



# **EsgynDB 安装指南 2.4.0**

2018 年 10 月

## 版权

© Copyright 2018 Esgyn

## 公告

本文档包含的信息如有更改，恕不另行通知。

保留所有权利。除非版权法允许，否则在未经 Esgyn 预先书面许可的情况下，严禁改编或翻译本手册的内容。Esgyn 对于本文中所包含的技术或编辑错误、遗漏概不负责。

Esgyn 产品和服务附带的正式担保声明中规定的担保是该产品和服务享有的唯一担保。本文中的任何信息均不构成额外的保修条款。

## 声明

Microsoft® 和 Windows® 是美国微软公司的注册商标。Java® 和 MySQL® 是 Oracle 及其子公司的注册商标。Bosun 是 Stack Exchange 的商标。Apache®、Hadoop®、HBase®、Hive®、openTSDB®、Sqoop® 和 Trafodion® 是 Apache 软件基金会的商标。Esgyn 和 EsgynDB 是 Esgyn 的商标。

# 目录

<b>前言</b> .....	<b>vi</b>
本文简介.....	vi
目标读者.....	vi
相关文档.....	vi
修订历史.....	viii
<b>1. 前提条件</b> .....	<b>1</b>
<b>2. 准备 PC</b> .....	<b>1</b>
<b>3. 验证集群环境</b> .....	<b>2</b>
3.1 集群要求.....	2
3.2 检查磁盘空间.....	3
3.3 检查 Linux Swap 空间 .....	4
<b>4. 安装 Hadoop 发行版</b> .....	<b>5</b>
4.1 强制 Hadoop 服务和设置 .....	5
<b>5. 准备安装</b> .....	<b>6</b>
5.1 获取 sudo 访问权限和无密码 SSH（命令行安装） .....	6
5.2 配置 AD/LDAP Identity Store.....	7
5.3 集成 Kerberos.....	7
5.4 用户 ID 和密码.....	8
5.5 所需软件.....	9
5.6 收集信息.....	10
<b>6. 安装 EsgynDB</b> .....	<b>12</b>
6.1 命令行安装程序.....	12

6.2 管理.....	16
6.3 Cloudera Manager 安装程序.....	17
6.3.1 安装 CSD.....	17
6.3.2 安装 Parcel .....	18
6.3.3 将 EsgynDB 添加至现有集群.....	19
6.3.4 创建新的 EsgynDB 集群.....	20
6.3.5 选择主机 .....	21
6.3.6 Hadoop 配置.....	22
6.3.7 必需的配置项 .....	23
6.3.8 重要的配置项 .....	24
6.3.9 自动配置 .....	25
6.3.10 EsgynDB 配置.....	26
6.3.11 初始化元数据.....	27
6.3.12 启动 EsgynDB .....	28
6.4 验证.....	29
<b>7. 卸载 EsgynDB .....</b>	<b>31</b>
7.1 停止 EsgynDB .....	31
7.2 卸载 EsgynDB .....	31
<b>8. 故障排除.....</b>	<b>32</b>
<b>9. 启用安全功能 .....</b>	<b>33</b>
9.1 配置 Kerberos.....	34
9.1.1 Kerberos 配置文件 .....	34
9.1.2 管理 Ticket .....	36
9.1.3 安装 Kerberos.....	37
9.2 配置 LDAP .....	38
9.3 配置 AD/LDAP 服务器 .....	39

9.3.1 AD/LDAP 配置文件.....	39
9.3.2 ldapconfigcheck 脚本.....	43
9.3.3 ldapcheck 工具.....	45
9.4 生成服务器证书.....	47
9.4.1 自签名证书.....	47
9.4.2 生成 CSR.....	48
9.4.3 CA 签名证书.....	48
9.5 管理用户.....	49
<b>10. 提高安全性.....</b>	<b>50</b>
10.1 提高 Linux 安全性.....	50
10.2 提高 Hadoop 安全性.....	50
10.3 提高 Jetty Server 安全性.....	51
10.4 更新密码.....	51
10.5 提高端口安全性.....	51
10.6 提高 AWS 安全性.....	52
10.6.1 限制访问 Ambari 或 Cloudera Manager.....	52
10.6.2 限制访问 EsgynDB 组件.....	53
10.6.3 限制访问 EsgynDB 实例.....	54
10.6.4 总结.....	54
10.6.5 最后步骤.....	55
10.6.6 最佳实践.....	55
<b>附录 1. 验证配置文件.....</b>	<b>56</b>
<b>附录 2. Inspector 工具.....</b>	<b>61</b>
<b>附录 3. EsgynDB 在线增加节点.....</b>	<b>64</b>
<b>附录 4. EsgynDB 离线删除节点.....</b>	<b>69</b>

附录 5. 安装后配置 DCS Master 的 HA .....	79
附录 6. 在安装 EsgynDB 之后配置 LDAP .....	82
附录 7. 安装后配置 Kerberos 认证 .....	86

# 前言

---

## 本文简介

本文介绍如何在 Hadoop 集群上安装和配置 EsgynDB 2.4.0 核心产品（基于 Trafodion）和所需组件。

安装 EsgynDB 之前，请安装好操作系统或 Hadoop 发行版。更多关于这些组件的安装和配置信息，请参阅相关供应商文档。

## 目标读者

本指南的目标读者为 EsgynDB 和 Hadoop 系统管理员。

## 相关文档

本文档为 EsgynDB 文档库的一部分，EsgynDB 文档库**包括但不限于**以下文档：

《EsgynDB ADO.NET Provider 手册》	本文介绍如何使用 EsgynDB ADO.NET Provider 访问 EsgynDB。
《EsgynDB 备份与恢复指南》	本文介绍 EsgynDB 时间点还原功能。
《EsgynDB CQD 参考手册》	本文介绍控制查询默认（Control Query Default）设置，它能更改当前编译器会话环境和影响查询执行计划。
《EsgynDB 产品指南》	本文介绍安装 EsgynDB，包括架构、管理、备份与还原、用户自定义函数、数据加载、高可用和跨数据中心复制等。
《EsgynDB Manager 用户指南》	本文介绍网页管理工具 EsgynDB Manager，包括仪表盘、工作负载、日志、数据库、连接服务、查询工作台、安全、租户、警报和工具等。

《EsgynDB 多数据中心复制指南》	本文介绍 EsgynDB 跨数据中心复制用户数据。
《EsgynDB Windows ODBC 驱动安装指南》	本文介绍如何在 Window 系统安装 EsgynDB ODBC 驱动。
《EsgynDB 客户端安装指南》	介绍如何安装和配置各类客户端应用程序，例如，Trafodion 命令行界面（TrafCI）、Trafodion odb、DbVisualizer、Squirrel SQL 客户端和 JDBC/ODBC 驱动程序，方便用户连接并使用 EsgynDB。
《EsgynDB SQL 手参考册》	本文介绍 EsgynDB SQL 语句、实用程序、函数和其它 SQL 语言元素的语法。
《Trafodion 命令行界面指南》	本文介绍 Trafodion 命令行界面（TrafCI），该界面允许用户连接至 EsgynDB，交互式地或通过脚本访问 EsgynDB。
《EsgynDB 连接服务参考指南》	本文介绍如何对 EsgynDB 连接服务（Database Connectivity Service, DCS）进行配置、调优、排故和调试，这为基于 ODBC/JDBC API 开发的应用程序提供了访问 EsgynDB SQL 数据库服务器的框架；另外，本文还介绍了 DCS API。
《Trafodion odb 用户指南》	本文介绍如何配置并使用 Trafodion odb 工具，该工具是一个多线程、ODBC 命令行工具，能对数据执行 Trickle Load。
《Trafodion REST 服务器参考指南》	本文介绍如何启动、关闭、配置、排故和调试 Trafodion REST（Representational State Transfer）服务器；另外，本文简要介绍了 REST API。
《EsgynDB Designer 用户指南》	本文介绍如何使用 EsgynDB Designer，包括数据库连接管理、SQL 编辑器、Schema 浏览器管理和表管理等。
《EsgynDB Designer 安装指南》	本文介绍如何安装 EsgynDB Designer。

《EsgynDB 迁移工具用户指南》	本文介绍如何安装和使用 EsgynDB 迁移工具。
《EsgynDB 傻瓜手册系列——如何安装和卸载 EsgynDB? 》	本文介绍如何安装和卸载 EsgynDB, 包括单点安装、集群安装、基于原生 Hadoop 安装和卸载等。
《EsgynDB 傻瓜手册系列——如何使用 EsgynDB? 》	本文介绍如何使用 EsgynDB。
《EsgynDB 傻瓜手册系列——如何集成 EsgynDB 与 Zeppelin? 》	本文介绍如何安装、配置和使用 Zeppelin。

## 修订历史

大版本	小版本	日期
2.4	2.4.0	2018 年 10 月
2.3	2.3.0	2017 年 11 月
2.2	2.2.3	2017 年 3 月
	2.2.2	2017 年 3 月
	2.2.1	2017 年 2 月
	2.2.0	2016 年 11 月
2.1	2.1.0.2	2016 年 7 月
	2.1.0.1	2016 年 7 月
2.0	2.0.0	2015 年 11 月
1.0	1.0.0	2015 年 9 月

## 1. 前提条件

从 EsgynDB 2.2.0 开始，安装 EsgynDB 需要许可证密钥。安装前，请确保已取得许可证密钥。

## 2. 准备 PC

如果您使用 Windows 系统，在安装 EsgynDB 之前，建议您装好以下软件：

- PuTTY 和 PuTTYgen（如需下载，请参阅 <http://www.chiark.greenend.org.uk/~sgtatham/PuTTY/download.html>）
- VNC 客户端（如需下载，请参阅 <http://www.realvnc.com/>）
- Firefox 或 Chrome 浏览器
- SFTP 客户端（传输 PC 和服务器之间的文件）：WinSCP 或 FileZilla

## 3. 验证集群环境

安装 EsgynDB 之前，请验证集群环境。

### 3.1 集群要求

硬件平台	x86-64
操作系统	CentOS 6.5 ~ 6.9, 7.2 (64 位) Red Hat 6.5 ~ 6.9, 7.2 (64 位)
Hadoop 发行版	Cloudera CDH 5.4 ~ 5.9 Hortonworks HDP 2.3 ~ 2.5
	 <b>注意</b> CentOS/Red Hat Enterprise Linux 7.2 需要 CDH 5.7 或更高版本。
用户 ID	<p>如果使用命令行安装方式，用户需具备无密码 sudo 访问权限。</p> <p>更多信息，请参阅<a href="#">获取 sudo 访问权限和无密码 SSH</a>。</p>
集群大小	<p>集群由单个或 n 个节点组成。</p> <p>目前暂无上限，建议至少安装两个节点。</p>
磁盘空间	<p>最小 20 GB。</p> <p>更多信息，请参阅<a href="#">检查磁盘空间</a>。</p>
内存	<p>最小配置 = 1GB * 集群中每个节点连接服务器 (MXOSRVR 进程) 的数量。</p>

## 3.2 检查磁盘空间

安装 Hadoop 发行版之前，请确保至少有 20 GB 可用空间。

Cloudera CDH 的默认安装路径为 `/var/lib/cloudera-scm-server-db`。

如需检查 `/var` 可用空间，请启动 PuTTY 会话或在即将安装 Cloudera 集群的节点上启动 VNC 终端窗口。执行以下命令需要 `root` 或 `sudo` 访问权限。

确认 `/var` 至少有 20GB 可用空间。

```
$ cd "/var"
$ df -hP
```

如果 `/var` 没有足够空间，请为 Cloudera 数据库提供一个连接至其它驱动的连接，该驱动应有足够空间。

```
$ cd <new drive> (eg. cd /DATA)
$ mkdir cloudera-scm-server-db
$ chmod 777 cloudera-scm-server-db
$ cd /var/lib
$ ln -s <new drive>/cloudera-scm-server-db
```

如果 `/var` 是集群根文件系统的子目录，Cloudera 数据库应具有足够的可用空间。

如果已安装 CDH 并且 `log` 目录为红色，这表示 Cloudera 安装在 `/var/lib` 且 `/var` 文件系统较小。此时，您可以使用一个非正式脚本 (`clouderaMoveDB.sh`) 移动目录，该脚本在解压安装程序 (`tar.gz` 文件) 时被创建，位于 `installer/tools`。直接执行命令 `clouderaMoveDB.sh` 将显示帮助信息。

### 3.3 检查 Linux Swap 空间

为了使 EsgynDB 正常运行，必须设置 Linux Swap 空间。建议每个节点的 Swap 空间=总内存\*2，如果该方案不可行，建议至少每个节点的 Swap 空间=总内存\*1/2。

## 4. 安装 Hadoop 发行版

EsgynDB 2.4.0 与 Cloudera 和 Hortonworks 发行版兼容。

发行版	版本	HBase版本	安装
Cloudera发行版 包括Apache Hadoop (CDH)	CDH 5.4.5 ~ 5.13	1.0 1.2	更多关于安装Cloudera的信息，请参阅Cloudera官网
Hortonworks数据平台 (HDP)	HDP 2.3 ~ 2.5	1.1	更多关于安装 Hortonworks 的信息，请参阅 Hortonworks 官网

### 4.1 强制 Hadoop 服务和设置

安装 Hadoop 发行版之前，请检查以下强制服务和设置，确保安装时选择这些服务和设置：

- HDFS
- Yarn/MapReduce
- ZooKeeper
- HBase
- Hive
- Embedded Databases



EsgynDB 命令行安装程序需要在 EsgynDB 集群中的某一节点上运行。目前暂不支持在集群外节点上安装。所有 EsgynDB 节点必须安装 HBase。

## 5. 准备安装

---

### 5.1 获取 sudo 访问权限和无密码 SSH（命令行安装）

EsgynDB 安装要求用户 ID 具备以下属性：

- sudo 访问权限
- ssh 无密码访问集群上所有节点



#### 注意

如需获得此类权限，请向集群管理者申请权限。

如需获取 ssh 无密码访问权限，请按照以下步骤设置您的用户 ID：

1、在当前安装的节点上执行以下命令。

```
$ echo -e 'y\n' | ssh-keygen -t rsa -N "" -f  
$HOME/.ssh/id_rsa  
$ cat $HOME/.ssh/id_rsa.pub >> $HOME/.ssh/authorized_keys  
$ echo localhost $(cat /etc/ssh/ssh_host_rsa_key.pub) >>  
$HOME/.ssh/known_hosts  
$ echo "NoHostAuthenticationForLocalhost=yes" >>  
$HOME/.ssh/config  
$ chmod 600 $HOME/.ssh/config
```

2、将公钥文件 `$HOME/.ssh/id_rsa.pub` 的内容追加到每个节点的 `$HOME/.ssh/authorized_keys` 文件。

3、将私钥文件 `$HOME/.ssh/id_rsa` 复制至其它节点的 `$HOME/.ssh` 目录，将该文件的所有者更改为您，将文件属性更改为 700 (`chmod 700`)。

## 5.2 配置 AD/LDAP Identity Store

如需启用 EsgynDB 验证 (Authentication) 功能, 您需使用 AD/LDAP Identity Store 进行验证。EsgynDB 安装程序将提示您设置指向一个 (或多个) AD/LDAP 服务器的验证配置文件, 这将启用 EsgynDB 系统中的安全功能, 即 **验证 (Authentication)** 和 **权限 (Authorization)** 功能。

如需手动设置验证配置文件并启用安全功能, 请参阅 [9. 启用安全功能](#)。

## 5.3 集成 Kerberos

如果系统已启用 Kerberos, 则您需要在 EsgynDB 也启用 Kerberos。EsgynDB 安装程序将提示您设置 Kerberos (例如, 安装 principal 和 keytab)。更多信息, 请参阅 [9. 启用安全功能](#)。

## 5.4 用户 ID 和密码

以下为安装 EsgynDB 时使用的用户 ID 和密码。



### 注意

您将使用两个用户 ID，即您的用户 ID 和 trafodion。

登录	用户 ID	密码	说明
Cloudera Manager 网页登录	admin (默认)	admin (默认)	<ul style="list-style-type: none"> <li>安装 Cloudera 后，系统会提示您登录到 Cloudera Manager 页面。</li> <li>请使用默认的用户 ID 和密码 (admin, admin)。</li> <li>如果您已安装 Cloudera，请使用您过去指定的用户 ID 和密码。</li> </ul>
Ambari 网页登录	admin (默认)	admin (默认)	<ul style="list-style-type: none"> <li>安装 Hortonworks HDP 后，系统会提示您登录到 Ambari 页面。</li> <li>请使用默认的用户 ID 和密码 (admin, admin)。</li> <li>如果您已安装 HDP，请使用您过去指定的用户 ID 和密码。</li> </ul>
具有sudo访问权 限的用户ID	<sudo- username>	<password>	<ul style="list-style-type: none"> <li>安装时，您可能需要 sudo 或 sudo userid 权限。</li> <li>您将使用您的用户 ID，它具备 sudo 权限，并能 ssh 无密码访问集群中所有节点。</li> </ul>
EsgynDB 登录	trafodion	traf123 (默认)	<ul style="list-style-type: none"> <li>安装 EsgynDB 时，该用户 ID 由 EsgynDB 安装程序 <b>自动创建</b>。</li> <li>请勿手动创建该用户 ID。</li> </ul>

## 5.5 所需软件

安装前，EsgynDB 需要在集群上安装 Linux 软件依赖包，这些依赖包通常不是核心 Linux 发行版的一部分。安装程序会通过互联网自动获取这些软件包，但如果集群不能访问互联网，则您需手动下载软件包。

操作系统	软件包
CentOS Linux 6.5 ~ 6.9, 7.2	pdsh apr
Red Hat Linux 6.5 ~ 6.9, 7.2	log4cxx apr-util
	sqlite protobuf
	expect lzo
	perl-DBD-SQLite lzop
	xerces-c unzip
	perl-Params-Validate gcc-c++
	perl-Time-HiRes unixODBC
	gzip unixODBC-devel
	gnuplot libiodbc s
	lsof libiodbc-devel
	keepalived openldap-clients
	libcgroup snappy
	python-pip
	python-crontab

## 5.6 收集信息

安装时，安装程序将提示输入其它信息。开始安装之前，请确保您已了解以下信息：

信息	默认	备注
安装程序解压文件的路径	无	您需指定该路径。
许可密钥	无	Esgyn 公司提供。
每个节点并行客户端会话的数量	8	指定每个节点并行会话的数量。每个会话最多需要 1GB 内存，您能在安装后更改该值 <sup>1</sup> 。
在现有 EsgynDB 上升级安装或全新安装	无	如果在新集群上安装，安装程序将执行额外操作。
trafodion 用户 ID 和密码	用户 ID: trafodion  密码: traf123	建议您不要更改用户 ID。  如果使用命令行安装程序，则在所有节点上完成安装后，应更改密码。
集群中的节点列表	无	可以使用 sudo 或 root 用户无密码访问所有节点。
trafodion 用户 ID 的根目录路径前缀	/home	如果 trafodion 用户 ID 的根目录为 /opt/home/trafodion，则前缀为 /opt/home。
JDK 的路径	无	JDK 的绝对路径。   示例  /usr/java/jdk1.8.0_112-cloudera

<sup>1</sup> 更多信息，请参阅《EsgynDB DCS 安装指南》。

EsgynDB 安装程序压缩文件的路径	无	指定 EsgynDB 安装程序的完整路径。
Hadoop 发行版 URL	无	<p>在表单中指定：</p> <p>&lt;IP-address&gt;:&lt;port&gt; 或 &lt;node name&gt;:&lt;port&gt;</p> <hr/> <p> 示例</p> <p>vm-1.yourcompany.local: 7180</p>
<p>Hadoop 发行版详情</p> <ul style="list-style-type: none"> <li>• 管理员界面用户 ID、密码</li> <li>• 集群名称</li> <li>• HDFS 用户 ID</li> <li>• HBase 用户 ID、组</li> <li>• HBase 服务名称</li> </ul>	<ul style="list-style-type: none"> <li>• 依赖于发行版</li> <li>• Cluster1</li> <li>• hdfs</li> <li>• hbase, hbase</li> <li>• hbase</li> </ul>	
EsgynDB 安装目录	无	<p>指定目录的绝对路径。</p> <p>允许您维护软件的多个版本。</p>
DCS HA (高可用)	禁用	您将需要为 DCS 主机使用浮动 IP 地址、接口和备份节点。
安全	禁用	如需启用安全功能，确保已配置 AD/LDAP，且 AD/KLDAP 配置文件的名称可用。
Kerberos	可选项	如果系统已启用 Kerberos，则 EsgynDB 需要为 trafodion 用户创建 principle 和 keytab。

## 6. 安装 EsgynDB

---

### 6.1 命令行安装程序

EsgynDB 命令行安装工具为 `db_install.py`，它是一个独立的安装包。



#### 注意

EsgynDB 必须安装在已安装了 HBase Regionserver 的节点上（即已安装 Hadoop 发行版，更多信息，请参阅 [4. 安装 Hadoop 发行版](#)）。

如需使用命令行安装程序安装 EsgynDB，执行以下步骤：

- 1、以用户 `<sudo-username>` 身份，从 EsgynDB 集群中的任一节点开始执行安装程序，在集群的任一节点（通常是集群的第一个节点）上创建 `esgyndb_downloads` 目录。
- 2、下载以下文件，将它们放在 `esgyndb_downloads` 目录：
  - 服务器包
    - 根据不同的操作系统，数据库软件包可能是：
      - `esgynDB_server-2.4.0-RH6-x86_64.tar.gz` 或
      - `esgynDB_server-2.4.0-RH7-x86_64.tar.gz`
    - 相应的安装软件包
      - `esgynDB_pyinstaller-2.4.0-RH6.tar.gz` 或
      - `esgynDB_pyinstaller-2.4.0-RH7.tar.gz`

## 6. 安装 EsgynDB

```
$ mkdir $HOME/esgyndb_downloads
$ mv <your-download-path>/esgyndb_server-2.4.0-RH6-
x86_64.tar.gz $HOME/esgyndb_downloads
$ mv <your-download-path>/esgyndb_pyinstaller-2.4.0-
RH6.tar.gz $HOME/esgyndb_downloads
$ cd $HOME/esgyndb_downloads
```

3、解压下载的安装文件。

```
$ tar -xzf esgyndb_pyinstaller-2.4.0-RH6.tar.gz
```

4、打开安装目录。

```
$ cd python-installer
```

5、运行安装脚本，您能使用以下任一安装模式：

模式	说明	操作
引导设置	推荐新手使用。 安装时，系统将提示所需信息。	执行 <code>./db_install.py</code>
专家设置	推荐以下用户使用： <ul style="list-style-type: none"><li>资深用户</li><li>使用无人值守安装（Unattended Setup）方式的用户</li></ul> 配置文件是一个预编辑好的文本文件，它包含安装所需信息。安装程序如果使用该配置文件，在安装时不会提示用户输入信息。  配置文件的模板在 <code>python-installer/configs/db_config_default.ini</code> 中。  将该文件复制至您的文件夹，输入安装所需参数。	在安装配置文件中输入所需参数后，调用安装程序 <code>./db_install.py</code> <code>-config_file &lt;installer-config-file&gt;</code>



**注意**

- 如果出现配置错误，安装程序将中止。请在重新运行之前更正错误。
- 如果安装后不启动 Trafodion（即，在 Start Trafodion after install (Y/N) 时输入 N），则您需要在 db\_install.py 完成后手动启动和初始化 Trafodion。更多信息，请参阅以下提示。
- 更多有关手动启用 EsgynDB 安全功能的详细信息，请参阅 [9. 启用安全功能](#)。



**提示**

安装过程将：

- (1) 提示输入许可证密钥。

```
Add a new license file or license string (Y/N) [N]: Y
Enter full path to license file or the license string
[NONE]:
```

- (2) 在 CentOS/Redhat Linux 系统安装必要的 RPM 包。
- (3) 创建 trafodion 用户 ID。
- (4) 为 trafodion 用户 ID 设置无密码 ssh。
- (5) 将 EsgynDB 发行版文件复制至集群所有节点。
- (6) 生成启动文件。
- (7) 启动 EsgynDB、数据库连接服务 (Database Connectivity Services, DCS) 和 EsgynDB Manager 服务。

6、安装完成后，您将看到以下消息：

```
*****
Installation Complete
*****
```

## 6. 安装 EsgynDB

---

7、EsgynDB 现已启动并正在运行。请以 trafodion 用户身份登录 EsgynDB。如果您选择安装后不启动 trafodion，则需启动并初始化 trafodion，执行以下步骤。

```
cds
sqstart

[trafodion@esgvm-test ~]$ sqlci
EsgynDB Enterprise Conversational Interface 2.4.0
Copyright (c) 2015-2018 Esgyn Corporation
>>initialize trafodion;
```

## 6.2 管理

管理 EsgynDB 需要以 trafodion 用户身份登录。

以下为管理子系统的脚本。

组件	启动	停止	状态
EsgynDB core	sqstart	sqstop	sqcheck
RMS Server	rmsstart	rmsstop	rmscheck
REST Server	reststart	reststop	-
LOB Server	lobstart	lobstop	-
DCS (Database Connectivity Services)	dcstart	dcstop	dccheck



### 示例

启动 EsgynDB。

```
cd $MY_SQROOT/sql/scripts
```

```
sqstart
```

```
sqcheck
```

## 6.3 Cloudera Manager 安装程序

本小节讲述如何使用 Cloudera Manager 安装 EsgynDB，仅适用于已安装 CDH 的情况。

EsgynDB 软件由以下文件组成：

- 一个 CSD (Custom Service Descriptor, 用户服务描述符)
- 两个 parcel 文件
- 一个 parcel manifest 文件
- 配置辅助脚本 (cm\_settings.sh) 组成。

您可以使用辅助脚本，或参阅 [6.3.6 Hadoop 配置](#) 章节中的所需配置项。

EsgynDB 是一个独立的压缩的 tar 包，例如，`esgyndb-CM-version.tgz`。

### 6.3.1 安装 CSD

CSD 是一个名为 `ESGYNDB-version.jar` 的 jar 文件 (例如，`ESGYNDB-2.4.0-1.jar`)，该文件必须存放在 Cloudera Manager 服务器主机的本地描述符文件夹 (Local Descriptor Repository) 中，本地描述符文件夹的默认路径是 `/opt/cloudera/csd`。

- 如果未安装 Cloudera Manager，则您需提前创建文件夹，并将 EsgynDB CSD 文件放置在该文件夹中。Cloudera Manager 安装完成后，EsgynDB CSD 文件会被自动识别。
- 如果已安装 Cloudera Manager，重启服务器进程 (`cloudera-scm-server`) 后，EsgynDB CSD 文件会被自动识别，例如，`sudo service cloudera-scm-server restart`。

### 6.3.2 安装 Parcel

ESGYNDB\_TRX parcel 文件是 HBase 处理事务的插件。ESGYNDB parcel 文件主要提供 SQL 引擎和其它数据库服务。

Parcel 文件和 parcel manifes 文件必须存放在远程 parcel 目录中，该目录是常规或临时网络服务器路径。

如需更改 parcel 文件位置，执行以下操作：

- 1、 点击 Cloudera Manager 菜单栏的 **Parcel** 图标。
- 2、 点击 **配置 (Configuration)**。
- 3、 选择 **添加远程 Parcel 文件 URL (Add a new Remote Parcel Repository URL)**。输入 EsgynDB parcel 文件位置。
- 4、 在 Parcel 主页上，点击 **检查新的 Parcel 文件 (Check for New Parcels)**。

现在 Cloudera Manager 了解 EsgynDB 服务和 EsgynDB parcel 文件的位置，您能开始安装 EsgynDB 服务。

### 6.3.3 将 EsgynDB 添加至现有集群

如需将 EsgynDB 添加至现有集群，执行以下步骤：

- 1、在 Parcel 主页上，选择**集群 (Cluster)**。
- 2、对 ESGYNDB\_TRX 和 ESGYNDB parcels 文件执行以下操作：
  - (1) 下载
  - (2) 分配
  - (3) 激活
- 3、更改所需 Hadoop 配置的设置，如有需要，重启服务（至少重启 HBase）。
- 4、在集群的**操作 (Action)** 菜单上选择**添加服务 (Add Service)**，再选择 EsgynDB。



#### 注意

必须在所有 HBase Regionserver 主机上激活 ESGYNDB\_TRX 文件。

### 6.3.4 创建新的 EsgynDB 集群

添加新的集群时，您也能安装 EsgynDB。

- 1、选择 parcel 文件时，请选择 CDH、ESGYNDB 和 ESGYNDB\_TRX。
- 2、选择服务时，在**用户服务 (Custom Service)** 列表中选择 EsgynDB，它会自动包括某些独立服务（例如，HBase）。



#### 注意

此时，EsgynDB 服务会报错且无法启动，请完成 HBase 所需的配置设置并重启 HBase。

如果 EsgynDB 启动进程报出 TRX 协处理器配置错误，Cloudera Manager 将允许您重试或退回。请返回主页面，按需配置 Hadoop 并重启服务。

您也需要启动 EsgynDB。在 EsgynDB **操作 (Action)** 菜单上，选择**初始化 EsgynDB 元数据 (Initialize EsgynDB MetaData)**，启动 EsgynDB。

## 6.3.5 选择主机

### 6.3.5.1 EsgynDB 节点

这是主要的工作角色，它运行数据库查询，并与其它 Hadoop 组件（例如，HDFS、HBase 和 Hive）集成。通常 EsgynDB 节点安装在 HBase Regionserver 节点上，也能安装在 HBase Gateway、Regionserver 或 Master 节点上。由于 EsgynDB 节点也能作为 Hive 客户端，所以它需要与 Hive Gateway 或服务器安装在相同位置。

### 6.3.5.2 分布式连接服务器

分布式连接服务器（Distributed Connectivity Server）将外部请求（JDBC/ODBC 连接）路由至指定节点。为了提高可用性，您需要部署多个节点。分布式连接服务器必须和 EsgynDB 节点安装在相同位置。

如果配置了浮动 IP，当前活动 DCS Master 节点将绑定该 IP 地址。使用该功能需要 sudo 权限执行一些网络配置命令，否则您需要为客户端驱动（JDBC/ODBC）提供服务器节点列表（而不是提供单个浮动 IP 地址）；或者使用 keepalived 包管理浮动 IP 网址。EsgynDB 将提供一个示例配置文件，但由于 Cloudera Manager 未管理 keepalived，所以您需要单独配置 keepalived。

### 6.3.5.3 EsgynDB Manager

EsgynDB Manager 提供监控和操作 EsgynDB 集群的管理界面。

EsgynDB Manager 必须和 EsgynDB 节点安装在相同位置。

### 6.3.6 Hadoop 配置

EsgynDB 依赖于某些 HDFS、Zookeeper 和 HBase 的配置项，如果设置错误，EsgynDB 将无法启动。您可以通过 Cloudera Manager 或其它工具，更改配置项的值。

### 6.3.7 必需的配置项

启动 EsgynDB 服务前，设置以下 HBase 配置项。

hbase-site.xml 中 Region Server 高级配置：

名称	值
hbase.hregion.impl	org.apache.hadoop.hbase.regionserver.transactional.TransactionRegion
hbase.regionserver.region.split.policy	org.apache.hadoop.hbase.regionserver.ConstantSizeRegionSplitPolicy



#### 注意

ESGYNDB\_TRX parcel 文件必须在所有 HBase Regionserver 节点启动，否则会导致 HBase 错误。

### 6.3.8 重要的配置项

建议按照以下方式设置 HBase。

名称	值
<code>hbase.regionserver.lease.period</code>	1 (小时)
<code>hbase.hregion.memstore.flush.size</code>	512 (MiB)
<code>hbase.hregion.memstore.block.multiplier</code>	7
<code>hbase.hstore.blockingStoreFiles</code>	200
<code>hbase.rootdir.perms</code>	750
<code>hbase.snapshot.master.timeoutMillis</code>	10 (分钟)
<code>hbase.superuser</code>	trafodion

建议按照以下方式设置 HDFS。

名称	值
<code>dfs.namenode.acls.enabled</code>	true

建议按照以下方式设置 Zookeeper。

名称	值
<code>maxClientCnxns</code>	0

如果已启用 Sentry，建议按照以下方式设置 Sentry。

名称	值
<code>sentry.service.admin.groups</code>	trafodion
<code>sentry.service.allow.connect</code>	trafodion

### 6.3.9 自动配置

您能通过 `cm_settings.sh` 工具设置 Hadoop，该工具可以在任何连接至集群管理器主机的 linux 系统上运行。

`-h` 显示所有选项列表。

该工具显示每个参数的当前设置和建议设置，并提示您进行相应操作（也可以取消该提示）。



#### 示例

```
cm_settings.sh -s https://myhost.domain.net:7180 -c  
"Cluster5" -u joe_admin
```

该工具需要您使用 Cloudera Manager 进行身份验证。验证结束后，验证信息保存在会话缓存中并被脚本的剩余部分使用，再被删除。

以下三个选项提供密码：

- 默认选项：支持底层 `curl` 命令，提示您输入密码。
- `-n` 选项：在标准 `~/.netrc` 文件中寻找密码。
- `-p` 选项：通过命令行输入密码。该选项安全性较低，不推荐使用。

使用该工具后，在 Cloudera Manager 网页上重启服务。

## 6.3.10 EsgynDB 配置

### 6.3.10.1 许可密钥

安装 EsgynDB 时，您需要输入许可密钥。您能在 EsgynDB 2.4.x 上使用 2.3.x 许可密钥。

初次安装时：

- 非生产环境：请使用 Esgyn 提供的密钥。
- 生产环境：您可以暂时不输入许可密钥（有一定的宽限期），继续完成剩余安装步骤。

如需获取许可密钥，请发送 `/etc/trafodion/esgyndb_id` 文件的副本至 Esgyn，该文件是一个较小的二进制文件，提供了唯一集群 ID。

### 6.3.10.2 其它

安装完成后，您能配置其它功能，包括 AD/openLDAP 连接和连接 HA。

如果 Hive 启用了 Sentry 安全，请在 **Hive Sentry enabled** 中将 `traf.sentry.enabled` 的值设置为 `true`。

### 6.3.11 初始化元数据

首次安装 EsgynDB 或安装新版本的 EsgynDB 后，需要初始化元数据。在 Cloudera Manager 的 EsgynDB 服务中，在操作 (Actions) 菜单上，选择启用 **EsgynDB 元数据 (Initialize EsgynDB MetaData)**。

重复执行以上操作不会报错。如果已开启初始化，重复执行以上操作不会产生任何影响。

如果已进行 ODBC/JDBC 连接 (例如，DB Manager)，即使成功完成初始化，但系统可能仍然会报告 EsgynDB 未初始化，此时请重启 EsgynDB 服务或使用 EsgynDB 操作 (Action) 菜单的**强制连接重启 (Force Connections Restart)**。

### 6.3.12 启动 EsgynDB

Cloudera Manager 报告 EsgynDB 角色已成功启动后，EsgynDB 子系统还需要几分钟启动并接受请求。

如需了解更详细的状态，您可在 EsgynDB 服务中的**操作 (Actions)** 菜单上获取检查 EsgynDB 状态的命令。

## 6.4 验证

执行基础完备性检查。

1、使用 sqlci 创建一张表，并写入数据。

```
[trafodion@edb001 ~]$ sqlci
EsgynDB Enterprise Conversational Interface 2.4.0
Copyright (c) 2015-2018 Esgyn Corporation

>>CREATE TABLE test1 (f1 int, f2 int);
--- SQL operation complete.

>>INSERT INTO test1 VALUES(1,1);
--- 1 row(s) inserted.

>>INSERT INTO test1 VALUES(2,2);
--- 1 row(s) inserted.

>>SELECT * FROM test1;

F1          F2
-----
          1          1
          2          2

--- 2 row(s) selected.

>>GET TABLES;

Tables in Schema TRAFODION.SEABASE
=====

TEST1
```

```
--- SQL operation complete.  
>>exit;
```

- 2、使用 `mgbly_check` 工具验证所有管理组件（EsgynDB Manager、TSD、TCollector 和 Bosun）正在运行。

```
[trafodion@edb001 ~]$ mgbly_check  
  
Status of OpenTSD...(Expect 1 per node)  
Total count of TSD process: 12  
  
Status of Tcollector...(Expect 1 per node)  
Total count of tcollector process: 12  
  
Status of DBMgr...(Expect 1 per DB Manager node)  
Total count of dbmgr process: 1  
  
Status of Bosun...(Expect 1 per DB Manager node)  
Total count of bosun process: 1
```

- 3、在浏览器中输入 `http://localhost:4205`，验证是否能启动并登陆 EsgynDB Manager<sup>2</sup>。
- 4、如需将客户端应用程序连接至 EsgynDB，您可以下载并安装 EsgynDB JDBC 和/或 ODBC 驱动程序（安装程序名称为 `esgynDB_clients-2.4-RH6-x86_64.tar.gz`<sup>3</sup>）。

---

<sup>2</sup> 更多信息，请参阅《EsgynDB Manager 用户指南》。

<sup>3</sup> 更多信息，请参阅《EsgynDB 客户端安装指南》，该指南说明如何安装 JDBC 和 ODBC 驱动程序、如何连接到 EsgynDB、以及如何运行示例程序测试连接。

## 7. 卸载 EsgynDB

---

使用 Trafodion 配置用户 ID 执行以下操作。

在集群的第一个节点上运行命令，请勿在非 EsgynDB 集群的节点上运行命令。



更新 EsgynDB 无需使用 `trafodion_uninstaller` 脚本。

### 7.1 停止 EsgynDB

以下命令停止 EsgynDB：

```
$ su trafodion
$ cd $TRAF_HOME/sql/scripts
$ sqstop
$ exit
```

### 7.2 卸载 EsgynDB

以下命令卸载 EsgynDB：

```
db_uninstall.py
```

## 8. 故障排除

---

- 1、如果启动环境失败或运行 sqlci/trafci 出现问题，使用命令 `trafcheck` 检查所有 EsgynDB 进程是否正常工作。
- 2、如果进程未正常运行，执行以下操作：
  - (1) 使用命令 `sqstop` 关闭 EsgynDB。如果无法关闭部分 EsgynDB 进程，使用命令 `ckillall`。
  - (2) 使用命令 `sqstart` 重启 EsgynDB。
- 3、如果问题仍然存在，请检查日志文件 `$TRAF_HOME/logs: EsgynDB logs`。

## 9. 启用安全功能

---

EsgynDB 使用 OpenLDAP 和 AD 进行用户验证、与 Kerberos 环境集成并支持权限功能（授予和撤回权限）。

您可以通过 EsgynDB 安装程序配置 AD/LDAP（可选项）。如果已启用 Kerberos，则 EsgynDB 安全安装程序将提示您输入所需信息。



### 注意

- 如果 Hadoop 已启用 Kerberos，则 EsgynDB 必须也启用 Kerberos。
- 如果未启用 Kerberos，则启用 AD/LDAP 是可选项。
- 如果启用 AD/LDAP 或多租户，则数据库权限功能将自动启用。

## 9.1 配置 Kerberos

Kerberos 是为服务或操作验证请求的协议，它使用票据 (ticket) 验证访问性。票据是身份证明，它通过密钥为特定请求服务加密。票据有效期较短，在票据的有效期内，您能使用服务。Hadoop 使用 Kerberos 为服务提供安全性，使用 EsqynDB 时，需启用 Kerberos。

### 9.1.1 Kerberos 配置文件

假设安装 EsqynDB 时，已在所有节点上配置 Kerberos。Kerberos 默认的配置文  
件为 /etc/krb5.conf，包括以下属性：

```
* log location: location where Kerberos errors and other
information are logged
* KDC location: host location where the KDC (Key
Distribution Center) is located
* admin server location: host location where the Kerberos
admin server is located
* realm: the set of nodes that share a Kerberos database
* ticket defaults: contains defaults for ticket
lifetimes, encoding, and other attributes
```

如需启用 Kerberos，您需要拥有访问 Kerberos 管理员账户权限。



#### 示例

以下是 Kerberos 定义的 principal，用于测试连接：

```
kadmin -p 'kdcadmin/admin' -w 'kdcadmin123' -s
'kdc.server' -q 'listprincs'
* -p (principal): please replace 'kdcadmin/admin' with
your admin principal
* -w (password): please replace 'kdcadmin123' with the
password for the admin principal
* -s (server location): please replace 'kdc.server' with
```

```
your KDC admin server location
```

```
* -q (command): defines the command to run, in this case  
principals are returned
```

## 9.1.2 管理 Ticket

在 EsgynDB 中启用 Kerberos 时，安全安装过程如下：

- 1、在 Kerberos 中添加 trafodion principal，每个节点添加一个 principal，principal 名称为 trafodion/hostname@realm。
- 2、为每个 principal 创建 keytab，将 keytab 分配至每个节点。所有节点的 keytab 名称相同（不同发行版的默认 keytab 名称不同），例如，etc/trafodion/keytab/trafodion.keytab。
- 3、为 Trafodion 用户在集群所有节点上执行 kinit 命令。
- 4、在每个节点上执行 kinit 命令并启动 EsgynDB ticket 更新程序。

Hadoop 更新服务会尽可能多地更新 Kerberos TGT (Ticket Granting Ticket)。如果 ticket lifetime 为 1 天且 renew lifetime 为 7 天，则该 ticket 能用 7 天。renew lifetime 过期后，EsgynDB 将重新初始化 ticket，因此 ticket 永远有效。EsgynDB 更新服务在集群的每个节点上运行，并监控 Esgyn Kerberos TGT 的状态。

EsgynDB 提供脚本 trafkerberos，它汇报 Kerberos TGT 的状态：

```
$TRAF_HOME/sql/scripts/trafkerberos { status | stop |
start }
status: reports the status of the Kerberos ticket across
all nodes:
stop: stops the EsgynDB ticket renewal process
start: starts or restarts the EsgynDB ticket renewal
process.
```

### 9.1.3 安装 Kerberos

EsgynDB 安装脚本自动决定是否在节点上启用 Kerberos。如果启用，环境变量 `SECURE_HADOOP` 将被设置为“Y”。为了集成 Kerberos 和 EsgynDB，安装程序将收集以下信息：

```
KDC server address
KDC admin principal
KDC admin password
Max lifetime for the trafodion user
Max renew lifetime for the trafodion user
```



安装完成后，KDC 管理员密码仅保存在安装程序目录的配置文件 `db_config.bakYYMMDD_HHMM` 中。为了提高安全性，您可以删除该文件。



CDH/HDP 集群中的安装程序将自动检测 keytab 文件。

## 9.2 配置 LDAP

EsgynDB 自身不管理用户名和密码，它通过使用 OpenLDAP 和 AD/LDAP 协议（即 AD/LDAP 服务器）的目录服务器支持验证功能。如需配置 AD/LDAP 服务器，请在安装过程中回答安装程序的问题。更多信息，请参阅 [9.2 配置 LDAP 服务器](#)。安装 AD/LDAP 将启用数据库权限功能。

启用验证和权限功能后，EsgynDB 允许在数据库中注册用户，并向用户和角色授予对象的权限。EsgynDB 还支持组件级（或系统级）权限，例如，您能向用户和角色授予 `MANAGE_USERS` 权限<sup>4</sup>。



### 注意

如果 EsgynDB 未启用 AD/LDAP，则客户端需输入用户名和密码才能连接至 EsgynDB，但 `trafodion` 忽略该用户名和密码，会话将以数据库根用户（`DB_ROOT`）身份运行（无限制）。如需限制用户，即限制某些用户访问数据库或限制访问对象或操作，您需要启用安全功能，即启用验证和权限功能。

---

<sup>4</sup> 更多信息，请参阅《EsgynDB SQL 参考手册》。

## 9.3 配置 AD/LDAP 服务器

EsgynDB 安装程序设置并传播 AD/LDAP 配置文

件.traf\_authentication\_config, 该文件位于

\$TRAF\_HOME/sql/scripts, 它是由一系列属性/值对组成的文本文件。

示例文件位于

\$TRAF\_HOME/sql/scripts/traf\_authentication\_config。

### 9.3.1 AD/LDAP 配置文件

AD/LDAP 配置文件是.traf\_authentication\_config。



#### 示例

```
SECTION: Defaults
  DefaultSectionName: local
  RefreshTime: 1800
  TLS_CACERTFilename:
SECTION: local
  Section configuration attributes
SECTION: aaa
  Section configuration attributes
. . .
SECTION: zzz
  Section configuration attributes
```

SECTION: local 是必选, 其它 section 是可选, 如需多个 AD/LDAP 配置, 您可以指定 section 参数。例如, 以 tenant1 身份登录的用户需通过在 section aaa 中定义的 AD/LDAP 服务器进行验证, 以 tenant2 身份登录的用户需通过在 section bbb 中定义的 AD/LDAP 服务器进行验证。

配置文件中的每个 section 至少具备以下参数:

- AD/LDAP 主机名

属性名称是 LDAPHostName。

必须指定一个或多个支持 OpenLDAP 或 AD 协议的主机名。EsgynDB 将尝试在验证过程中连接所有提供的主机名。所有主机上的用户名和密码集应相同。



示例

```
LDAPHostName: ldap.company.com
```

- LDAP 端口号

属性名称是 LDAPPort。

AD/LDAP 服务器的端口号。通常不使用加密或 TLS 的服务器的端口号是 389，使用 SSL 的服务器的端口号是 636。



示例

```
LDAPPort: 389
```

- LDAP 唯一标识符。

属性名称是 UniqueIdentifier。

目录服务器使用该属性唯一地识别用户名。您可以指定一个或多个唯一标识符。



示例

```
UniqueIdentifier: uid=,ou=users,dc=com
```

- 加密等级

属性名称为 LDAPSSL。

AD/LDAP 服务器使用的加密方式等级，等级为：

0: 不加密

1: SSL

2: TLS



示例

```
LDAPSSL: 2
```

如果 AD/LDAP 服务器使用 TLS，则必须指定包含证书的文件，该证书用于加密密码。默认情况下，EsgynDB 在 \$MY\_SQROOT/cacerts 中查找该文件，但您必须指定一个绝对路径文件名，或在另一个目录中设置环境变量 CACERTS\_DIR。如需指定包含证书的文件，您需要设置位于 Defaults section 的属性 TLS\_CACERTFilename。



示例

```
TLS_CACERTFilename: mycert.pem  
TLS_CACertFilename: /usr/etc/cert.pem
```

- LDAP 查找识别名、LDAP 查找密码

属性名称为 LDAPSearchDN、LDAPSearchPwd。

为了查找用户名的目录，某些 AD/LDAP 服务器需要已有用户名和密码。如果您的环境有类似要求，请提供用户名和密码。



示例

```
LDAPSearchDN: lookup@company.com  
LDAPSearchPwd: Lookup123
```

如果已配置的 AD/LDAP 服务器需要用户组执行查找操作，则需要以下属性：

- LDAPSearchGroup
  - LDAPSearchGroupBase
  - LDAPSearchGroupObjectClass
  - LDAPSearchGroupMemberAttr
  - LDAPSearchGroupNameAttr

如需使用其它属性自定义 EsgynDB 验证，请参阅示例配置文件 `$TRAF_HOME/sql/scripts/traf_authentication_setup`。



#### 注意

EsgynDB 安装脚本仅设置 local section，不设置 group 属性。如需配置多个 section 和 group，请修改文件 `.ldap_authentication_config` 并将该文件复制至所有节点。

### 9.3.2 ldapconfigcheck 脚本

ldapconfigcheck 检查验证配置文件中的语法错误。

- 如果已加载 EsgynDB 环境 (sqenv.sh), 则 ldapconfigcheck 会自动检查文件

```
$MY_SQLROOT/sql/scripts/.traf_authentication_config.
```

- 如果未加载 EsgynDB 环境, 您可以指定待检查的文件, EsgynDB 无需运行 ldapconfigcheck。

#### 9.3.2.1 语法

```
ldapconfigcheck [<option>]...
<option> ::= --help|-h : display usage information
           -file <config-filename>
```

如果未指定配置文件名, 则 ldapconfigcheck 会查找使用环境变量的文件。

以下是环境变量和查找顺序:

- 1、 TRAFAUTH\_CONFIGFILE  
指定完全限定名称。
- 2、 TRAFAUTH\_CONFIGDIR  
文件名.traf\_authentication\_config/追加至指定目录。
- 3、 TRAF\_HOME  
/sql/scripts/.traf\_authentication\_config追加至 TRAF\_HOME。



#### 示例

```
ldapconfigcheck -file myconfigfile
File myconfigfile is valid.
```

如果发现错误, ldapconfigcheck 会显示错误及行号。

### 9.3.2.2 错误

使用 `ldapconfigcheck` 时，可能会返回以下值，但仅报告遇到的第一个错误。

代码	文本
0	<code>filename</code> 文件有效。
1	未找到 <code>filename</code> 文件。
2	文件: <code>filename</code> line-number 行中的属性名称无效。
3	文件: <code>filename</code> line-number 行缺少值。
4	文件: <code>filename</code> line-number 行中的值超出范围。
5	文件: <code>filename</code> 打开 <code>traf_authentication_config</code> 文件失败。
6	文件: <code>filename</code> 读取 <code>traf_authentication_config</code> 文件失败。
7	未提供文件。请指定文件参数或验证环境变量。
8	配置文件中至少已使用一次 TLS，但未提供 TLS_CACERTFilename。
9	配置文件中至少有一组缺失主机名。 每个 LDAP 连接配置必须提供至少一个主机名。
10	配置文件中至少有一组缺失唯一标识符。 每个 LDAP 连接配置必须提供至少一个唯一标识符。
11	必须指定至少一个 LDAP 连接配置。
12	解析 <code>.traf_authentication_config</code> 文件时出现内部错误。

### 9.3.3 ldapcheck 工具

ldapcheck 测试 AD/LDAP 连接。

使用该命令时必须加载 EsgynDB 环境 (sqenv.sh)，但无需运行 EsgynDB 实例。如果仅测试连接，您能指定任何用户名或 group 名，此时，traf\_authentication\_config 中的属性将查找您指定的用户名或 group 名。

#### 9.3.3.1 语法

```
ldapcheck [option]...
option ::= --help|-h

           --username=<LDAP-username>
           --password[=<password>]

or

           --groupname=<LDAP-groupname>
           --confignumber=<config-section-number>
           --configname=<config-section-name>
           --verbose
```

如需查看更详细的错误信息，请使用 `--verbose` 选项。ldapcheck 将日志事件记录在文件夹 `$TRAF_HOME/logs`，日志名称格式为 `dbsecurity_<host>_<pid>.log`。

如果提供密码，则 ldapcheck 将尝试验证指定的用户名和密码。以下示例显示了密码，但建议您将密码留空 (`--password=`)，ldapcheck 将提示输入密码 (不回显)。



```
ldapcheck --username=user1 --password=user1passwd
Authentication request: externalName user1, configName
'local' (configNumber 0), result 0 (Authentication
successful)

Member of group: group1
```

## 9.4 生成服务器证书

EsgynDB 使用证书加密/解密密码（验证用户）以及为网页应用程序提供 HTTPS 支持。默认情况下，自签名证书使用 OpenSSL 生成，保存在集群每个节点的 `$HOME/sqcert` 中。另外，您还能使用 CA 签名证书。

### 9.4.1 自签名证书

自签名证书是一个身份认证证书，该证书由一个实体签发，该实体的身份由其自身进行认证。安装和更新时，EsgynDB 安装程序将生成自签名证书，并保存在集群每个节点的 `$HOME/sqcert` 中。证书有效期为 365 天，保存以下文件：

- `server.crt`  
证书。
- `server.key`  
私钥。
- `server.keystore`

Java KeyStore，用于保存实例在 SSL 加密时的安全证书。



#### 注意

Java KeyStore 保存授权证书或公钥证书，通常被 Java 应用程序用于加密、验证和服务 HTTPS。keystore 密码保护 Java KeyStore 中的实体。keystore 实体由别名（alias）识别，它由 key 和证书组成，从而形成了信任链。

如果集群使用了证书且您收到证书过期的通知，则您需要手动生成自签名证书（运行脚本 `sqcertgen` 和 `sqcertget gen_keystore`），再重启连接和管理服务（运行命令 `dcstop`、`mgblyt_stop`、`dcstart` 和 `mgblyt_start`）。

如需验证证书，运行命令 `certcheck`。

## 9.4.2 生成 CSR

- 1、使用服务器秘钥生成 CSR (Certificate Signing Request, CSR), 运行命令 `sqcertgen gen_csr`。
- 2、发送 CSR 至证书授权中心 (Certificate Authorit, CA)。

CA 签名后, 您将得到一个签名证书, 您可以在集群中部署该签名证书。

## 9.4.3 CA 签名证书

证书授权中心 (Certificate Authorit, CA) 是发放数字证书的实体。数字证书证明证书主体拥有公钥, 这允许依赖方 (Relying Parties) 依赖签名或使用对应的私钥进行认证。

CA 是受信任的第三方, 它被证书所有者和依赖证书者信任。证书的格式遵循 X.509 标准。

安装 EsgynDB 后, 您能部署 CA 签名证书 (运行命令 `distcacert cosigned <pem file name>`), 再重启连接和管理服务 (运行命令 `dcstop`、`mgblyt_stop`、`dcstart` 和 `mgblyt_start`)。

公共 (`server.crt`) 和私人 (`server.key`) 文件都应存放在 `$HOME/sqcert` 中。

## 9.5 管理用户

如需更安全的 Hadoop 环境，安装 EsgynDB 时可启用 Kerberos。AD/LDAP 对任何连接至 EsgynDB 的用户实施强制验证。EsgynDB 支持数据库级、Schema 级、对象级（表、视图和其它等）和操作级权限。启用权限功能后，您能授予权限。如果启用了 AD/LDAP 或 Kerberos，权限功能也将自动启用。

如需查看验证功能和权限功能的状态，在 `sqlci` 中执行命令 `env`。



### 示例

```
>>env;
-----
Current Environment
-----
AUTHENTICATION      enabled
AUTHORIZATION       enabled
CURRENT DIRECTORY   /opt/trafodion/esgynDB-2.4.0
. . .
```

启用权限功能后，EsgynDB 将会创建预定义数据库用户 `DB__ROOT` 和 `DB__ADMIN`，这些用户与您指定的 AD/LDAP 用户名（在安装 EsgynDB 时设置）相关。请以用户 `DB__ROOT` 或 `DB__ADMIN` 身份登录 EsgynDB，创建所需的 Schema、用户、角色和权限<sup>5</sup>。

---

<sup>5</sup> 更多关于如何注册用户、向对象和组件授予权限、管理用户和角色的信息，请参阅《EsgynDB SQL 参考手册》。

## 10. 提高安全性

本章讲述如何提高 EsqynDB 安装过程的安全性。

### 10.1 提高 Linux 安全性

更多关于如何提高 Linux 安装过程的安全性，请参阅以下信息。

操作系统	版本	网址
RedHat Enterprise Linux	7.x	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux 7 安全指南 <a href="https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/index">https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/index</a></li> </ul>
RedHat Enterprise Linux	6.x	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux 6 安全指南 <a href="https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/index">https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/index</a></li> </ul>
CentOS	通用	<ul style="list-style-type: none"> <li>CentOS 安全指南 <a href="https://wiki.centos.org/HowTos/OS_Protection#head-f80d332aeea03f57d34d7a5c09493a7d69cce177">https://wiki.centos.org/HowTos/OS_Protection#head-f80d332aeea03f57d34d7a5c09493a7d69cce177</a></li> </ul>

### 10.2 提高 Hadoop 安全性

更多关于如何提高 Hadoop 安装过程的安全性，请参阅以下信息。

Hadoop 发行版	网址
Hortonworks' HDP 2.x	<ul style="list-style-type: none"> <li>Hadoop 安全指南 <a href="https://docs.hortonworks.com/HDPDocuments/HDP2/HDP-2.4.0/bk_Security_Guide/content/ch_hdp-security-guide-overview.html">https://docs.hortonworks.com/HDPDocuments/HDP2/HDP-2.4.0/bk_Security_Guide/content/ch_hdp-security-guide-overview.html</a></li> </ul>
Cloudera CDH 5.x	<ul style="list-style-type: none"> <li>CDH 5 安全指南 <a href="https://www.cloudera.com/documentation/cdh/5-0-x/CDH5-Security-Guide/CDH5-Security-Guide.html">https://www.cloudera.com/documentation/cdh/5-0-x/CDH5-Security-Guide/CDH5-Security-Guide.html</a></li> </ul>

### 10.3 提高 Jetty Server 安全性

EsgynDB 中大量组件使用 Jetty web 服务器模块为网页提供服务。Jetty web 服务器使用 HTTPS 和强 SSL 密码。

更多关于如何提高 Jetty 的安全性，请参阅以下信息。

- 配置 Jetty Connector

<http://www.eclipse.org/jetty/documentation/current/configuring-connectors.html>

- 配置 Jetty 安全性

<http://www.eclipse.org/jetty/documentation/current/configuring-security.html>

### 10.4 更新密码

将默认密码替换成安全性更高的密码。更多信息，请参阅 [5.4 用户 ID 和密码](#)。

### 10.5 提高端口安全性

以下端口需要对外部应用程序开放：

应用程序	端口号范围	说明
DCS Master	23400 ~ 23400+n n=MXOSRVR 的数量	开放端口号的范围取决于配置的 MXOSRVR 的数量
DB Manager	4206	

## 10.6 提高 AWS 安全性

本小节讲述如何提高在 AWS 上安装 EsgynDB 的安全性。

### 10.6.1 限制访问 Ambari 或 Cloudera Manager

确保 Hadoop 管理工具（例如，Amari 或 Cloudera Manager）仅能被定义的 IP 地址访问，即可能是使用您公司网络的客户端设备或其它设备。



示例

仅允许客户端 76.244.44.66 访问 Ambari。

The screenshot shows the AWS IAM console interface for a security group. At the top, there is a search bar with 'Group ID : sg-44412031' and an 'Add filter' button. Below this is a table listing security groups. The table has columns for Name, Group ID, Group Name, VPC ID, and Description. One group is listed: 'sg-44412031' with Group Name 'External access to HDP cluster', VPC ID 'vpc-43f5053b', and Description 'Access Ambari server from external network'. Below the table, the details for 'Security Group: sg-44412031' are shown. There are tabs for 'Description', 'Inbound', 'Outbound', and 'Tags'. The 'Inbound' tab is selected. An 'Edit' button is visible. Below the tabs is a table of inbound rules. The table has columns for Type, Protocol, Port Range, Source, and Description. One rule is listed: 'Custom TCP Rule' with Protocol 'TCP', Port Range '8080', Source '76.244.44.66/32', and Description 'Ambari'.

Name	Group ID	Group Name	VPC ID	Description
sg-44412031	sg-44412031	External access to HDP cluster	vpc-43f5053b	Access Ambari server from external network

Security Group: sg-44412031

Description Inbound Outbound Tags

Edit

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	8080	76.244.44.66/32	Ambari

## 10.6.2 限制访问 EsgynDB 组件

设置 AWS 安全规则，限制访问 DCS 子系统和 EsgynDB Manager。



仅允许客户端 76.244.44.66 访问 DCS 子系统和 EsgynDB Manager。

### Edit inbound rules ✕

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>	
Custom TCP <small>f</small> ▾	TCP	23400 - 23410	Custom ▾ 76.244.44.66/32	DcsMaster	✕
Custom TCP <small>f</small> ▾	TCP	4205 - 4206	Custom ▾ 76.244.44.66/32	DB Manager	✕

**Add Rule**

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

### 10.6.3 限制访问 EsgynDB 实例

EsgynDB 组件需要在实例内跨节点通信，但某些组件（例如，DCS Master 和 MXOSRVR 进程）需要被外部客户端访问，此时您可以设置相应规则。



示例

允许客户端 34.204.77.209/32 和 54.158.104.187/32 访问 DCS Master 和 MXOSRVR 进程。。

Description	Inbound	Outbound	Tags	
<b>Edit</b>				
Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>
All TCP	TCP	0 - 65535	172.31.0.0/16	
Custom TCP Rule	TCP	23400 - 23410	34.204.77.209/32	saturn001 external...
Custom TCP Rule	TCP	23400 - 23410	54.158.104.187/32	saturn002 external...

### 10.6.4 总结

下图总结了为 EsgynDB 集群设置的访问规则，该 EsgynDB 集群运行 Hortonworks HDP。以下端口和 IP 能访问该 EsgynDB 集群，其它 IP 无法访问该 EsgynDB 集群。

Security Groups associated with i-0066f6deaf70a008a						
Ports	Protocol	Source	SSH access	External access to HDP cluster	External access for EsgynDB	Internal subnet access
22	tcp	76.244.44.66/32	✓			
5901	tcp	76.244.44.66/32	✓			
8080	tcp	76.244.44.66/32		✓		
23400-23410	tcp	76.244.44.66/32			✓	
4205-4206	tcp	76.244.44.66/32			✓	
0-65535	tcp	172.31.0.0/16				✓
23400-23410	tcp	34.204.77.209/32, 54.158.104.187/32				✓

### 10.6.5 最后步骤

使用 AWS:

- 1、 创建弹性 IP。
- 2、 创建网络接口；检查**允许重新关联 (Allow Re-association)** 选项。
- 3、 关联弹性 IP 和网络接口。
- 4、 创建用户 ID，生成访问 key。
- 5、 创建规则，并对用户应用这些规则。

### 10.6.6 最佳实践

更多关于如何设置访问亚马逊 EC2 云的 IAM (Identity and Access Management, 身份识别与访问管理)、用户规则和角色，请参阅

<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>。

## 附录 1. 验证配置文件

默认情况下，EsgynDB 验证配置文件保存在

`$TRAF_HOME/sql/scripts/.traf_authentication_config` 中。

如需将该文件保存在其它位置或使用不同文件名，您可以使用环境变量指定备用位置/文件名。

以下列表为 `.traf_authentication_config` 中支持的属性及其说明。

属性名称	用途	示例值	注意
LDAPHostName	本地 LDAP 服务器的主机名	ldap.master.com	如果提供两个及以上的 LDAPHostName 值，EsgynDB 将尝试与每个 LDAP 服务器连接。 如果全部验证失败，系统将返回验证错误。 更多信息，请参阅 <a href="#">RetryCount</a> 和 <a href="#">RetryDelay</a> 。
LDAPPort	本地 LDAP 服务器的端口号	345	必须为数值。与 LDAPSSL 相关。  OpenLDAP 标准端口号： <ul style="list-style-type: none"> <li>• 非安全：389</li> <li>• SSL：636</li> <li>• TLS：389</li> </ul>
LDAPSearchDN	如需搜索用户，请指定搜索用户的区别名	cn=aaabbb, dc=demo, dc=net	如果本地服务器允许匿名搜索，则无需指定该属性

	(Distinguished Name)。		或指定该属性为空值。目前系统支持匿名搜索功能。
LDAPSearchPWD	LDAPSearchDN 的密码。 更多信息，请参阅 <a href="#">LDAPSearchDN</a> 。	welcome	无
LDAPSSL	指定本地 LDAP 服务器接口不加密或使用 TLS 或 SSL。 0 表示未加密，1 表示 SSL，2 表示 TLS。	0	无
UniqueIdentifier	包含用户唯一标识符的目录属性。	uid=,ou=Users,dc=demo, dc=net	考虑到给定 LDAP 服务器支持 DN 的多种形式，使用不同值多次指定 UniqueIdentifier 参数。查找过程中，每个 UniqueIdentifier 按照在配置文件中列出的顺序被使用。
LDAPNetworkTimeout	如果连接请求没有响应，指定下一个 LDAPHostName 的超时时间（单位：秒）。 该参数与 ldap_conf(5) 中的	20	该参数的值必须为正数或 -1，-1 表示无限超时。

	<p>NETWORK_TIMEOUT 类似。</p> <p>默认值为 30 秒。</p>		
LDAPTimelimit	<p>指定在 LDAP 服务器上执行用户名搜索的等待时间。</p> <p>该参数的值必须为正数。</p> <p>该参数与 ldap_conf(5) 中的 TIMELIMIT 类似。</p> <p>默认值为 30 秒。</p>	15	<p>在搜索过程中，服务器端可能使用比 LDAPTimelimit 更短的超时时间。</p>
LDAPTimeout	<p>指定在调用同步 LDAP API 后，未收到回应到终止调用之间的超时时间（单位：秒）。</p> <p>该参数与 ldap_conf(5) 中的 TIMEOUT 类似。默认值为 30 秒。</p>	15	<p>该参数的值必须为正数或 -1，-1 表示无限超时。</p>
RetryCount	<p>建立成功 LDAP 连接的尝试次数。</p> <p>默认值为 5。如果重试 5 次后全部失败，将返回错误。</p>	10	<p>重试失败操作时，EsgynDB 将尝试连接每个配置 LDAP 服务器，直到操作成功或超过允许的重试次数。</p>
RetryDelay	<p>指定重试之间延迟的时间。</p>	1	无

	<p>默认值为 2 秒。</p> <p>更多信息，请参阅 <a href="#">RetryCount</a>。</p>		
PreserveConnection	<p>操作完成后，指定 LDAP 服务器连接保留 (YES) 或关闭 (NO)。</p> <p>默认值为 NO。</p>	YES	无
RefreshTime	<p>指定重新读取配置文件之前必须等待的时间。</p> <p>默认值为 1800 秒 (30 分钟)。</p>	3600	<p>如果设置为零，则不会读取配置文件。</p> <p>如果该值为零，则必须重启服务器连接才能使更改生效。</p> <p>该属性不特定于任何配置，且必须在 DEFAULTS 组定义。</p>
TLS_CACERTFilename	<p>指定 LDAP 服务器证书文件的位置。文件名可以是绝对路径名或与 \$CACERTS_DIR 相关。</p>	cert.pem	<p>该属性适用于两种配置。</p> <p>如果一种配置无需证书，则忽略该属性。</p> <p>该属性必须在 DEFAULTS 组定义。</p>
DefaultSectionName	<p>如果未指定验证类型，则指定由 REGISTER USER 命令分配给用户的配置类型。</p> <p>初始 trafodion 版本仅支持一种配置。</p>	LOCAL	<p>如果指定了 DefaultSectionName 属性，则必须在 .traf_ldapconfig 中定义使用该名称 (或等效值) 的部分。</p>

			合法值为 LOCAL 和 ENTERPRISE。该语法可能会更改。
--	--	--	-----------------------------------

## 附录 2. Inspector 工具

安装前，EsgynDB Python Installer 将检查集群的状态，例如，检查和记录硬件、固件和软件的所有必要组件，以及所有子系统配置。

以下步骤为 EsgynDB Python Installer 调用预安装检查：

- 1、显示检查结果概览。

```
$ python-installer/inspector.py
```

- 2、显示所有检查结果。

```
$ python-installer/inspector.py --all
```

- 3、无密码 ssh 运行检查程序。

```
$ python-installer/inspector.py --all --enable-pwd
```

- 4、使用指定远程用户，在远程节点上无密码 ssh 运行检查程序。

```
$ python-installer/inspectors.py --all --enable-pwd --  
remote-user <user>
```

- 5、如果使用 --enable-pwd 参数，输入远程主机 ssh 密码。

```
Input remote host SSH Password:
```

- 6、调用检查程序脚本时，输入目标节点列表。

```
Enter list of Nodes separated by comma, support  
numeric RE, i.e. n[01-12]:
```

**注意**

- 如果未指定 `--remote-user` 选项，检查程序将使用目前登录用户作为远程用户。`--remote-user` 应在远程节点上具有 `root` 或 `sudo` 权限。
- 运行检查程序的节点需知晓目标节点的主机名和 IP 地址。
- 如需使用 `--enable-pwd` 参数，您需安装 `sshpas` 工具，安装命令为 `yum install -y sshpass`。

**示例**

```
[centos@esgvm-test python-installer]$ ./inspector.py
Enter list of Nodes separated by comma, support numeric
RE, i.e. n[01-12]: developer-[1-2]
```

```
TASK: Environment Discover
```

```
*****
*****
```

```
Time Cost: 0 hour(s) 0 minute(s) 8 second(s)
```

```
*****
```

```
Discover results
```

```
*****
```

```
Hosts:test-1,test-2
```

Overview	Stat	Expected
CPU architecture	o	-
CPU cores	w	4
Disk numbers	x	4
Free data File System spaces	x	1000GB
Free System spaces	x	200GB
Total memory size	x	64GB

Current free memory size	w	8GB
Swap/Mem percentage	x	25%
Network Card bandwidth	x	10Gbps
Linux distro	o	-
FQDN	o	-
Localhost setting in /etc/hosts	o	-
Ntp service status	x	-
Firewall status	o	-
Kernel pid max	o	-
Kernel tcp keep alive time	w	240
Kernel tcp keep alive interval	w	15
Kernel tcp keep alive probes	w	4
NFS on /home	o	-
Sudo access	o	-
NetworkManager service status	o	-
SSH PAM settings	o	-
Default java version	o	-
HBase version	o	-
HDFS version	o	-
Hive version	o	-
Leftover Trafodion process	o	-
license status	x	-
+-----+-----+		

## 附录 3. EsgynDB 在线增加节点

- 1、禁用 HBase 负载均衡功能。

在 HBase shell 中输入：

```
balance_switch false
```

- 2、在 HDP/CDH 中手动增加 HBase Regionserver 节点、HDFS Datanode 节点 Yarn/MapReduce 节点<sup>6</sup>。

- 3、增加 EsgynDB 节点。

在现有节点上输入：

```
[root@esgvm-test python-installer]# ./add_nodes.py --  
nodes=suyan20,suyan21,suyan22,  
suyan23,suyan24
```

### 输出

```
*****  
Trafodion Elastic Add Nodes script  
*****  
***[INFO]: Creating trafodion packages of  
/home/trafodion/  
esgynDB_server-2.4.0, this will take awhile ...  
***[INFO]: Copying trafodion files to new nodes, this  
will take a while ...  
*****  
AddNode sub scripts start  
*****  
***[INFO]: Running add node setup on new node(s)  
[suyan20,
```

---

<sup>6</sup>更多关于如何在 HDP/CDH 中增加这些节点，请参阅《如何在 Hadoop 和 Cloudera 集群增加节点》。

```
suyan21,suyan22,suyan23,suyan24] ...
TASK: Add nodes Setup
*****
TASK: Install Trafodion dependencies
*****
Time Cost: 0 hour(s) 2 minute(s) 26 second(s)
***[INFO]: Running dcs setup on all node(s)
[suyan02,suyan03,
suyan04,suyan05,suyan06,suyan07,suyan08,suyan17,suyan1
8,suyan19,suyan20,suyan21,suyan22,suyan23,suyan24] ...
TASK: DCS/REST Setup
*****
Time cost: 0 hour(s) 0 minute(s) 51 second(s)
***[INFO]: Trafodion instance is up, adding node in
sqshell ...
***[INFO]: Trafodion instance is up, adding node in
sqshell ...
***[INFO]: adding node [suyan20] in sqshell ...
***[OK]: Node [suyan20] added!
***[INFO]: adding node [suyan21] in sqshell ...
***[OK]: Node [suyan21] added!
***[INFO]: adding node [suyan22] in sqshell ...
***[OK]: Node [suyan22] added!
***[INFO]: adding node [suyan23] in sqshell ...
***[OK]: Node [suyan23] added!
***[INFO]: adding node [suyan24] in sqshell ...
***[OK]: Node [suyan24] added!
***[INFO]: starting DCS on new nodes ...
***[INFO]: Run sqregen ...
*****
AddNode complete
*****
```

## 4、检查 Trafodion 运行状况。

## 输入

```
sqcheck
```

## 输出

```
*** Checking Trafodion Environment ***
Checking if processes are up.
Checking attempt: 1; user specified max: 2. Execution
time in seconds: 0.
The Trafodion environment is up!
Process      Configured      Actual      Down
-----
DTM           23              23
RMS           46              46
DcsMaster     1               1
Dcsserver     23              23
mxosrvr      2254            2254
Restserver    1               1
```

## 5、检查每个节点的运行状况。

## 输入

```
sqshell -a
```

## 输出

```
[$Z000EJ2] Shell/shell Version 1.0.1 EsgynDB Release
2.4.0 (Build release [centos], date 09Nov17)
[$Z000EJ2] %node info
[$Z000EJ2] Logical Nodes      = 23
[$Z000EJ2] Physical Nodes     = 23
[$Z000EJ2] Spare Nodes        = 0
[$Z000EJ2] Available spares= 0
[$Z000EJ2] NID Type          State Processors      #Procs
```



[\$Z000EJ2]	016	Up	40	3712684	66914132
281733864 suyan18					
[\$Z000EJ2]	017	Any Up	2	106	
[\$Z000EJ2]	017	Up	40	2621536	66980652
280225512 suyan19					
[\$Z000EJ2]	018	Any Up	2	108	
[\$Z000EJ2]	018	Up	40	75295732	66950316
335096680 suyan20					
[\$Z000EJ2]	019	Any Up	2	108	
[\$Z000EJ2]	019	Up	40	35179380	67051084
306800276 suyan21					
[\$Z000EJ2]	020	Any Up	2	108	
[\$Z000EJ2]	020	Up	40	64271476	66985376
332396772 suyan22					
[\$Z000EJ2]	021	Any Up	2	108	
[\$Z000EJ2]	021	Up	40	53754092	67105416
312541096 suyan23					
[\$Z000EJ2]	022	Any Up	2	108	
[\$Z000EJ2]	022	Up	40	46462700	67097284
310962924 suyan24					

## 6、启用 HBase 负载均衡功能。

在 HBase shell 中输入：

```
balance_switch true
```

## 7、重启 HBase RegionServer。

在 Cloudera Manager 管理界面上，重启新增节点的 HBase RegionServer。



图 1 重启 HBase RegionServer

## 附录 4. EsgynDB 离线删除节点

- 1、停止数据库。

输入

```
sqstop
```

输出

```
Stopping DBMgr...
2017-11-16_12:36:51: Stopping EsgynDB Manager pid
(32532)
2017-11-16_12:36:54: stopped EsgynDB Manager
Stopping Bosun...
2017-11-16_12:36:59: Bosun process is not started
SQ shutdown (normal) from
/home/trafodion/esgynDB_server-2.4.0/sql/scripts
successful
```

- 2、检查 Trafodion 运行状况。

输入

```
sqcheck
```

输出

```
[trafodion@esgvm-test scripts]$ sqcheck
*** Checking Trafodion Environment ***
Checking if processes are up.
Checking attempt: 1; user specified max: 2. Execution
time in seconds: 4.
The Trafodion environment is not up at all, or
partially up and not operational. Check the logs.
Process          Configured      Actual         Down
-----
DTM              0               0
```

```
RMS          0          0
DcsMaster    1          0          1
Dcsserver    23         0          23
mxosrvr      2254        0          2254
Restserver   0          0
The Trafodion environment is down.
```

3、修改 servers 文件。

输入

```
pwd
```

输出

```
/home/trafodion/esgynDB_server-2.4.0/dcs-2.4.0/conf
```

输入

```
cat servers
```

输出

```
suyan02 98
suyan03 98
suyan04 98
suyan05 98
suyan06 98
suyan07 98
suyan08 98
suyan09 98
suyan10 98
suyan11 98
suyan12 98
suyan13 98
suyan14 98
suyan15 98
```

```
suyan16 98  
suyan17 98  
suyan18 98  
suvan19 98
```

- 4、将 servers 文件复制至 \$MY\_NODES（所有节点）的当前目录。

输入

```
pdcp $MY_NODES servers $PWD/
```

- 5、修改 sqconfig 文件，删除待删除节点的信息。

输入

```
pwd
```

输出

```
/home/trafodion/esgynDB_server-2.4.0/sql/scripts
```

输入

```
vi sqconfig
```

输出

```
node-id=0;node-name-suyan02;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=1;node-name-suyan03;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=2;node-name-suyan04;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=3;node-name-suyan05;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=4;node-name-suyan06;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=5;node-name-suyan07;cores=0-
```

```
39;processors=2;roles=connection,aggregation,storage
node-id=6;node-name-suyan08;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=7;node-name-suyan09;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=8;node-name-suyan10;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=9;node-name-suyan11;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=10;node-name-suyan12;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=11;node-name-suyan13;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=12;node-name-suyan14;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=13;node-name-suyan15;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=14;node-name-suyan16;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=15;node-name-suyan17;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=16;node-name-suyan18;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=17;node-name-suyan19;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=18;node-name-suyan20;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=19;node-name-suyan21;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=20;node-name-suyan22;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=21;node-name-suyan23;cores=0-
39;processors=2;roles=connection,aggregation,storage
node-id=22;node-name-suyan24;cores=0-
```

```
39;processors=2;roles=connection,aggregation,storage
```

删除待删除节点的信息后，sqconfig 文件为：

```
node-id=0;node-name-suyan02;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=1;node-name-suyan03;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=2;node-name-suyan04;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=3;node-name-suyan05;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=4;node-name-suyan06;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=5;node-name-suyan07;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=6;node-name-suyan08;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=7;node-name-suyan09;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=8;node-name-suyan10;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=9;node-name-suyan11;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=10;node-name-suyan12;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=11;node-name-suyan13;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=12;node-name-suyan14;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=13;node-name-suyan15;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=14;node-name-suyan16;cores=0-  
39;processors=2;roles=connection,aggregation,storage
```

```
node-id=15;node-name-suyan17;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=16;node-name-suyan18;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=17;node-name-suyan19;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=18;node-name-suyan20;cores=0-  
39;processors=2;roles=connection,aggregation,storage  
node-id=19;node-name-suyan21;cores=0-  
39;processors=2;roles=connection,aggregation,storage
```

- 6、备份 sqconfig.db 文件。

输入

```
mv sqconfig.db sqconfig.db.bak
```

- 7、生成启动脚本和配置数据库。

输入

```
sqgen
```

输出

```
Checking for the configuration file (sqconfig.db).  
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08  
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1  
5,suyan16,suyan17,suyan18,suyan19  
  
Creating directories on cluster nodes  
/usr/bin/pdsh -R exec -w  
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08  
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1  
5,suyan16,suyan17,suyan18,suyan19 -x suyan02 ssh -q -  
n %h mkdir -p /home/trafodion/esgynDB_server-2.4.0/etc  
/usr/bin/pdsh -R exec -w
```

```
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08  
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1  
5,suyan16,suyan17,suyan18,suyan19 -x suyan02 ssh -q -  
n %h mkdir -p /home/trafodion/esgynDB_server-2.4.0/logs  
/usr/bin/pdsh -R exec -w
```

```
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08  
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1  
5,suyan16,suyan17,suyan18,suyan19 -x suyan02 ssh -q -  
n %h mkdir -p /home/trafodion/esgynDB_server-2.4.0/tem  
/usr/bin/pdsh -R exec -w
```

```
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08  
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1  
5,suyan16,suyan17,suyan18,suyan19 -x suyan02 ssh -q -  
n %h mkdir -p /home/trafodion/esgynDB_server-  
2.4.0/sql/scripts
```

The SQ environment variable file

/home/trafodion/esgynDB\_server-2.4.0/etc/ms.env exists.

The file will not be re-generated.

Copying the generated files to all the nodes in the  
cluster

Copying /home/trafodion/esgynDB\_server-2.4.0/etc/ms.env  
to /home/trafodion/esgynDB\_server-2.4.0/etc of all the  
nodes

```
/usr/bin/pdcp -R ssh -w suyan02, suyan03, suyan04,  
suyan05, suyan06, suyan07, suyan08, suyan09, suyan10,  
suyan11, suyan12, suyan13, suyan14, suyan15, suyan16,  
suyan17, suyan18, suyan19| -x suyan02
```

/home/trafodion/esgynDB\_server-2.4.0/etc/ms.env

/home/trafodion/esgynDB\_server-2.4.0/etc

Copying /home/trafodion/esgynDB\_server-

```

2.4.0/etc/seamonster.env to
/home/trafodion/esgynDB_server-2.4.0/etc of all the
nodes
/usr/bin/pdcp -R ssh -w
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1
5,suyan16,suyan17,suyan18,suyan19 -x suyan02
/home/trafodion/esgynDB_server-2.4.0/etc/ms,env
/home/trafodion/esgynDB_server-2.4.0/etc
Copying /home/trafodion/esgynDB_server-
2.4.0/etc/seamonster.env to
/home/trafodion/esgynDB_server-2.4.0/etc of all the
nodes
/usr/bin/pdcp -R ssh -w
suyan02,suyan03,suyan04,suyan05,suyan06,suyan07,suyan08
,suyan09,suyan10,suyan11,suyan12,suyan13,suyan14,suyan1
5,suyan16,suyan17,suyan18,suyan19 -x suyan02
/home/trafodion/esgynDB_server-2.4.0/etc/seamonster.env
/home/trafodion/esgynDB_server-2.4.0/etc
pdcp@suyan02: can't stat
/home/trafodion/esgynDB_server-2.4.0/etc/seamonster.env

```

#### 8、验证环境变量 MY\_NODES 是否正确。

输入以下命令后将返回集群中节点的信息，此时，应不包含被删除的节点，否则，需重新登录验证环境变量是否正确。

输入

```

su - trafodion
echo $MY_NODES

```

#### 9、启动 Trafodion。

输入

```

sqstart

```

**输出**

```

Checking if processes are up.
Checking attempt: 1; user specified max: 2. Execution
time in seconds: 0.

The Trafodion environment is up!

Process      Configured      Actual      Down
-----
DTM          18              18
RMS          36              36
DcsMaster    1               1
Dcsserver    18              18
mxosrvr      1764            1226       538
Restserver   1               1

Startup time 0 hour(s) 7 minute(s) 57 second(s)
    
```

10、检查 Trafodion 运行状况。

**输入**

```
sqcheck
```

**输出**

```

*** Checking Trafodion Environment ***

Checking if processes are up.
Checking attempt: 1; user specified max: 2. Execution
time in seconds: 1.

The Trafodion environment is up!

Process      Configured      Actual      Down
    
```

-----		
DTM	18	18
RMS	36	36
DcsMaster	1	1
Dcsserver	18	18
mxosrvr	1764	1764
Restserver	1	1

## 附录 5. 安装后配置 DCS Master 的 HA

### 1、配置服务端文件。

(1) 复制以下内容至 DCS\_INSTALL\_DIR/conf/dcs-site.xml 文件。

```
<property>
  <name>dcs.zookeeper.property.clientPort</name>
  <value>2181</value>
</property>
<property>
  <name>dcs.zookeeper.quorum</name>
  <value>gy08.esgyncn.local,gy07.esgyncn.local,gy09.esgyncn.local</value>
</property>
<property>
  <name>dcs.dns.interface</name>
  <value>eth1</value>
</property>
<property>
  <name>dcs.master.floating.ip</name>
  <value>>true</value>
</property>
<property>
  <name>dcs.master.floating.ip.external.interface</name>
  <value>eth1</value>
</property>
<property>
  <name>dcs.master.floating.ip.external.ip.address</name>
  <value>10.10.12.252</value>
</property>
```

(2) 复制以下内容至 DCS\_INSTALL\_DIR/conf/master 文件。

```
gy09.esgyncn.local
```

(3) 复制以下内容至 DCS\_INSTALL\_DIR/conf/backup-masters 文件。

```
gy07.esgyncn.local  
gy10.esgyncn.local
```

(4) 复制以下内容至 vi /home/trafodion/.bashrc 文件。

```
export ENABLE_HA=true  
then have to re-login all terminates
```

(5) 复制以下内容至 MY\_SQLROOT/dbmgr-2.4.0/conf/config.xml 文件。

```
jdbc:t4jdbc://suyan02:23400/:
```

## 2、配置客户端。

在客户端的 Connection String 中指定浮动 IP (10.10.12.252:23400)，而不能 DCS 节点的 IP。

## 3、配置操作系统。

复制以下内容至/etc/sudoers.d/trafodion。

```
## Trafodion Floating IP commands  
Cmnd_Alias IP = /sbin/ip  
Cmnd_Alias ARP = /sbin/arping  
  
## Allow Trafodion id to run commands needed to configure  
floating IP  
%trafodion ALL = NOPASSWD: IP,ARP
```

```
## Allow trafodion id to run commands needed for backup  
and restore  
%trafodion ALL =(hbase) NOPASSWD: /usr/bin/hbase
```

4、重新启动 DCD Master。

输入

```
dcstop  
dcstart  
dcscheck
```

## 附录 6. 在安装 EsgynDB 之后配置 LDAP

### 1、安装 IPA-server。

#### 输入

```
yum install ntp
yum install krb5-server krb5-server-ldap
yum install 389-ds-base
yum install bind bind-dyndb-ldap
yum install httpd tomcat6
yum install ipa-server
```



#### 提示

如需管理 IPA-server，请参阅以下信息：

- 添加新用户

```
ipa user-add user01 --first=user01 --last=user01 -passwd
```

- 重置密码

```
kinit admin
ipa user-mod user01 --password
```

- 用户密码失败后解锁

```
kinit admin
ipa user-unlock user01
```

- 删除用户

```
ipa user-del user01
```

- 禁用用户

```
ipa user-disable user01
```

- 启用用户

```
ipa user-enable user01
```

- 添加组

```
ipa group-add sale --desc="sales team"
```

- 添加用户

```
ipa group-add-member group01 --  
users=user01,user02,user03
```

- 删除用户

```
ipa group-remove-member group01 --users=user01
```

- 删除组

```
ipa group-del sale
```

- 查看用户和组

```
ipa user-show -all  
ipa group-show --all
```

- 启动和停止 IPA

```
ipactl stop  
ipactl start
```

## 2、停止 EsgynDB 实例。

### 输入

```
sqstop  
sqcheck
```

### 3、配置 LDAP。

以 sudo 用户或 root 用户身份，在已安装 EsgynDB 的节点上执行以下脚本，并根据提示输入 LDAP 相应的参数：

```
[root@esgvm-test python-installer]# ./secure_setup.py
*****
Trafodion Security Setup Script
*****

TASK: Environment Discover
*****

Time Cost: 0 hour(s) 0 minute(s) 6 second(s)

**[INFO]: Kerberos is not enabled in Hadoop, skipped
Enable LDAP security (Y/N) [N]: Y
Enter LDAP user name to be assigned DB root privileges
(DB__ROOT) [trafodion]:
Enter LDAP user name to be assigned DB Admin privileges
[qaadmin]: qaadmin
Enter list of LDAP Hostnames (comma separated if more
than one host): 10.10.10.3
Enter LDAP Port number (Example: 389 for no encryption or
TLS, 636 for SSL) [389]:
Enter all LDAP unique identifiers (semi-colon separated
if more than one identifier):
uid=,cn=users,cn=accounts,dc=esgyncn,dc=local
Enter LDAP Encryption Level (0: Encryption not used, 1:
SSL, 2: TLS) [0]:
Does the LDAP server require search user name/password
(Y/N) (optional) [N]:
Does the LDAP server support group searches (Y/N)
(optional) [N]:
```

```
***[INFO]: Running LDAP setup on all node(s) [esggy-qa-  
n014.esgyncn.local,esggy-qa-n015.esgyncn.local] ...
```

```
TASK: Deploy Client Configurations
```

```
*****
```

```
Time Cost: 0 hour(s) 0 minute(s) 2 second(s)
```

```
***[INFO]: Trafodion is running or partially running.
```

```
***[INFO]: Init authorization
```

```
***[INFO]: Restarting DCS to take effect...
```

```
*****
```

```
Security Setup Completed
```

```
*****
```

#### 4、启动 EsgynDB。

输入

```
sqstart
```

#### 5、注册用户。

在 sqlci 中输入

```
register user traf1;
```

#### 6、用户登录。

在 trafci 中登录，用户名为 traf1，密码之前已设置过。

## 附录 7. 安装后配置 Kerberos 认证

如果在安装前 Hadoop 已经启用了 Kerberos 认证功能，则安装程序会自动进行 EsgynDB 的 Kerberos 相关配置。

如果在安装 EsgynDB 之后才开启了 Hadoop 的 Kerberos 认证功能，则可以通过 `secure_setup.py` 脚本进行 EsgynDB 部分的配置。在配置之前，需要事先获取以下信息：

### 1、前期确认。

- (1) 确认 CDH 是否安装了 Kerberos 组件，在 Cloudera Manager 界面中依次选择 **管理 > 安全**，查看是否存在以下信息：



图 2 确认 CDH 是否安装了 Kerberos 组件

- (2) 确认 KDC server address。在 Cloudera Manager 界面中依次选择**管理 > 安全 > Kerberos**，查看以下信息：

<b>KDC 类型</b>	<input checked="" type="radio"/> MIT KDC <input type="radio"/> Active Directory
<b>Active Directory 后缀</b>	ou=hadoop,DC=hadoop,DC=com
<b>Active Directory Delete Accounts on Credential Regeneration</b>	<input type="checkbox"/>
<b>Active Directory Set Encryption Types</b>	<input type="checkbox"/>
<b>Active Directory Password Properties</b>	length=12,minLowerCaseLetters=2,minUpperCaseLetters=2,minDigits=2,minSpaces=0,minSpecialChars=0,s
<b>Active Directory Account Properties</b>	accountExpires=0,objectClass=top,objectClass=person,objectClass=organizationalPerson,objectClass=user
<b>KDC Server 主机</b> kdc	
<b>Active Directory LDAPS 端口</b>	636
<b>Kerberos 安全领域</b> default_realm	HADOOP.COM

图 3 确认 KDC server address

- (3) 确认 admin principal（包括 realm）。

#### 输入

```
[root@hadoop05 krb5kdc]# cat
/var/kerberos/krb5kdc/kadm5.acl
```

#### 输出

```
*/admin@PUNEETHA.COM *
cloudera-scm@PUNEETHA.COM admilc
```

(4) 确认 HDFS 用户已经完成 Kerberos 授权，您可以使用以下任一方式：

- 执行命令 `hbase shell` 后是否能正常 list 出 table 对象
- 执行命令 `hadoop fs -ls /` 后是否能正常显示文件目录

如果没有完成授权，以上操作都会报 java 错误信息：Mechanism level:  
Failed to find any Kerberos tgt。

授权方式：kinit hdfs 然后输入密码即可（密码通过安装 Kerberos 的人员获取）

2、启用 EsgynDB 的 Kerberos 支持。

以 sudo 用户或 root 用户身份，在已安装 EsgynDB 的节点上执行 `./secure_setup.py` 命令，该脚本会自动检测 Hadoop 的 Kerberos 是否开启。如果开启，将会提示输入 KDC admin principal 等信息，并根据提示输入即可开启 Kerberos 支持。