.

Node	Content
webapps.main (on TMS)	Home to all the DigitalEdge APIs, Setup tools, and Runtime tools, including: • Management Console • Data Modeler • Table Manager • System Builder • System Monitor
anchor (on TMS)	Security and authentication node, housing: • CAS (JA-SIG Central Authentication Service) • LDAP • TMS database • TMS Gateway
gateway	The node that controls a DigitalEdge system, including: • Launching the master node • Starting and stopping systems • Creating and deleting systems and security groups • Synchronizing components and repositories • Housing: ◦ CAS for single sign-on permissions ◦ LDAP for user account credentials ◦ APIs ◦ Tenant database
master	The management node of DigitalEdge, controlling: • Starting and stopping all instances • Monitoring for auto-scaling • Adding and removing nodes based on load and storage utilization • Handling virtual storage allocations

Node	Content
	• Gathering metrics for auto-scaling decisions • Housing the System Repository
transport	Controlling all transports through the Transport API
jms.external	First entry point into DigitalEdge, and a staging area for incoming data to: • Receive data pushed into the jms.external queue by other clients • Feed data directly into DigitalEdge • Manage the parsing queue • Receive processed alerts from the datasink.alert that match alerting criteria, and place a message in this queue for notifications
ingest.all	Ingest node to handle processing pipeline tasks, including: • Parsing • Enrichment
jms.internal	Internal staging area for the next steps in the processing pipeline; a buffer for records queued up waiting for the next phase of processing: • Post-enrichment record holding • Temporary record storage
datasink	Each type of data sink has its own node and processes data for specialized uses; for example: • datasink.alert - filtering records against alert criteria, sending alert messages to the configured recipient (such as a topic on the jms.external node, an email message, etc.) • datasink.hbase - storing records to the Hadoop Distributed File System (HDFS) • datasink.hive - storing records to HDFS • datasink.lucene - indexing records for searching • datasink.mongodb - storing JSON-based records and providing a query interface Some data sinks automatically add additional nodes when they are spawned; for example, HBase and Hive add nodes (such as zookeeper) that are needed for a complete HBase ecosystem

Node	Content
webapps.main (on tenant)	Home to all webapps and REST APIs, including: • Search app • Metrics API

Appendix C: Alternative to DNS Forwarding

If your organization is not able to create a DNS forwarder for the DigitalEdge subdomain on Eucalyptus, you can assign an elastic IP using the DigitalEdge **System Builder**. In this case, DigitalEdge will use IP addresses instead of DNS to access all its applications.

This solution may not be ideal for end users who prefer entering a name rather than remembering IP numbers.

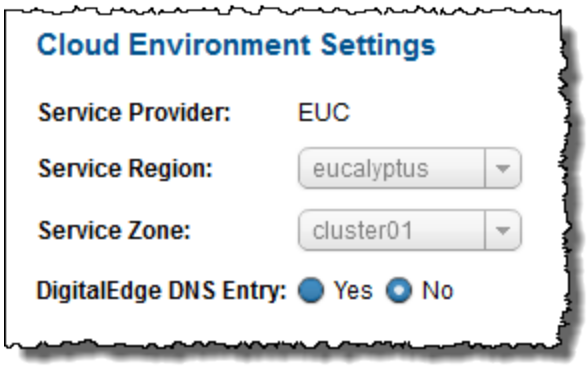
After you have installed DigitalEdge, when you configure and build a DigitalEdge system with **System Builder**, include these steps in the configuration process:

1. Access **System Builder**.
2. On the **Overview** tab, select:

a. **Service Provider** = EUC

b. **Service Region** and **Service Zone** = accept the defaults

c. **DigitalEdge DNS Entry** = No



a. Make sure the **Webapps** that you are using for your system are selected.

3. On the **Details** tab, double-click the **Public IP** selection of the **webapps.main** process group to assign the elastic IP.

a. In the **Specify Persistent IP Address** dialog box, check **Specific Address**.

b. Enter the IP address you wish to use for DigitalEdge. Or, click **Allocate IP Address** to have Hybridfox create an IP address for you to use (make note of the IP address for step 5).

c. Click **OK**.

4. When you are done with the system configuration, you must build (or rebuild, if you built the DigitalEdge system prior to this procedure) the site. Click **Build**.

5. Access the **Management Console** with:

   `https://<ip_address>/accounts/login`

   where `ip_address` is the address from step 3b.

6. **Start** the system.

Users will access the DigitalEdge system with the newly assigned IP address rather than by name. This IP address will be exclusive to DigitalEdge until the system is completely deleted from Eucalyptus.

Appendix D: What a Full Installation Does

The DigitalEdge installer does most of the installation work behind the scenes with minimal manual intervention. Here is what the installer does for a full installation:

- Checks to determine if an EMI is needed or if one is already created
- Verifies an existing EMI or creates and installs an EMI if needed
- Downloads several required third-party components
- Adds a Eucalyptus account for TMS
- Creates access and secret keys for the Eucalyptus account
- Creates a key pair to launch a Eucalyptus system
- Installs security groups needed for TMS
- Creates Walrus buckets that are needed for TMS
- Extracts, changes, and uploads files
    - Extracts the software release
    - Updates the domain to your specified name
    - Updates the interface files to use your parameters
    - Checks for Eucalyptus 3.2 or earlier versions
    - Updates services for TMS
    - Uploads software to the Walrus bucket
- Starts the TMS Master node
    - Creates elastic IP addresses for each TMS node, so that each node will always come up (from a down state) on the same IP
    - Waits for the second IP/node to launch
    - Connects to the TMS database
    - Pushes files to the TMS database
    - Adds an internal account to TMS for the creation of the first system
- Creates the first tenant account and primary tenant - You need at least one tenant account (cloud services account) to use the DigitalEdge platform. You can add multiple tenant accounts later, each representing a project in your organization which will be using DigitalEdge but will not be sharing data with other projects. You can also add secondary tenants later (via the Management Console) who share tenant resources but who have separate logon credentials.
    - Adds the primary tenant name and password (which you entered in the **Full Installation Parameters**) to the Eucalyptus tenant account
    - Creates keys in a PEM file
    - Shares EMIs

- Sets ACLs for the software release for the tenant account
- Sets up security groups to allow TMS into the tenant gateway node, enabling functionality such as creating user accounts in the DigitalEdge **Management Console**
- Sets up security groups to allow the tenant into the TMS Master Repository, enabling the sharing of common plug-in components used by DigitalEdge during configuration and the building of the processing pipeline
- Bounces Jetty on the TMS API node, so that the new domain and tenant ID appear in the database
- Adds the new tenant account to DigitalEdge (so that DigitalEdge knows which tenants are authorized to configure and build systems) and populates the tenant database
- Generates the DigitalEdge tenant ID and creates a Walrus bucket for the tenant
- Launches the tenant Gateway (which starts and stops systems, creates and deletes systems, and synchronizes components)

Appendix E: What the Tenant Installer Does

Here is what the tenant installer does to create a new account:

- Verifies an existing EMI
- Extracts, changes, and uploads files
    - Extracts the software release
    - Checks for Eucalyptus 3.2 or earlier versions
    - Updates services for TMS
    - Uploads software to the Walrus bucket
- Starts the TMS Master node
    - Creates elastic IP addresses for each TMS node, so that each node will always come up (from a down state) on the same IP
    - Waits for the second IP/node to launch
    - Connects to the TMS database
    - Pushes files to the TMS database
- Creates a new tenant account
    - Adds the primary tenant name and password (which you entered in the **Tenant Installation Parameters**) to the Eucalyptus account
    - Creates keys in a PEM file
    - Shares EMIs
    - Changes ACLs on all DigitalEdge software releases for the new tenant account
    - Sets up security groups to allow TMS into the tenant gateway node, enabling functionality such as creating user accounts in the DigitalEdge **Management Console**
    - Sets up security groups to allow the tenant into the TMS Master Repository, enabling the sharing of common plug-in components used by DigitalEdge during configuration and the building of the processing pipeline
    - Bounces Jetty on the TMS API node, so that the new tenant ID appears in the database
    - Adds the new tenant account to DigitalEdge and populates the tenant database
    - Generates the DigitalEdge tenant ID and creates a Walrus bucket for the tenant
    - Creates user startup data (users, schemas, tables, and indexes) for the tenant database
    - Launches the tenant Gateway (which starts and stops systems, creates and deletes systems, and synchronizes components)
    - Creates a default user for the new tenant

Appendix F: What the EMI Installer Does

The DigitalEdge installer does most of the installation work behind the scenes with minimal manual intervention. Here is what the EMI installer does:

- Links to the process for downloading an AMI
- Downloads several required third-party components
- Creates an EMI from the AMI and pushes it to Eucalyptus
- Bundles, uploads, and registers the ramdisk
- Bundles, uploads, and registers the machine image
- Bundles, uploads, and registers the EMI in Eucalyptus

Appendix G: What the Software Upgrade Installer Does

The DigitalEdge software upgrade installer does most of the installation work behind the scenes with minimal manual intervention. Here is what the software upgrade installer does:

- Extracts, changes, and uploads files
    - Extracts the software release
    - Updates the domain to your specified name
    - Updates the interface files to use your parameters
    - Checks the Eucalyptus version for an acceptable version and hypervisor
    - Updates services for TMS
    - Uploads software to the Walrus bucket
- Brings down the old TMS and starts a new master instance.
- Sets the ACLs for every tenant to have access to the new software.
- Starts the TMS Master node
    - Creates elastic IP addresses for each TMS node, so that each node will always come up (from a down state) on the same IP
    - Waits for the second IP/node to launch
    - Connects to the TMS database
    - Pushes files to the TMS database

Appendix H: What the Gateway Restart Install Option Does

The DigitalEdge gateway restart installer is only used as the final step in a software upgrade; it is not used on its own. To activate a new version of the software, DigitalEdge must stop and restart the gateway with the newest software release. Here is what the gateway restart does:

- Brings down the old gateway
- Sets up required gateway files from a template
- Generates and signs a certificate for the gateway to access DigitalEdge
- Launches the new gateway

Appendix I: Install Hybridfox

Hybridfox is an optional Firefox extension used to manage your cloud accounts, launch new instances, mount volumes, manage images and security groups, and map IP addresses in the Eucalyptus® environment. (Eucalyptus provides the same functionality offered by Hybridfox in the Eucalyptus Console and in their command-based Euca2ools.) Hybridfox serves the same purpose as the AWS Management Console.

1. Download Hybridfox.
2. Open Firefox.
3. Install Hybridfox 1.7+ by dragging the downloaded file into a Firefox window.
4. Restart Firefox after Hybridfox has been installed.
5. Start Hybridfox by selecting **Tools** > **Hybridfox**.
6. Click **Regions** and fill in the **Manage EC2 Regions** information:
   a. For a **Region Name**, enter *eucalyptus*.
   b. Select a **Signature Version** of *2.0*.
   c. Click a **Type** of **Eucalyptus**.
   d. Enter service **Endpoint URL**, such as http://<*IP_address*>/services/Eucalyptus.
   e. Click **Add**.

Appendix J: Create PuTTY PPK

PuTTY provides a terminal window to access remote machines that support SSH. For cloud-based systems, SSH is set up with public and private access keys. Use these instructions to generate a PuTTY-compatible private key file that will allow SSH access.

1. Start the program: `S:\Software\PuTTY\puttygen`.
2. Click **Conversions** > **Import Key**.
3. Navigate to the PEM file containing the private key you downloaded from your cloud.
4. Click **Save private key** and save it in PuTTY private key format (`.ppk`)

Appendix K: Create Environment for Euca2ools

Euca2ools are optional Eucalyptus command-line programs that interact with the Eucalyptus cloud and storage controllers to configure, manage, and run the cloud environment. To use them:

1. Be sure the Systems Administrator installed Euca2ools when he installed Eucalyptus.
2. Long on to the Eucalyptus controller node.
3. Run these commands:

```
$ mkdir ~/.euca; cd ~/.euca
$ sudo /usr/sbin/euca_config --get-credentials admin.zip
$unzip admin.zip
$source ~/.euca/eucarc
```

Index

A

account ID 59

accounts

creating a tenant account 32

setting up a tenant account 41

alerts

defined 58

Amazon EC2 1

defined 58

Amazon Elastic Compute Cloud

defined 58

Amazon Machine Image

defined 58

Amazon S3

defined 59

Amazon Simple Storage Service

defined 59

Amazon Virtual Private Cloud

defined 60

Amazon VPC

defined 60

Amazon Web Services

defined 58

AMI

defined 58

anchor node

defined 58

architecture

Eucalyptus 16

high level 4

Tenant Management System 5

TMS 5

AWS

defined 58

B

building a system

nodes 61

C

CentOS

installation 13

cloud controller

defined 16

installing 17

registering 19

cluster controller

configuring 20

defined 16

installing 19

registering 21

common components

synchronizing 39

components

DNS 8, 64

hardware 7

software 8

configuration

cluster controller 20

node controller 23

nodes 61

D

data sinks

defined 58

dead letter queue

defined 58

definitions 58

deleting

tenants 35

users 36

DigitalEdge

described 1

DNS entries

creating for tenant accounts 37

DNS Entry 64

DNS forwarder

setting up for tenant accounts 37

DNS forwarding 8

alternative 64

DNS zones

setting up for tenant accounts 37

documentation

types 2

typographical conventions 2

E

EC2

defined 58

Elastic Compute Cloud

defined 58

elastic IP

defined 58

EMI

defined 58

installing 45

ETL 1

euca2ools

configuring 74

Eucalyptus 1

architecture 16

cloud controller 17, 19

cluster controller 19

installation 16, 25

node controller 22-23, 25

storage controller 20-21

TMS administration 32

Eucalyptus Machine Image

defined 58

G

gateway node

creating for tenant accounts 37

defined 58

gateway restart 53

glossary 58

H

hardware requirements 7

Hybridfox

- defined 58
- installing 72

I

IAAS number

- defined 59

Infrastructure As a Service number

- defined 59

installation

- CentOS 13
- cloud controller 17
- cluster controller 19
- DigitalEdge 27
- EMI 45
- Eucalyptus 16, 25
- gateway restart 53
- Hybridfox 72
- node controller 22
- operating system 13
- overview 11
- prerequisites 7
- roadmap 11
- software 11
- software upgrade 49, 53
- steps 11
- tenants 41
- what the DigitalEdge installer does 66, 70-71
- what the software upgrade installer does 69
- what the tenant installer does 68

instances 61

IP addresses

- assigning 64
- webapps.main 64

IP, elastic

- defined 58

IP, private

- defined 59

IP, public

- defined 59

K

keys

- creating 73

L

log files 25

logging in 32

- tenant 31

logging out 39

M

Management Console

- allocating Master Repository space 36
- creating a tenant gateway node 37

creating DNS entries 37
creating security rules 38
creating tenant accounts 34
security groups 38
security rules 38
TMS Administrator tasks 32
using 32
master node
defined 59
Master Repository
allocating space for tenants 36
defined 59
N
NAT
defined 59
network address translation
defined 59
node controller
configuring 23
defined 16
installing 22
registering 25
nodes 61
NoSQL 1
Not Only SQL 1
O
operating system
installation 13
P
PaaS 1
platform-as-a-service 1
POC
defined 59
PPK
creating 73
primary tenants
defined 59
deleting 35
editing 35
private cloud 1
private IP
defined 59
private keys
creating 73
public cloud 1
public IP
defined 59
PuTTY PPK
creating 73
R
registration
cloud controller 19
cluster controller 21
node controller 25
storage controller 21

repositories
defined 59
Master defined 59
requirements 7
DNS 8
software components 8
S
S3
defined 59
secondary tenants
adding 34
defined 59
deleting 35
editing 35
security groups
creating at the TMS level 38
security rules 38
security rules
adding 38
creating at the TMS level 38
deleting 39
setup
Tenant Management System 27
TMS 27
Simple Storage Service
defined 59
software releases
upgrading 39, 49
software requirements 7-8
splitters
defined 59
standards
documentation 2
storage controller
configuring 20
registering 21
style conventions
documentation 2
synchronizing
repositories 39
systems 39
system architecture
high level 4
System Repository
defined 59
systems
synchronizing 39
upgrading 39
T
tenant account
defined 59
tenant ID 59
Tenant Management System 5
allocating Master Repository space 36
creating a tenant gateway node 37
creating DNS entries for tenant account 37

creating security rules 38
creating tenant accounts 34
defined 60
setup 27
tenants
adding 34, 41
creating accounts 32, 41
defined 5, 59
deleting 35
editing 35
primary 5, 59
secondary 5, 59
terminology 58
TMS 5
allocating Master Repository space 36
creating a tenant gateway node 37
creating DNS entries for tenant accounts 37
creating security rules 38
creating tenant accounts 34
defined 60
setup 27
typographical conventions
documentation 2
U
upgrading
software releases 39
systems 39
users
adding 36
deleting 36
editing 36
V
Virtual Private Cloud
defined 60
VPC 1
defined 60
W
webapps.main
assigning an IP 64