

# UniCloud BDP 大数据平台

## 安装部署手册

紫光云技术有限公司  
[www.unicloud.com](http://www.unicloud.com)

资料版本：5W100-20220809  
产品版本：UniCloud BDP (E6102)

© 紫光云技术有限公司 2022 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光云保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光云尽全力在本手册中提供准确的信息，但是紫光云并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

# 前言

本手册主要介绍了 UniCloud BDP 大数据平台的产品概述、部署前说明、安装管理系统和创建大数据集群的操作指导、License 配置、安装后检查与配置、卸载以及部署相关的常见问题解答等内容。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

## 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员






## 本书约定

### 1. 图形界面格式约定

格式	意义
<>	带尖括号“<>”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

### 2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

### 3. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

## 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

**E-mail: [unicloud-ts@unicloud.com](mailto:unicloud-ts@unicloud.com)**

感谢您的反馈，让我们做得更好！

# 目 录

<b>1 产品概述</b> .....	<b>1-1</b>
1.1 产生背景.....	1-1
1.2 架构.....	1-1
1.3 相关概念.....	1-2
1.4 应用场景.....	1-3
<b>2 部署前说明</b> .....	<b>2-1</b>
2.1 版本说明.....	2-1
2.2 大数据平台软件包.....	2-1
2.3 大数据平台安装规划.....	2-1
2.3.1 主机节点类型.....	2-1
2.3.2 主机使用规划.....	2-3
2.4 操作系统要求.....	2-5
2.5 网络要求.....	2-6
2.6 浏览器要求.....	2-6
2.7 部署流程.....	2-7
<b>3 安装大数据平台管理系统</b> .....	<b>3-1</b>
3.1 安装前必读.....	3-1
3.2 安装前规划内容.....	3-1
3.3 管理节点主机配置要求.....	3-2
3.3.1 主机硬件要求.....	3-2
3.3.2 磁盘目录规划.....	3-3
3.3.3 安装操作系统.....	3-3
3.4 安装过程.....	3-4
3.4.1 修改时区及时间.....	3-4
3.4.2 安装管理系统.....	3-4
3.4.3 检查安装结果.....	3-9
<b>4 创建大数据集群</b> .....	<b>4-1</b>
4.1 创建前必读.....	4-1
4.2 创建前规划内容.....	4-1
4.2.1 系统内置的组件部署规则.....	4-2
4.3 大数据集群主机配置要求.....	4-2
4.3.1 主机硬件要求.....	4-2

4.3.2	磁盘目录规划 .....	4-5
4.3.3	安装操作系统 .....	4-5
4.3.4	磁盘 RAID 方案 .....	4-6
4.3.5	数据盘规划 .....	4-7
4.4	新建集群前准备 .....	4-8
4.4.1	新增主机 .....	4-8
4.4.2	新增虚拟 IP .....	4-10
4.5	新建集群 .....	4-11
4.5.1	新建 Hadoop 集群 .....	4-12
4.5.2	新建 Elasticsearch 集群 .....	4-20
4.5.3	新建 Solr 集群 .....	4-23
4.5.4	新建 Kafka 集群 .....	4-26
4.5.5	新建 Redis 集群 .....	4-29
<b>5</b>	<b>大数据平台相关配置 .....</b>	<b>5-1</b>
5.1	软件授权 .....	5-1
5.1.1	License 远程授权操作 .....	5-1
5.1.2	配置大数据集群的 License .....	5-1
5.2	添加浏览器安全证书 .....	5-1
<b>6</b>	<b>集群创建后检查 .....</b>	<b>6-1</b>
6.1	集群巡检 .....	6-1
6.2	检查主机 .....	6-2
6.2.1	主机运行状态检查 .....	6-2
6.2.2	主机健康检查 .....	6-3
6.3	检查组件 .....	6-4
6.3.1	组件存储路径检查 .....	6-4
6.3.2	组件运行状态检查 .....	6-4
6.3.3	组件检查 .....	6-5
<b>7</b>	<b>关于集群配置的说明 .....</b>	<b>7-1</b>
7.1	访问管理 .....	7-1
7.2	禁用/启用 root 权限 .....	7-1
7.3	配置组件快速链接 .....	7-2
7.4	日志管理 .....	7-2
7.5	安全管理 .....	7-3
7.5.1	开启 Kerberos .....	7-3
7.5.2	开启审计日志 .....	7-4
7.5.3	开启权限和密钥管理 .....	7-4

7.6 租户管理 .....	7-7
<b>8 卸载 .....</b>	<b>8-1</b>
8.1 卸载大数据集群 .....	8-1
8.1.1 删除集群 .....	8-1
8.1.2 删除组件 .....	8-2
8.1.3 删除进程 .....	8-3
8.2 卸载数据工厂 .....	8-5
8.3 卸载大数据平台管理系统 .....	8-5
<b>9 常见问题解答 .....</b>	<b>9-1</b>

# 1 产品概述

## 1.1 产生背景

随着 DT 时代的到来，企业数据规模不断增长，数据类型也变得复杂多样，传统数据库技术已无法满足企业海量多样化数据的有效存储、快速读取以及分析挖掘的需求，急需一套专业化的大数据解决方案来点石成金，大数据平台在此背景下应运而生。

大数据平台深度定制 Hadoop 生态系统，提供向导式的快速部署能力、方便易用的监控告警能力以及多层次高可靠的数据安全能力，是全链路的数据接入、存储、计算、分析、管理与开发的新一代大数据平台，助力企业业务快速创新，完成 ICT 转型。

## 1.2 架构

大数据平台架构如[图 1-1](#)所示，说明如下：

- **系统管理**：提供大数据平台运行支撑能力，包括统一用户管理、流程管理、操作日志、软件授权、系统升级等。大数据平台服务支持部署在物理机、虚拟机，用户可以根据实际业务场景需求灵活选择。
- **大数据集群**：提供丰富的大数据组件即服务，包括但不限于分布式文件系统、NoSQL 数据库服务、内存数据库服务、离线计算、流式计算、内存计算、SQL on Hadoop 等服务，同时还提供自研统一 SQL 服务，可兼容标准 SQL，对外提供统一的数据查询/分析服务，提升平台的整体易用性。
- **管理中心**：提供可视化安装部署、监控告警、主机扩容、大数据组件、日志统一等管理能力，大幅提升大数据平台运维效率。
- **安全中心**：提供基于 Kerberos 安全认证体系以及基于角色的用户权限管理体系。对用户身份进行认证，拒绝非法用户访问，恶意用户“进不来”；对用户操作行为进行不同维度的审计，非法用户“逃不掉”；通过角色绑定对用户授予访问不同组件数据的权限，数据“拿不走”；将密钥的权限与用户绑定，对数据进行透明加密，数据“看不懂”。
- **数据工厂**：提供一站式可视化的数据开发环境，全托管的数据处理流程调度，实现一整套完整的数据集成、数据表及文件管理、数据处理脚本程序开发、拖拽式工作流及调度、作业状态监控运维等全生命周期数据开发服务。



图1-1 大数据平台架构图



## 1.3 相关概念

表1-1 大数据平台相关术语

术语		说明
集群		通过大数据平台管理系统部署/管理的大数据集群，提供分布式存储计算能力
集群模式	独立模式	每个租户独立使用一套集群，网络和资源互相隔离
	租户模式	多个租户之间共享一套集群，共享网络和集群资源，但每个租户仅可访问自己对应的资源（资源严格隔离）
集群部署模式	非融合部署	大数据集群与管理系统分开部署，即部署大数据集群时完全不使用部署管理系统的主机节点
	融合部署	大数据集群与管理系统混合部署，即部署大数据集群时同时使用部署管理系统的主机节点
集群存储类型	HDFS	存储类型选择HDFS时，表示将HDFS数据存储于HDFS组件的DataNode中，即属于存储和计算未分离情况
组件		大数据集群中的应用组件，对外提供某种业务功能，例如：HDFS、YARN、Spark等
进程		进程是组件的组成部分，每个组件由一个或多个进程组成，例如：HDFS的NameNode或DataNode等
节点实例		大数据组件中的不同进程部署在不同节点上，将节点划分为不同的实例

术语	说明
专有节点实例	专门用来部署某个组件的节点称为专有节点实例 【说明】根据实际需求，此节点上也可选择部署其他组件
租户	从租户集群中申请存储、计算等组件资源，租户之间通过权限进行隔离
密钥	通过密钥可以存储和操作加密数据
密钥授权	用户经过指定密钥的授权之后，才可以访问通过该密钥加密的数据

## 1.4 应用场景

- 多数据源的快速接入：**通过简易的工作流管理界面，可轻松将存储在文件、关系型数据库、实时数据流（如设备 **syslog** 信息）等各类数据源中的海量结构化数据、非结构化数据、半结构化数据采集至大数据平台中。
- 海量数据的存储：**对结构化、半结构化和非结构化数据提供低成本存储，通过先进的 **Ensure Code** 技术实现数据低冗余、高容错，并通过集群高可用和多副本机制，避免单节点故障，保证节点损坏时数据不丢失。此外平台还具有高可扩展性，用户可以增加集群节点数量，横向扩展数据存储和计算能力。
- 多计算框架融合：**融合了稳定的离线计算 **MapReduce**、高效的内存计算 **Spark** 以及实时的流计算 **Flink** 等多种计算框架，为客户提供灵活的计算支持能力，全面支持各类计算业务场景，客户无需切换平台或架构即可完成复杂多变的计算任务。在各类计算框架之上，大数据平台通过统一 **SQL** 引擎，高度兼容标准 **SQL**，智能选择计算引擎，极大降低使用复杂度，为上层应用程序提供标准的 **JDBC/ODBC/REST** 接口、多种语言的编程 **API** 和 **DaaS** 接口，辅以 **BI** 展示和可视化工具，通过即时报表、直方图、柱状图等方式直观呈现数据价值。
- 丰富的行业应用：**大数据平台经过不断的产品优化和架构演进，已经成功在医疗、电力、税务、高校等多个行业落地实施，配合行业先进的应用服务开发商为客户提供丰富的大数据应用。

## 2 部署前说明

### 2.1 版本说明

大数据集群在大数据平台管理系统中直接创建。此时，大数据集群的主机资源直接使用独立的物理服务器资源，在大数据平台管理系统中可直接新增和管理主机资源。

部署大数据平台时，包括[安装大数据平台管理系统](#)和[创建大数据集群](#)两个步骤，并且有严格的部署顺序，请按照本文档执行部署操作。

### 2.2 大数据平台软件包

部署大数据平台时，需要准备的软件如[表 2-1](#)所示。

表2-1 软件列表

软件	软件包名称	用途说明	获取方式
UniCloud BDP大数据平台	BDP-<version>.tar.gz	用于安装大数据平台管理系统、大数据集群依赖YUM源、数据工厂（选装）	由紫光云提供



说明

安装大数据平台管理系统时可以选择是否同时安装数据工厂（缺省不安装），大数据平台管理系统安装完成之后数据工厂也可以进行单独的安装或卸载。

### 2.3 大数据平台安装规划

#### 2.3.1 主机节点类型

部署大数据平台时，包括安装大数据平台管理系统和创建大数据集群两个步骤，其中安装大数据平台管理系统需要 2 个主机节点（称为管理节点），创建大数据集群需要至少 3 个主机节点（称为集群节点），不同节点类型的详细说明如[表 2-2](#)所示。

表2-2 主机节点类型说明

主机类型	数量	说明
管理节点	2	通过BDP软件包安装大数据平台的管理系统，安装管理系统的节点即为管理节点 <b>【说明】</b> 管理系统提供大数据平台统一的访问入口，在管理系统中可执行创建集群的操作，同时支持对平台中的集群、主机、告警、日志等进行集中管理。

主机类型	数量	说明
集群节点	≥3	<p>对于Hadoop集群，集群节点类型为：</p> <ul style="list-style-type: none"> <li>• <b>Master 节点</b>：即大数据集群的主节点，控制和监控在 <b>Core</b> 节点上执行存储数据、接收数据等过程的状态。  <b>【说明】</b> 若不开启高可用则 <b>Master</b> 节点需要配置 1 个节点，若开启高可用则 <b>Master</b> 节点需要配置 2 个节点</li> <li>• <b>Core 节点</b>：即大数据集群的工作节点，用于存储数据或运行计算作业等。  <b>【说明】</b> 若不开启高可用则 <b>Core</b> 节点至少配置 2 个节点，若开启高可用则 <b>Core</b> 节点至少配置 1 个节点</li> </ul>
		<p>对于Elasticsearch集群，集群节点类型为：</p> <ul style="list-style-type: none"> <li>• <b>专有 Master 实例（可选）</b>：用于处理数据读写请求的实例，大数据量时可分担 <b>Data</b> 实例的工作负载。  <b>【说明】</b> <ul style="list-style-type: none"> <li>○ 若 <b>Elasticsearch</b> 集群开启专有 <b>Master</b> 实例则节点个数只能为奇数，且至少配置 3 个节点。</li> <li>○ 推荐集群规模在大于等于 10 节点时开启该功能，当集群节点数为 10-49 时建议配置 3 个 <b>Master</b> 实例节点，当集群节点数为 50-100 时建议配置 5 个 <b>Master</b> 实例节点。</li> </ul> </li> <li>• <b>Data 实例（必选）</b>：用来存储数据的实例。当集群中不配置专有 <b>Master</b> 实例时，<b>Data</b> 实例同时承担数据读写请求。  <b>【说明】</b> 至少配置 3 个节点。当集群中不配置专有 <b>Master</b> 实例和 <b>Client</b> 实例时，<b>Data</b> 实例的节点个数只能为奇数。</li> <li>• <b>Client 实例（可选）</b>：用于对读写请求进行负载均衡的实例。  <b>【说明】</b> 推荐集群规模在大于等于 50 节点时开启该功能，且至少配置 1 个节点。</li> </ul>
		<p>对于Solr集群，集群节点类型为：</p> <ul style="list-style-type: none"> <li>• <b>Solr 实例</b>：用于存储数据及处理读写请求的实例。  <b>【说明】</b> 至少配置 3 个节点。</li> </ul>
		<p>对于Kafka集群，集群节点类型为：</p> <ul style="list-style-type: none"> <li>• <b>kafka 实例</b>：用于存储数据及处理生产和消费请求的实例。  <b>【说明】</b> 至少配置 3 个节点。</li> </ul>
		<p>对于Redis集群，节点类型为：</p> <ul style="list-style-type: none"> <li>• <b>Redis 实例</b>：用于存储数据及处理读写请求的实例。  <b>【说明】</b> <b>Redis</b> 支持单机模式和集群模式，其中： <ul style="list-style-type: none"> <li>○ 单机模式仅包含 1 个节点，且一旦创建不可横向扩容。</li> </ul> </li> </ul>

主机类型	数量	说明
		<ul style="list-style-type: none"> <li>集群模式下，至少配置 3 个节点，且节点数量必须为奇数个。</li> </ul>

### 2.3.2 主机使用规划

根据现场主机节点数目，可决定大数据平台管理系统和大数据集群是否部署在相同节点上。

- 若大数据平台管理系统和大数据集群不部署在相同节点上  
部署大数据平台管理系统的节点与部署大数据集群的节点不存在任何关系。
- 若大数据平台管理系统和大数据集群部署在相同节点上  
大数据平台支持创建的集群类型包括 Hadoop、Elasticsearch、Solr、Kafka、Redis 集群，不同节点数量下，不同集群类型的节点复用策略不同，详情请参见[表 2-3](#)、[表 2-4](#)和[表 2-5](#)。



注意

- 当大数据平台管理系统和大数据集群部署在相同节点上，复用节点的硬件要求和磁盘目录规划等必须同时符合不同节点类型的要求（如：节点内存必须  $\geq 256\text{GB}$ ），详情请参见[3.3](#)和[4.3](#)章节。
- 大数据平台中支持部署多套大数据集群，部署大数据平台管理系统的管理节点建议仅同时被一套大数据集群复用。

表2-3 Hadoop 集群主机复用管理节点时

节点数量	主机节点	节点部署规划	说明
3节点	主机1	管理节点-1	<ul style="list-style-type: none"> <li>两个管理节点作为集群的 Master 节点</li> <li>此时集群的 Master 节点缺省同时作为 Core 节点</li> </ul>
		Master节点-1（同时当做Core节点-1使用）	
	主机2	管理节点-2	
		Master节点-2（同时当做Core节点-2使用）	
主机3	Core节点-3		
4节点	主机1	管理节点-1	<ul style="list-style-type: none"> <li>为确保大数据集群稳定性，管理节点全部作为集群的 Core 节点，管理节点不与 Master 节点混合部署</li> <li>集群的 Master 节点缺省同时作为 Core 节点</li> </ul>
		Core节点-1	
	主机2	管理节点-2	
		Core节点-2	
主机3	Master节点-1（同时当做Core节点-3使用）		
主机4	Master节点-2（同时当做Core节点-4使用）		
5节点及5节点	主机1	管理节点-1	<ul style="list-style-type: none"> <li>两个管理节点作为集群的</li> </ul>

节点数量	主机节点	节点部署规划	说明
以上		Master节点-1	Master 节点 <ul style="list-style-type: none"> <li>Master 节点和 Core 节点分开部署,避免大数据集群工作负载高时资源竞争</li> </ul>
	主机2	管理节点-2	
		Master节点-2	
	主机3	Core节点-1	
	主机4	Core节点-2	
	主机5	Core节点-3	
	主机N	Core节点-N	

表2-4 Elasticsearch 集群主机复用管理节点时

节点数量	主机节点	节点部署规划	说明
3~9节点	主机1	管理节点-1	两个管理节点作为集群的Data实例节点
		Data实例-1	
	主机2	管理节点-2	
		Data实例-2	
	主机3	Data实例-3	
主机N	Data实例-N		
10~49节点	主机1	管理节点-1	两个管理节点均作为集群的专有Master实例节点的前两个节点
		专有Master实例-1	
	主机2	管理节点-2	
		专有Master实例-2	
	主机3	专有Master实例-3	
	主机4	Data实例-1	
	主机5	Data实例-2	
主机N	Data实例-N		
50节点及以上	主机1	管理节点-1	两个管理节点作为集群的Client实例节点（有多个Client实例需求,可以在其他节点上继续部署）
		Client实例-1	
	主机2	管理节点-2	

节点数量	主机节点	节点部署规划	说明
		Client实例-2	
	主机3	专有Master实例-1	
	主机4	专有Master实例-2	
	主机5	专有Master实例-3	
	主机6	专有Master实例-4	
	主机7	专有Master实例-5	
	主机8	Data实例-1	
	主机9	Data实例-2	
	主机10	Data实例-3	
	主机N	Data实例-N	

表2-5 Solr、Kafka、Redis 集群主机复用管理节点时

节点数量	主机节点	节点部署规划	说明
3节点及3节点以上	主机1	管理节点-1	两个管理节点均作为集群的实例节点的前两个节点
		实例节点-1	
	主机2	管理节点-2	
		实例节点-2	
	主机3	实例节点-3	
主机N	实例节点-N		

## 2.4 操作系统要求

部署大数据平台时，管理系统占用的管理节点和大数据集群占用的集群节点，支持的操作系统均如[表 2-6](#)所示。

表2-6 操作系统说明

操作系统	版本说明	获取方式
银河麒麟V10（ARM）	Kylin-Server-10-Release-Build06.12.04-lic-zj-20200620-arm64.iso	麒麟厂商提供



### 说明

- 操作系统版本不支持中文语言。
  - 安装操作系统时，建议手动配置 KDUMP 预留 memory 值为 256MB。若安装操作系统时未配置 KDUMP，请联系紫光云技术支持工程师协助处理。
  - 安装操作系统时，对于时区和时间的修改可能不生效，所以安装大数据平台管理系统时必须执行[修改时区及时间的操作](#)。
- 

## 2.5 网络要求

---



### 注意

- 安装大数据平台管理系统前，进行网络规划需注意：系统默认占用了网段 172.17.0.1/16（缺省 docker 网桥网段，即 docker0 所在网段），此网段必须单独预留供 docker 容器使用。若用户已有的网络与该地址段冲突，则需要修改系统 docker 容器网络，详情请参见 [9.6](#) 章节。
  - 安装大数据平台管理系统后，才发现用户已有的网络与系统默认占用的网段冲突，处理方案详情请参见 [9.7](#) 章节。
- 
- 网络带宽要求在 10Gb/s 以上。
  - 大数据集群中各节点之间不能跨越防火墙。

## 2.6 浏览器要求

访问大数据平台管理系统时，支持的浏览器如下：

- Chrome 68 及以上版本



## 2.7 部署流程

图2-1 大数据平台部署流程图

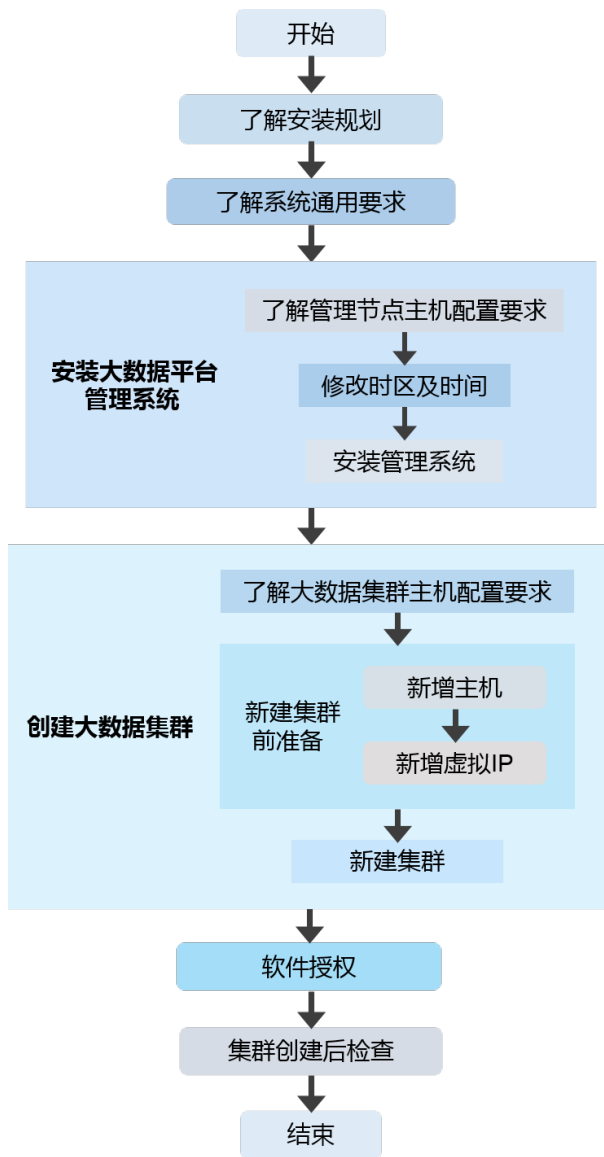


表2-7 大数据平台部署流程说明

序号	步骤	是否必须	详细操作
1	了解安装规划	必选	了解 <a href="#">主机节点类型</a> 和 <a href="#">主机使用规划</a>
2	了解系统通用要求	必选	了解 <a href="#">操作系统要求</a> 、 <a href="#">网络要求</a> 和 <a href="#">浏览器要求</a>
3	安装大数据平台管理系统	必选	了解 <a href="#">管理节点主机配置要求</a>
		必选	执行安装操作之前，必须 <a href="#">修改时区及时间</a>

序号	步骤	是否必须	详细操作
		必选	<a href="#">安装管理系统</a> ，此时数据工厂为选装
		必选	<a href="#">检查安装结果</a> ，此时即可访问大数据平台的管理系统（为保证安全访问，此时建议 <a href="#">添加浏览器安全证书</a> ）
4	创建大数据集群	必选	了解 <a href="#">大数据集群主机配置要求</a>
		必选	了解 <a href="#">新建集群前准备</a> ，按需准备主机资源和虚拟IP资源
		必选	访问大数据平台的管理系统进行大数据集群的创建，包括Hadoop集群、Elasticsearch集群、Solr集群、Kafka集群、Redis集群。对应不同的集群类型，新建集群的配置不同，详情请参见 <a href="#">新建集群</a>
5	软件授权	必选	生产环境中，UniCloud BDP需要经过正式License授权之后，才可永久使用。详情请参见 <a href="#">软件授权</a> 章节
6	集群创建后检查	可选	大数据集群创建成功之后，建议执行 <a href="#">集群巡检</a> ，保证集群健康状态
		可选	大数据集群创建成功之后，建议执行 <a href="#">检查主机</a> ，保证主机健康状态
		可选	大数据集群创建成功之后，建议执行 <a href="#">检查组件</a> ，保证组件健康状态

# 3 安装大数据平台管理系统

## 3.1 安装前必读



注意

- UniCloud BDP 大数据平台的产品软件包用于安装大数据平台管理系统、大数据集群依赖 YUM 源和数据工厂。其中数据工厂为选装模块，其他均为必装。
  - 当大数据平台管理系统安装成功以后，才可以创建大数据集群。
  - 在生产环境中，大数据平台管理系统要求安装在 2 个节点上，并配置虚拟 IP 保证管理系统高可用。安装完成后，这 2 个节点会自动注册到[资源管理/主机管理]的主机列表中，创建大数据集群时可根据实际情况选择是否将这 2 个节点作为大数据集群的节点，选择策略请参见 [2.3.2](#) 章节。
  - 安装大数据平台管理系统时可以选择是否一起安装数据工厂，安装大数据平台管理系统完成之后数据工厂也可以进行单独的安装或卸载。
  - 大数据平台缺省以管理节点第一个主机的本地时间作为基准时间，集群里的所有节点通过 NTP 协议向此管理节点进行时钟校准，建议集群中所有节点与用户现场统一 NTP 服务器保持时钟校准(配置请参见 [3.4.1](#) 章节)。若出现时间不同步的情况，可参考 [9.5](#) 章节。
- 

## 3.2 安装前规划内容



说明

为帮助准确把握安装大数据平台管理系统前的规划内容，请提前了解产品相关术语说明，详情请参见 [表 1-1](#)。

---

根据现场实际情况和业务需求，安装大数据平台管理系统前进行相关规划时，需关注以下内容：

- 根据现场主机节点数目，可选择将大数据平台管理系统与大数据集群是否部署在相同节点上，部署方案详情请参见 [2.3.2](#) 章节。
- 规划大数据平台管理系统的每个节点所在的子网、规划每个节点的 IP 地址。
- 在安装管理系统的网段中规划一个 IP 地址作为虚拟 IP（访问 IP 地址），通过虚拟 IP 可访问大数据平台管理系统。该 IP 地址要求必须是同网段内，未被使用的任一 IP 地址。
- 安装大数据平台管理系统前，需要提前获知管理节点 root 用户的密码。安装成功后，管理节点的主机 root 用户密码会被自动修改为 Passw0rd@\_。

## 3.3 管理节点主机配置要求

### 3.3.1 主机硬件要求



说明

- 在生产环境中，大数据平台管理系统要求安装在 2 个节点上。
- 若规划将安装大数据平台管理系统的 2 个管理节点独立使用，则这 2 个管理节点上的硬件配置要求请参见表 3-1。若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个管理节点上的硬件配置要求请参见表 3-2。
- 在实际生产环境中，管理系统要求使用物理机进行部署，若物理机主机硬件有特殊配置要求或者有使用虚拟机部署的需求，详情请咨询紫光云技术支持工程师。

表3-1 管理节点硬件配置要求（独立使用）

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路10核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 128 GB，推荐 $\geq$ 256GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：1块，推荐：容量 $\geq$ 800GB，转速 $\geq$ 10000r/min 【说明】支持SSD或HDD
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡

表3-2 管理节点硬件配置要求（混合使用）

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路10核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 256GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：至少2块，推荐：转速 $\geq$ 10000r/min

配置项	最低配置要求
	<b>【说明】</b> 1. 管理系统使用 1 块数据盘（容量 $\geq$ 800GB），大数据集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量） 2. 支持 SSD、HDD，也支持 SSD 和 HDD 混合使用
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡

### 3.3.2 磁盘目录规划

在生产环境中，大数据平台管理系统要求安装在 2 个节点上，各节点上的磁盘目录规划请参见[表3-3](#)。

表3-3 磁盘目录规划

目录	容量要求	用途说明	文件系统类型
/	独立分区， $\geq$ 500GB	系统盘，Linux系统目录	ext4
/data	独立分区， $\geq$ 500GB	数据盘，大数据平台管理服务配置、数据、脚本地址	ext4
/var/lib/docker	独立分区， $\geq$ 300GB	数据盘，容器存储地址	ext4

#### 注意

- 创建大数据集群时，若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个节点上的目录规划还需要同时满足 [4.3.2](#) 章节的要求。
- 创建大数据集群时，若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个节点上的数据盘需要进行格式化及挂载，详情请参见 [4.3.5 1.](#) 章节。

### 3.3.3 安装操作系统

在生产环境中，大数据平台管理系统要求安装在 2 个节点上，各节点对操作系统的要求详情请参见[2.4 操作系统要求](#)。

#### 说明

因不同版本的 BDP 软件支持的操作系统版本存在差异，强烈建议同一套环境中大数据平台管理系统的管理节点与大数据集群的集群节点安装相同版本的操作系统。

## 3.4 安装过程

### 3.4.1 修改时区及时间



- 若在安装操作系统时已修改过时区和时间，此步骤仍为必选。
  - 修改时区及时间的操作，建议在安装大数据平台管理系统时规划配置的 2 台管理节点中的第一个上执行（即安装大数据平台管理系统时，在 [3.4.2 3. \(1\)](#) 步骤中配置文件 config.json 的 node 配置项中配置的第一个主机节点 IP）。
- 

修改主机节点的时区及时间的操作步骤如下：

- (1) 先使用 `timedatectl` 命令查看节点的时区，检查时区是否为“Shanghai”，若时区不正确，则需要修改时区。（示例将时区修改为 Shanghai）命令如下：

```
timedatectl set-timezone Asia/Shanghai
```

- (2) 使用 `date` 命令查看系统时间，若系统时间与当前物理时钟不同，则需将系统时间修改为当前物理时钟。（示例将系统时间修改为 2021-3-12 15:48:00）命令如下：

```
date -s "2021-3-12 15:48:00"
```

- (3) 本机硬件时间会影响主机重启后的系统软件时间，校准本机硬件时间的命令如下：

```
hwclock --systohc
```

```
hwclock --show
```

### 3.4.2 安装管理系统



安装大数据平台管理系统的操作，仅需要在任意一台规划的管理节点上执行即可。

---

#### 1. 上传软件包

登录任意一台规划的管理节点上，使用 SFTP 等工具，将 BDP 软件包上传至/opt 目录下（本文档的/opt 仅为示例目录，实际可上传至其他任意目录）。

【说明】为保证安装成功，建议安装目录≥50G。

#### 2. 解压软件包

进入/opt 目录下，解压软件包，命令如下：

```
tar -zxvf BDP-<version>.tar.gz
```

解压完成后，当前目录/opt 中出现 BDP-<version>文件夹。

#### 3. 修改配置文件

- (1) 配置管理节点 IP（必选）

进入解压文件夹中，修改/conf 目录下的配置文件 config.json。修改说明如表 3-4，修改完成后保存退出。

```
cd BDP-<version>/conf
```

```
vi config.json
```

表3-4 配置文件 config.json 修改说明

参数	说明	数量	要求
node	安装大数据平台管理系统时规划的管理节点IP地址	2	必选。 要求：在中括号中添加所有管理节点IP地址，每个IP地址添加双引号，并以逗号分隔
vip	安装大数据平台管理系统时规划的虚拟IP（访问IP地址）	1	必选。 要求：将虚拟IP地址添加双引号
extranet_vip	安装大数据平台管理系统时规划的外网虚拟IP（外网访问IP地址）	1	可选。 要求： <ul style="list-style-type: none"> <li>大数据平台管理系统开启 SSO 且配置内外网映射访问时，将外网映射的虚拟 IP 地址添加双引号</li> <li>大数据平台管理系统未开启 SSO 或未配置内外网映射访问时，无需配置</li> </ul>
ntp_servers	配置大数据平台使用的外部 NTP服务器的IP地址。大数据集群中的所有节点向NTP服务器进行时钟校准	1	可选。 要求： <ul style="list-style-type: none"> <li>若不配置外部 NTP 服务器的 IP 地址（ntp_servers 值为空），则缺省使用大数据平台的两个管理节点作为 NTP 服务器（第一个管理节点为主 NTP 服务器，第二个管理节点为备 NTP 服务器）</li> <li>若配置了外部 NTP 服务器的 IP 地址，则要求此 NTP 服务器的 IP 与大数据集群的 IP 网络互通</li> </ul>

---

 注意

- 大数据平台的管理节点 IP 地址和虚拟 IP 地址要求处于同一网段，且 IP 地址一旦设定，安装完成后均不支持修改。
  - 大数据平台管理系统开启 SSO 且配置内外网映射访问时，`extranet_vip` 必须配置为外网映射 vip。
  - 安装大数据平台管理系统时，若没有开启内外网映射访问，则在后续的使用过程中仍可进行配置，配置方法详情请参见 [9.11. 章节](#)。
  - 安装大数据平台管理系统时，若没有配置外部 NTP 服务器，则在后续的使用过程中仍可进行配置，配置方法详情请参见 [9.10. 章节](#)。
- 

图3-1 配置文件 config.json 修改后

```
{
  "node": ["10.121.68.161", "10.121.68.162"],
  "vip": "10.121.68.160",
  "extranet_vip": "101.12.68.160",
  "ntp_servers": ["10.121.73.136"]
}
```

---

(2) 选择是否修改管理节点缺省主机名（可选）

 说明

- 安装大数据平台管理系统时，管理节点的主机名缺省会被自动修改为 `management0.hde.com` 和 `management1.hde.com`。若需要自定义修改管理节点主机名，则需要修改配置文件 `default.json`，若不需要自定义修改管理节点主机名则跳过此步骤即可。
  - 大数据平台管理系统安装之后，禁止再修改管理节点主机名。
  - 管理节点的整个主机名必须符合完全合格域名/全称域名（Fully Qualified Domain Name，简称 FQDN）。管理节点的主机名默认从 0 开始排序，即以“主机名前缀+数字+主机名后缀”的方式表示多个主机名（主机名字符总长度最少为 5 位，最多不得超过 60 位），比如：`management0.hde.com` 和 `management1.hde.com`。
- 

进入解压文件夹中，修改 `/conf` 目录下的配置文件 `default.json`。修改说明如 [表 3-5](#) 所示，修改 `services.hostname.host_prefix` 和 `services.hostname.domain` 两个配置项的值即可修改管理节点的缺省主机名，修改完成后保存退出即可。关于配置文件 `default.json` 中更多参数项的说明，详情请参见 [9.8. 安装大数据平台管理系统的配置文件说明](#)。

```
cd BDP-<version>/conf
vi default.json
```

表3-5 配置文件 default.json 修改说明

参数	说明
<code>services.hostname.host_prefix</code>	管理节点的主机名前缀 【要求】仅支持以小写字母开头，可包含小写字母、-、数字

---



参数	说明
services.hostname.domain	管理节点的主机的域（即主机名后缀）  【要求】仅支持以小写字母开头，可包含小写字母、.，主机名后缀要求至少两个字符串（且建议以.com、.net、.cn、.org等顶级域名后缀结尾），且建议主机名后缀字符长度不超过12位

图3-2 修改配置文件 default.json 中 services.hostname 下配置项的值

```

"services": {
  "docker": {
    "bip": "172.17.0.1/16"
  },
  "hostname": {
    "host_prefix": "management",
    "domain": "hde.com"
  },
},

```

(3) 选择是否安装数据工厂（可选）



注意

- 安装大数据平台管理系统时，数据工厂模块为选装。若需要安装数据工厂，则需要修改配置文件 default.json，若不需要安装数据工厂则跳过此步骤即可。
- 若安装大数据平台管理系统时，没有同步选择安装数据工厂，在后续使用过程中又有数据工厂的需求，则补充安装数据工厂的方式请参见 [9.9](#) 章节。

进入解压文件夹中，修改/conf 目录下的配置文件 default.json。修改说明如[表 3-6](#)所示，将 df.install 的值由 false 改为 true（df.install 的值默认为 false，即默认不安装数据工厂），修改完成后保存退出即可。关于配置文件 default.json 中更多参数项的说明，详情请参见 [9.8. 安装大数据平台管理系统的配置文件说明](#)。

```
cd BDP-<version>/conf
```

```
vi default.json
```

表3-6 配置文件 default.json 修改说明

参数	说明
df.install	false表示不安装数据工厂，true表示安装数据工厂

图3-3 修改配置文件 default.json 中 df.install 配置项的值

```
"df":{  
  "install": "true"  
}
```

(4) 选择是否对接认证通（可选）



注意

- 安装大数据平台管理系统时，若需要对接认证通，则需要修改配置文件 default.json，若不需要对接认证通则跳过此步骤即可。
- 若大数据平台管理系统需对接认证通，则部署前需在认证通应用管理中添加 BDP 应用，添加完成后获取应用的 appID 和 appSecret 参数。关于在认证通中添加 BDP 应用以及获取应用相关参数的方法详情请参见认证通相关使用手册。
- 安装大数据平台管理系统时，若没有对接认证通，则在后续的使用过程中仍可进行配置，配置方法详情请参见 [9.12. 章节](#)。

进入解压文件夹中，修改/conf 目录下的配置文件 default.json。修改说明如[表 3-7](#)所示，将 use\_rzt 的值由 false 改为 true（use\_rzt 的值默认为 false，即默认不对接认证通），app\_id 和 app\_secret 的值改为认证通中应用具体的参数，修改完成后保存退出即可。关于配置文件 default.json 中更多参数项的说明，详情请参见 [9.8. 安装大数据平台管理系统的配置文件说明](#)。

```
cd BDP-<version>/conf
```

```
vi default.json
```

表3-7 配置文件 default.json 修改说明

参数	说明
use_rzt	false表示不对接认证通，true表示对接认证通
app_id	app_id修改为认证通中BDP应用的appID
app_secret	app_secret修改为认证通中BDP应用的appSecret

图3-4 修改配置文件 default.json 中 use\_rzt、app\_id、app\_secret 配置项的值

```
"sso": {  
  "port": "28026",  
  "proxy_port": "28027",  
  "mysql_database": "sso",  
  "use_rzt": "true",  
  "app_id": "rsF19gJc",  
  "app_secret": "269e1d2f3ec747f2aa986b6ae9f33b12ed9a3f4e"  
}
```

## 4. 启动安装

在解压文件夹中，执行安装脚本，命令如下：

```
sh install.sh
```

---

### 说明

- 安装脚本执行过程中，会出现相关的询问信息（比如：输入主机 root 密码），请根据提示输入信息后继续执行。
  - 安装过程会持续一段时间，请耐心等待。因 YUM 源还原时间较长，会重试多次打印“RETRYING: check yum”日志。
  - 如果安装大数据平台管理系统失败，可以通过卸载脚本进行删除后再重新安装，卸载操作详情请参见 [8.3](#) 章节。
  - 大数据平台管理系统安装成功之后，安装节点自动会被加入到[资源管理/主机管理]的主机列表中。此时，管理节点的主机 root 用户密码会被自动修改为 Passw0rd@\_，若在 [3.4.2 3. \(2\)](#) 章节没有修改管理节点的主机名则主机名缺省为 management0.hde.com 和 management1.hde.com。
- 

## 3.4.3 检查安装结果

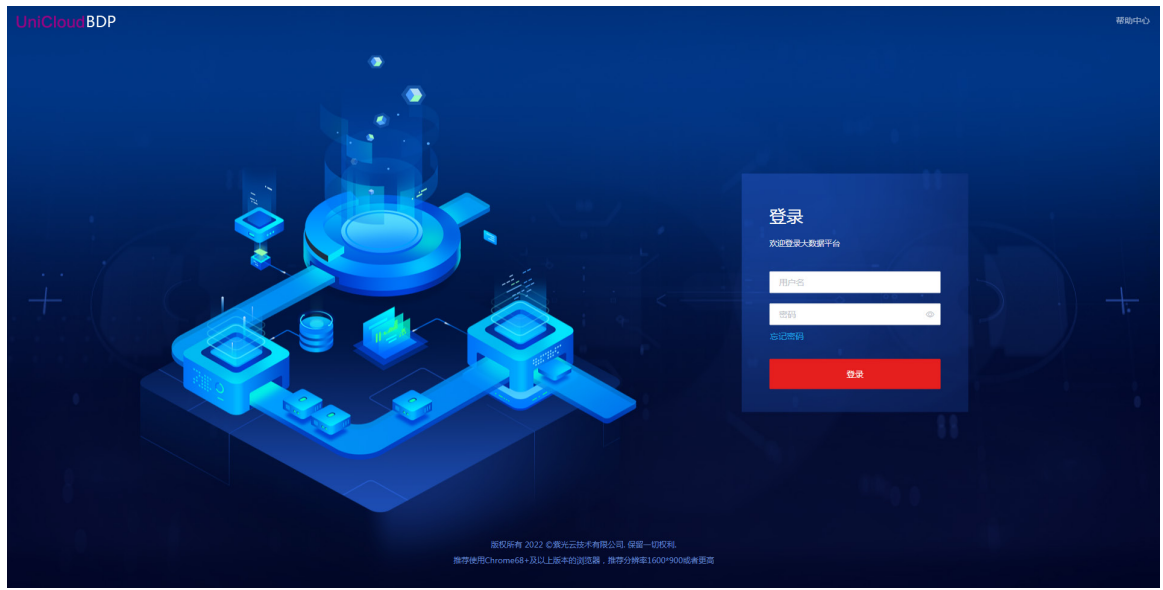
安装完成后，会出现相关提示信息，显示访问大数据平台管理系统的 URL 地址。访问大数据平台管理系统，如 [图 3-5](#) 所示，此时通过缺省用户名/密码（admin/Passw0rd@\_）即可登录系统，开始创建大数据集群。

---

### 说明

- 由于大数据平台管理系统仅支持通过 https 协议访问，所以需要为浏览器添加授权证书以保证安全访问，配置客户端的操作详情请参见 [5.2](#) 章节。
  - 若大数据平台管理系统被扫描出存在 CSRF（跨站点请求伪造）漏洞，处理方案请参见 [9.14](#) 章节。
-

图3-5 大数据平台管理系统



# 4 创建大数据集群

## 4.1 创建前必读



注意

- 大数据平台管理系统安装成功以后，即可创建大数据集群。
- 在生产环境中，大数据平台管理系统要求安装在 2 个节点上，并配置虚拟 IP 保证高可用。安装完成后，这 2 个节点会自动注册到[资源管理/主机列表]中，创建大数据集群时可根据实际情况选择是否将这 2 个节点作为大数据集群的节点，选择策略请参见 [2.3.2](#) 章节。
- 当大数据平台管理系统和大数据集群部署在相同节点上，复用节点的硬件要求和磁盘目录规划等必须同时符合不同节点类型的要求，详情请参见 [3.3](#) 和 [4.3](#) 章节。
- 大数据集群内置高可用方案，在生产环境中为避免单机故障的风险，强烈建议集群开启高可用。
- 部署大数据集群前，务必规划集群是否开启安全管理（Kerberos 认证、审计日志、权限与密钥管理），规划集群是否开启日志管理。请知：安全管理、日志管理等功能若在新建集群时没有开启，则后续在使用过程中将再也无法开启，且一旦开启将再也无法关闭。
- 开启 Kerberos 后，业务端需要进行安全认证适配。所以在生产环境中，部署集群前，请务必确认清楚是否要开启 Kerberos。
- 在大数据平台中，大数据集群内置组件部署规则，可使得大数据集群部署更简单。

## 4.2 创建前规划内容



说明

为帮助准确把握创建大数据集群前的规划内容，请提前了解产品相关术语说明，详情请参见[表 1-1](#)。

根据现场实际情况和业务需求，创建大数据集群前进行相关规划时，需关注以下内容：

- 根据现场主机节点数目，可选择将大数据平台管理系统与大数据集群是否部署在相同节点上，部署方案详情请参见 [2.3.2](#) 章节。
- 规划大数据集群的类型，选择：Hadoop、Elasticsearch、Solr、Kafka 或 Redis 集群。
- 规划大数据集群的模式，选择：独立模式或租户模式。
- 根据现场实际情况，规划大数据集群中的主机节点数目。
- 规划大数据集群中的每个节点所在的子网、规划每个节点的主机名和 IP 地址。
- 规划大数据集群是否开启高可用（强烈建议：生产环境必须开启高可用）。若规划大数据集群开启高可用，则需规划集群对应的虚拟 IP。

- 规划大数据集群是否开启安全管理（Kerberos 认证、审计日志、权限与密钥管理），规划大数据集群是否开启日志管理。请知：安全管理、日志管理等功能若在新建集群时没有开启，则后续在使用过程中将再也无法开启，且一旦开启将再也无法关闭。
- 创建大数据集群前，需要提前获知集群中各节点 root 用户的密码。创建大数据集群前，需要提前将主机新增到[资源管理/主机管理]的主机列表中（新增主机成功后，主机的 root 用户密码会被自动修改为 Passw0rd@\_）。
- 根据现场业务需求，对于 Hadoop 集群，需要规划大数据集群中安装哪些组件，为提升产品易用性，创建 Hadoop 集群时系统缺省内置了组件部署策略，详情请参见 4.2.1 章节；对于 Elasticsearch、Solr、Kafka 和 Redis 集群，各类集群中可安装组件已缺省配置（不可更改）。
- 规划大数据集群中各主机的节点实例类型、规划是否需要专有节点实例（专门用来部署某个组件的节点）。

## 4.2.1 系统内置的组件部署规则



注意

在生产环境中，为避免单机故障的风险，大数据集群内置了高可用方案（即 HA 策略）。当集群开启高可用时，Master 实例要求部署 2 个，组件相关的进程也会同时部署 2 个并自动开启高可用。

---

为提升产品易用性，创建大数据集群时缺省内置了组件部署策略，整体规则如下：

- 若某组件规划了专有实例节点，则相应组件优先默认部署在相应的专有实例节点上。
- Client 类组件和进程默认在所有主机节点上都安装。
- 若某组件进程部署策略为“用户不可自行勾选”，说明该组件进程部署规则已做限制，用户不可以自定义修改；若某组件进程部署策略为“用户可自定义勾选”，说明根据现场实际情况，用户可调整该组件进程的部署配置，但是调整需遵循对应的部署原则。
- 若某组件如果有固定部署数量限制，则以部署数量为准，即虽然默认勾选了某类型的实例节点，但是并不是所有该类型的实例节点上都部署该组件。

## 4.3 大数据集群主机配置要求

### 4.3.1 主机硬件要求



注意

- 创建大数据集群时，若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个节点上的硬件配置要求请参见表 3-2。
  - 大数据集群至少部署在 3 个节点上，本章节的主机硬件要求仅适用部署大数据集群的单台主机（即：在该节点上不部署管理系统）。
  - 在实际生产环境中，大数据集群要求使用物理机进行部署，若物理机主机硬件有特殊配置要求或者有使用虚拟机部署的需求，详情请咨询紫光云技术支持工程师。
-

表4-1 Hadoop 集群单节点硬件配置要求

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路10核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 256GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：至少1块，推荐：转速 $\geq$ 10000r/min <b>【说明】</b> <ul style="list-style-type: none"> <li>• Hadoop 集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量）</li> <li>• 支持 SSD、HDD，也支持 SSD 和 HDD 混合使用</li> </ul>
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡

表4-2 Kafka 集群单节点硬件配置要求

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路8核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 64 GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：至少1块，推荐：转速 $\geq$ 10000r/min <b>【说明】</b> <ul style="list-style-type: none"> <li>• Kafka 集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量）</li> <li>• 支持 SSD、HDD，也支持 SSD 和 HDD 混合使用</li> </ul>
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡

表4-3 Redis 集群单节点硬件配置要求

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路8核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 64 GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：至少1块，推荐：转速 $\geq$ 10000r/min <b>【说明】</b> <ul style="list-style-type: none"> <li>Redis 集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量）</li> <li>支持 SSD、HDD，也支持 SSD 和 HDD 混合使用</li> </ul>
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡

表4-4 Elasticsearch 集群单节点硬件配置要求

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数 $\geq$ 2路10核 主频： $\geq$ 2.0 GHz
内存	$\geq$ 128 GB
系统盘	HDD（至少2块），推荐：每块盘容量 $\geq$ 600GB，转速 $\geq$ 10000r/min
数据盘	要求：至少1块，推荐：转速 $\geq$ 10000r/min <b>【说明】</b> <ul style="list-style-type: none"> <li>Elasticsearch 集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量）</li> <li>支持 SSD、HDD，也支持 SSD 和 HDD 混合使用</li> </ul>
RAID卡	缓存： $\geq$ 1GB，支持掉电保护
网卡	要求：2张万兆网卡



表4-5 Solr 集群单节点主机配置要求

配置项	最低配置要求
型号	主流服务器厂商x86服务器
CPU	Intel Xeon V3系列或更新型号，总核数≥2路10核 主频：≥2.0 GHz
内存	≥128 GB
系统盘	HDD（至少2块），推荐：每块盘容量≥600GB，转速≥10000r/min
数据盘	要求：至少1块，推荐：转速≥10000r/min <b>【说明】</b> <ul style="list-style-type: none"> <li>Solr 集群至少使用 1 块数据盘（可参考业务数据量规划磁盘数量和容量）</li> <li>支持 SSD、HDD，也支持 SSD 和 HDD 混合使用</li> </ul>
RAID卡	缓存：≥1GB，支持掉电保护
网卡	要求：2张万兆网卡

### 4.3.2 磁盘目录规划

在生产环境中，大数据集群要求至少部署在 3 个节点上，各节点上的磁盘目录规划请参见[表 4-6](#)。

表4-6 磁盘目录规划

目录	容量要求	用途说明	文件系统类型
/	独立分区，≥500G	系统盘，Linux系统目录	ext4
/var/de_log	独立分区，≥300G	数据盘，大数据组件日志目录	ext4



注意

创建大数据集群时，若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个节点上的目录规划还需要同时满足 [3.3.2](#) 章节的要求。

### 4.3.3 安装操作系统

在生产环境中，大数据集群要求至少部署在 3 个节点上，各节点对操作系统的要求详情请参见 [2.4 操作系统要求](#)。



因不同版本的 BDP 软件支持的操作系统版本存在差异，强烈建议同一套环境中大数据平台管理系统的管理节点与大数据集群的集群节点安装相同版本的操作系统（集群扩容时有同样要求）。

---

#### 4.3.4 磁盘 RAID 方案

---



本章节内容仅适用于部署大数据集群的所有主机节点。

---

部署大数据集群时，集群各节点的磁盘 RAID 整体原则如下：

- 操作系统盘做 RAID1。
  - 对于 Hadoop 集群，根据集群中是否规划专有实例节点，数据盘分为两种情况：
    - 大数据集群中的非专有实例节点，数据盘建议做单盘 RAID0 或直接裸磁盘（JBOD）。
    - 若大数据集群中规划了专有实例节点（即：在 Hadoop 集群中为 Redis、Zookeeper、Elasticsearch、Solr 或 Kafka 配置专有实例节点），此时，对应专有实例节点的磁盘 RAID 方案如下：
      - Zookeeper 专有实例：建议做单盘 RAID0 或者直接裸磁盘（JBOD）
      - Kafka 专有实例：建议做单盘 RAID0 或者直接裸磁盘（JBOD）
      - Redis 专有实例：要求做 RAID5
      - Solr 专有实例：要求做 RAID5
      - Elasticsearch 专有实例：建议做单盘 RAID0 或者直接裸磁盘（JBOD）
  - 对于 Elasticsearch、Solr、Kafka 或 Redis 集群，大数据集群中各主机的数据盘 RAID 方案如下：
    - 在 Solr 或 Kafka 集群中，若规划为 Zookeeper 配置专有实例节点，则：建议 Zookeeper 专有实例节点做单盘 RAID0 或者直接裸磁盘（JBOD）
    - Elasticsearch 集群中的 Data 实例或专有 Master 实例：建议做单盘 RAID0 或者直接裸磁盘（JBOD）
    - Solr 集群中的 Solr 实例：要求做 RAID5
    - Kafka 集群中的 Kafka 实例：建议做单盘 RAID0 或者直接裸磁盘（JBOD）
    - Redis 集群中的 Redis 实例：要求做 RAID5
- 



因不同厂商的硬件服务器设置方式略有不同，这里仅说明部署不同类型的大数据集群时配置 RAID 的建议，对于配置过程不做说明。

---

## 4.3.5 数据盘规划



说明

- 本章节内容仅适用于部署大数据集群的所有主机节点，且此时集群的存储类型必须为 HDFS。
- 数据盘空间主要由现场数据业务量决定，请根据实际情况进行规划。

### 1. 对数据盘进行格式化及挂载



注意

- 在大数据集群所有主机节点上，操作系统安装完成后，数据盘均必须执行格式化及挂载操作，否则会导致大数据组件无法识别到数据盘。
- 创建大数据集群时，若规划将安装大数据平台管理系统的 2 个管理节点同时作为大数据集群节点使用，则这 2 个节点上的数据盘也需要进行格式化及挂载，详情请参见 [3.3.2](#) 章节。

对数据盘执行格式化及挂载操作时，当前版本，仅支持手动方式。

- 手动方式  
手动对数据盘进行格式化及挂载操作时，操作示例如下：
  - a. 格式化文件系统：`mkfs.ext4 /dev/sdc`
  - b. 挂载：`mount /dev/sdc /opt/disk1`
  - c. 将挂载信息写入 `/etc/fstab` 文件中，实现开机自动挂载

### 2. 集群节点数规划（示例）

若仅从硬盘空间来考虑，集群主要分为离线计算、在线查询、全文检索。其中：离线计算主要是 MapReduce2/Spark/Hive 集群针对 HDFS 文件的运行计算；在线查询主要是对 HBase 的操作及查询；全文检索主要是针对 Elasticsearch 或 Solr 的操作及查询。

- 离线计算与在线查询都是基于 HDFS 的操作，所以磁盘规划的原则是一致的。按照以下公式计算集群节点规模：

$$\begin{aligned} & \text{集群的数据节点数} \\ & = \text{RoundUp} \left( \frac{\text{集群总数据量\_TB} * \text{HDFS 副本数量} * \text{应用层数据压缩率} * \text{数据膨胀率}}{(\text{单硬盘大小\_TB} * \text{单节点硬盘数量} * \text{硬盘利用率}) / \text{磁盘格式化率}} \right) \end{aligned}$$

表4-7 基于 HDFS 的磁盘空间规划计算示例

配置项	配置值
集群总数据量 (TB)	100
HDFS副本数量	3
应用层数据压缩率	1

配置项	配置值
数据膨胀率	1.2
单硬盘大小 (TB)	1.8
单节点硬盘数量	25
磁盘利用率	70%
磁盘格式化率	1.093
集群数据节点数	13

- 全文检索的磁盘规划主要基于 Solr 或 Elasticsearch，按照以下公式计算集群节点规模：

集群的数据节点数

$$= \text{RoundUp} \left( \frac{\text{集群总数据量\_TB} * (\text{Solr 或者 Elasticsearch 的副本数})}{\text{单条数据大小} * \text{单节点数据的条目}} \right)$$

表4-8 基于 Elasticsearch 的磁盘空间规划计算示例

配置项	配置值
集群总数据量 (TB)	100
Solr或者Elasticsearch副本数量	2
单条数据大小 (KB)	0.2
单节点数据条目 (亿条)	200
集群数据节点数	50

## 4.4 新建集群前准备

### 4.4.1 新增主机



注意

- 创建大数据集群之前，必须提前将所需主机新增进[集群管理/资源管理/主机管理]的主机列表中，新增主机包括单台新增主机或批量新增主机两种方式。新增主机的操作系统、硬件要求、磁盘方案、RAID 方案等需满足 [4.3](#) 章节中的要求。
- 规划部署在同一个大数据集群内的主机，要求其所有主机 IP 必须处于同一网段，且未被占用。
- 在[集群管理/资源管理/主机管理]的主机列表中单台新增主机或批量新增主机时，均要求输入主机的 root 用户密码。新增主机成功后，主机的 root 用户密码会被自动修改为 PasswOrd@\_（注意：当主机处于“未使用”状

态时，其 root 密码禁止修改，否则将导致大数据集群创建失败；当主机处于“已使用”状态时，其 root 密码可在[使用此主机的集群详情页面](#)进行修改。

- 在[\[集群管理/资源管理/主机管理\]](#)的主机列表中新增主机时，需要配置主机名。其中：主机名前缀可自定义，主机名后缀为固定格式。
- 

新增主机包括单台新增主机或批量新增主机两种方式，根据实际需要任意选择一种即可。访问大数据平台管理页面，新增主机的步骤如下：

- (1) 在集群管理的左侧导航树中选择[\[资源管理/主机管理\]](#)，进入主机管理页面。
- (2) 在主机管理页面，选择[\[主机列表\]](#)页签，单击左上角的<新增主机>按钮，弹出新增主机窗口。
- (3) 新增主机包括“主机”和“主机组”两个页签，可根据实际需要进行选择。根据提示配置对应参数项的值，如下：
  - 主机，即单台新增主机方式。
    - 主机 IP：输入符合规则的主机 IP 地址（示例 1.1.1.1），单击<测试连通性>测试此主机与系统是否网络互通。
    - 主机名：主机名包括前缀和后缀，此时需要输入符合命名规则的主机名前缀，主机名后缀为固定格式。
    - 用户名：缺省配置为主机的 root 用户。
    - 用户密码：输入主机的 root 用户密码。
  - 主机组，即批量新增主机方式。
    - 导出模板：单击<导出模板>按钮，可将批量新增主机时需要的模板文件下载至本地（在模板文件中添加主机参数信息时，不允许删除标题行，且必须按行顺序填写，不支持跨空行填写）。模板文件中包含的主机参数信息说明为：
      - 1) 管理 IP 和主机 IP 相同，均需填写主机的 IP 地址。
      - 2) 用户名必须填写 root 用户，不可修改。
      - 3) 密码为主机的 root 用户密码，请根据实际 root 用户密码填写。
      - 4) SSH 端口号固定为 22，不可修改。
      - 5) 主机名只需要添加主机名前缀（主机名后缀会自动生成），且前缀可自定义。
    - 导入模板：在下载模板文件中填写各主机的相关信息并保存后，单击<选择文件>按钮可上传至系统。上传成功后页面会显示该文件（此时仅支持单文件上传，若重复上传会执行替换旧文件的操作）。
- (4) 配置完成后，单击<确定>按钮即可新增主机，单台新增主机成功后直接在主机列表中显示，批量新增主机时需耐心等待一段时间直至所有主机均在主机列表中显示。

图4-1 新增主机

新增主机

主机 主机组

\* 主机IP  测试连通性

\* 主机名  .hde.com

用户名

\* 用户密码

操作提示：用户主机添加成功后，密码和主机名将会被重置。

确定 取消

## 4.4.2 新增虚拟 IP



### 注意

- 进行大数据集群部署规划时，若规划集群开启高可用，则需要提前新增集群对应的虚拟 IP 池。
- 新增虚拟 IP 池要求：在集群主机所处的 IP 段中，选取一段未被占用的 IP 作为虚拟 IP 池，供集群开启高可用时选用。
- 新增虚拟 IP 池时，需要保证子网掩码和其对应的集群中各主机节点的子网掩码一致，否则即使虚拟 IP 池中有资源，在新建集群时也会提示虚拟 IP 池中资源不足。
- 部署多个大数据集群时，若各集群主机 IP 不属于同一个 IP 段，则需要分别为各集群新增对应的虚拟 IP 池。

若集群规划开启高可用，则需要为集群新增对应的虚拟 IP。访问大数据平台管理页面，新增虚拟 IP 池的步骤如下：

- (1) 在集群管理的左侧导航树中选择[资源管理/主机管理]，进入主机管理页面。
- (2) 在主机管理页面，选择[虚拟 IP 列表]页签，单击左上角的<新增虚拟 IP>按钮，弹出新增虚拟 IP 池窗口。
- (3) 根据提示配置对应参数项的值，如下：
  - 名称：自定义输入符合命名规则的虚拟 IP 池名称。
  - 子网掩码：要求输入的子网掩码必须和对应集群的主机 IP 子网掩码相同。
  - 可分配 IP 段：包括起始地址和结束地址，要求在此 IP 段内的所有 IP 必须和对应集群的主机 IP 处于同一网段，且均未被占用。
- (4) 配置完成后，单击<确定>按钮即可新增虚拟 IP 池。

图4-2 新增虚拟 IP 池



新增虚拟IP池

\* 名称

\* 子网掩码

\* 可分配IP段

确定 取消

## 4.5 新建集群



### 注意

- 普通用户新建集群时，需要走流程审批，待审批人审批通过后才能触发新建集群的操作。管理员用户新建集群时，会直接触发新建集群的操作。
- 集群名称具有唯一性，在系统中创建多个集群时名称不能重复。
- 新建集群前，要求在[集群管理/资源管理/主机管理]页面的主机列表页签中已完成所需主机的新增。
- 若规划集群开启高可用，则新建集群前，要求必须在[集群管理/资源管理/主机管理]页面的虚拟 IP 列表页签中已完成所需虚拟 IP 的新增。
- 不同组件之间可能存在依赖关系，请根据页面提示进行关联选择即可。
- 大数据集群支持安装的组件类别和版本号，详情请以实际页面为准。
- 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。
- 如果当前版本中的大数据集群需对接 UniCloud 数据管理平台，请配置“安全管理-Kerberos 认证”和“安全管理-权限管理”为同时开启或关闭。

当前版本中，大数据平台中支持创建的集群类型包括：

- [新建 Hadoop 集群](#)
- [新建 Elasticsearch 集群](#)
- [新建 Solr 集群](#)
- [新建 Kafka 集群](#)
- [新建 Redis 集群](#)

## 4.5.1 新建 Hadoop 集群



注意

- 新建集群前需要提前规划集群模式和集群超级用户，且同时需要提前对节点数量、待安装组件、是否开启安全管理、是否开启日志管理、是否开启高可用等进行规划。
- 新建集群时，若没有开启安全管理（Kerberos 除外）和高可用，则后续在使用过程中将再也无法开启。所以在生产环境中，强烈建议新建集群时同时开启安全管理和高可用。
- 选择安装组件时，Hadoop 组件提供针对大数据集群的分布式数据存储、离线计算、统一资源调度框架，包含 HDFS、MapReduce、YARN。
- 新建集群时，若规划安装支持磁盘配置的组件（如 Redis、Solr、Elasticsearch、HDFS 等），可在磁盘配置步骤自定义设置其对应的管理配置组或磁盘挂载点；若不设置，则将按照内置缺省规则进行组件部署。
- 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。

集群类型为 Hadoop 集群时，集群中可安装 Spark、Elasticsearch、Hive、Flink、Zookeeper、Kafka 等组件，支持部署多种模式或多种功能用途的大数据集群，比如查询分析集群、流式计算集群、全文检索集群等。

新建 Hadoop 集群的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击<新建集群>按钮，跳转至新建集群页面。
- (3) 输入集群名称，选择集群类型为 Hadoop，即可开始新建 Hadoop 集群。
- (4) 新建 Hadoop 集群包括 5 个配置步骤，根据提示配置对应参数项的值，如下：

**第一步：基础配置**，参数说明如下：

- 集群名称：自定义输入符合命名规则的集群名称。
- 集群类型：选择 Hadoop 类型。
- 集群模式：选择新建集群的模式，包括独立模式和租户模式两种。
- 集群超级用户：配置集群的超级用户，用于访问集群中的组件，并拥有对应组件权限，关于集群超级用户权限详情请参见产品在线联机帮助。注意：admin 用户、root 用户、组件超级用户（如 hdfs、storm、hbase 等）、hadoop 用户等不可被选作为集群超级用户。待新建集群成功后，集群超级用户会自动同步到[集群权限/用户管理]中。
- 密码：输入集群超级用户对应的密码。
- 确认密码：再次输入集群超级用户对应的密码，进行确认。
- 集群描述：自定义添加集群的描述信息，以便于快速了解集群相关信息。
- 选择安装组件：根据部署规划，勾选待安装的组件。其中：基础组件 Hadoop 和 Zookeeper 为必选项，其他组件可选。
- 安全管理：独立集群可选择是否开启安全管理。若选择开启，则同时提供 Kerberos 认证、审计日志、权限与密钥管理功能，提供用户安全认证和数据安全访问等功能，保证数据安全性。租户集群缺省开启安全管理功能（不支持关闭）。
  - Kerberos 认证：Kerberos 认证可以提供用户安全认证方式功能。独立集群可选择是否开启 Kerberos 认证。租户集群缺省开启 Kerberos 认证功能（不支持关闭）。



- 审计日志：选择集群是否开启审计日志。审计日志可以记录用户访问组件的信息，并提供界面化的查询功能。
- 权限与密钥管理：开启安全管理时默认开启权限与密钥管理（不支持关闭）。权限与密钥管理可以提供数据的权限访问控制和 **HDFS** 密钥管理工具。
- o 日志管理：选择集群是否开启日志管理。若选择开启，则该集群提供组件日志功能；若没有开启，则后续在使用过程中将再也无法开启。
- o 存储类型：为 **Hadoop** 组件选择存储类型 **HDFS**，表示将 **HDFS** 数据存储在 **HDFS** 组件的 **DataNode** 中，即属于存储和计算未分离情况。

图4-3 基础配置

返回 | 新建集群

1 基础配置 2 硬件配置 3 实例分配 4 磁盘配置 5 确认信息

\* 集群名称：

\* 集群类型： Hadoop  Elasticsearch  Solr  Kafka  Redis

\* 集群模式： 独立模式  租户模式

\* 集群超级用户：

\* 密码：

\* 确认密码：

集群描述：

\* 选择安装组件：

**基础组件**

<input checked="" type="checkbox"/>	组件名	版本	描述
<input checked="" type="checkbox"/>	Hadoop	3.0.0	针对大数据集的分布式数据存储HDFS、离线计算MapReduce、统一资源调度框架YARN
<input checked="" type="checkbox"/>	ZooKeeper	3.4.5	分布式应用程序协调服务，为集群提供一致性服务

**查询分析**

<input type="checkbox"/>	组件名	版本	描述
<input type="checkbox"/>	Hive	2.1.1	建立在Hadoop上的数据仓库框架，提供HQL语言进行数据离线分析处理
<input type="checkbox"/>	Spark2	2.4.0	基于内存的分布式计算框架，提供批量处理、流式计算、SQL以及机器学习的能力
<input type="checkbox"/>	Sqoop	1.4.7	用于Hadoop与传统关系型数据库间数据迁移的工具
<input type="checkbox"/>	HBase	2.1.0	基于Hadoop的分布式NoSQL数据库，具备高并发、低延迟的实时查询能力
<input type="checkbox"/>	HBase Indexer	1.5	HBase异步索引组件，利用Solr为HBase提供二级索引能力
<input type="checkbox"/>	Oozie	5.1.0	用于Hadoop平台的开源的工作流调度引擎
<input type="checkbox"/>	Redis	6.2.1	基于内存的分布式缓存数据库，满足高性能读写业务需求
<input type="checkbox"/>	Presto	1.5.0	一款高性能数据虚拟化引擎，提供统一SQL接口，具备跨数据源/数据中心分析能力以及...
<input type="checkbox"/>	DLH	1.0.0	基于Hive的数据湖仓库服务，融合批处理、交互式及流处理，具备数据协同分析能力

**流式计算**

<input type="checkbox"/>	组件名	版本	描述
<input type="checkbox"/>	Storm	1.2.1	一种分布式流式数据处理系统，支持毫秒级级别的实时数据处理，具有良好的稳定性和...
<input type="checkbox"/>	Kafka	2.7.2	高吞吐量的分布式消息队列系统，具有出色的性能和可靠性
<input type="checkbox"/>	Flink	1.13.6	一种统一流处理和批处理的分布式计算引擎，支持亚秒级的流式处理延迟，提供批流统...
<input type="checkbox"/>	Flume	1.9.0	一种分布式、高可靠、高可用的系统，用于有效地从多种数据源收集、聚合、移动日志...

**全文检索**

<input type="checkbox"/>	组件名	版本	描述
<input type="checkbox"/>	Elasticsearch	7.10.0	基于Lucene的分布式搜索和分析引擎，提供大数据集的实时搜索、分析和探索的能力
<input type="checkbox"/>	Solr	7.4.0	基于Lucene的高性能全文搜索引擎，具备强大的搜索和近实时的索引能力

安全管理： 提供用户安全认证和数据安全访问等功能，保证数据安全性

Kerberos认证： 提供用户安全认证方式

审计日志： 记录用户访问组件的信息，并提供界面化的查询功能

权限与密钥管理： 提供数据的访问权限控制和HDFS密钥管理工具

组件日志： 提供组件的日志信息

存储类型： HDFS

下一步:硬件配置 取消

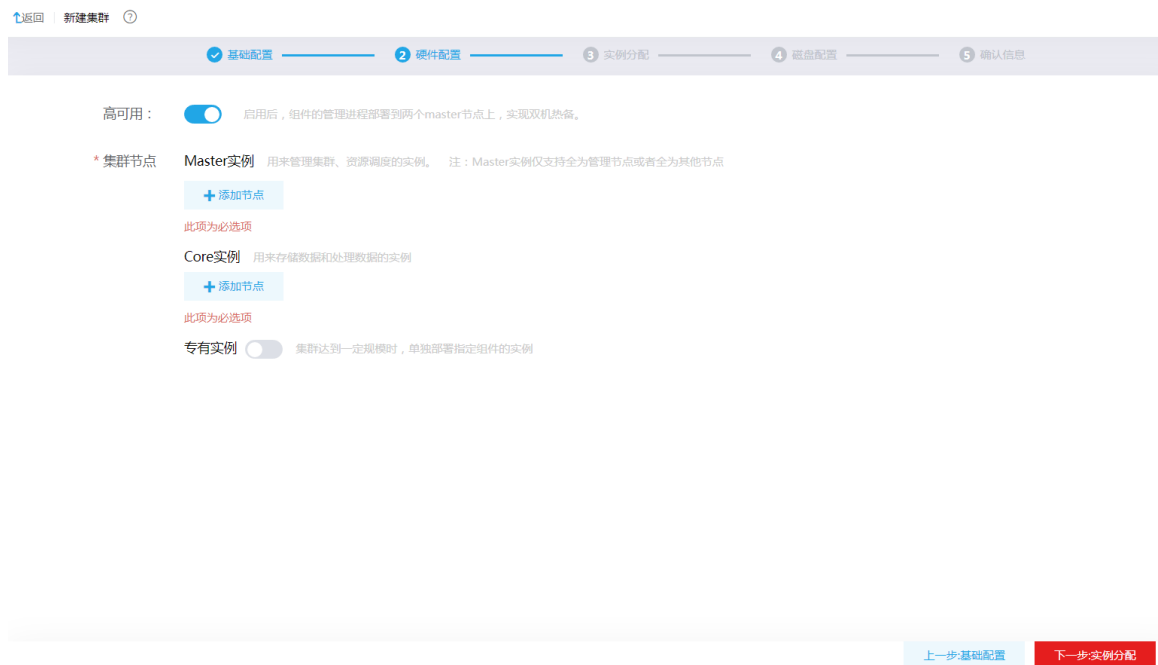
**第二步：硬件配置**，参数说明如下：

- 高可用：选择集群是否开启高可用。若选择开启，则组件的管理进程将同时部署到两个节点上，实现双机热备；若未开启高可用，则存在单机故障的风险。创建集群时，缺省开启高可用。
- 集群节点：创建集群时，集群节点包含多种类型，详情请参见[表 4-9](#)。新建集群时，集群节点数量至少为 3 个。根据是否开启高可用，Master 实例要求部署个数不同，且 Core 实例的最少部署个数也不同。

**表4-9 集群节点说明**

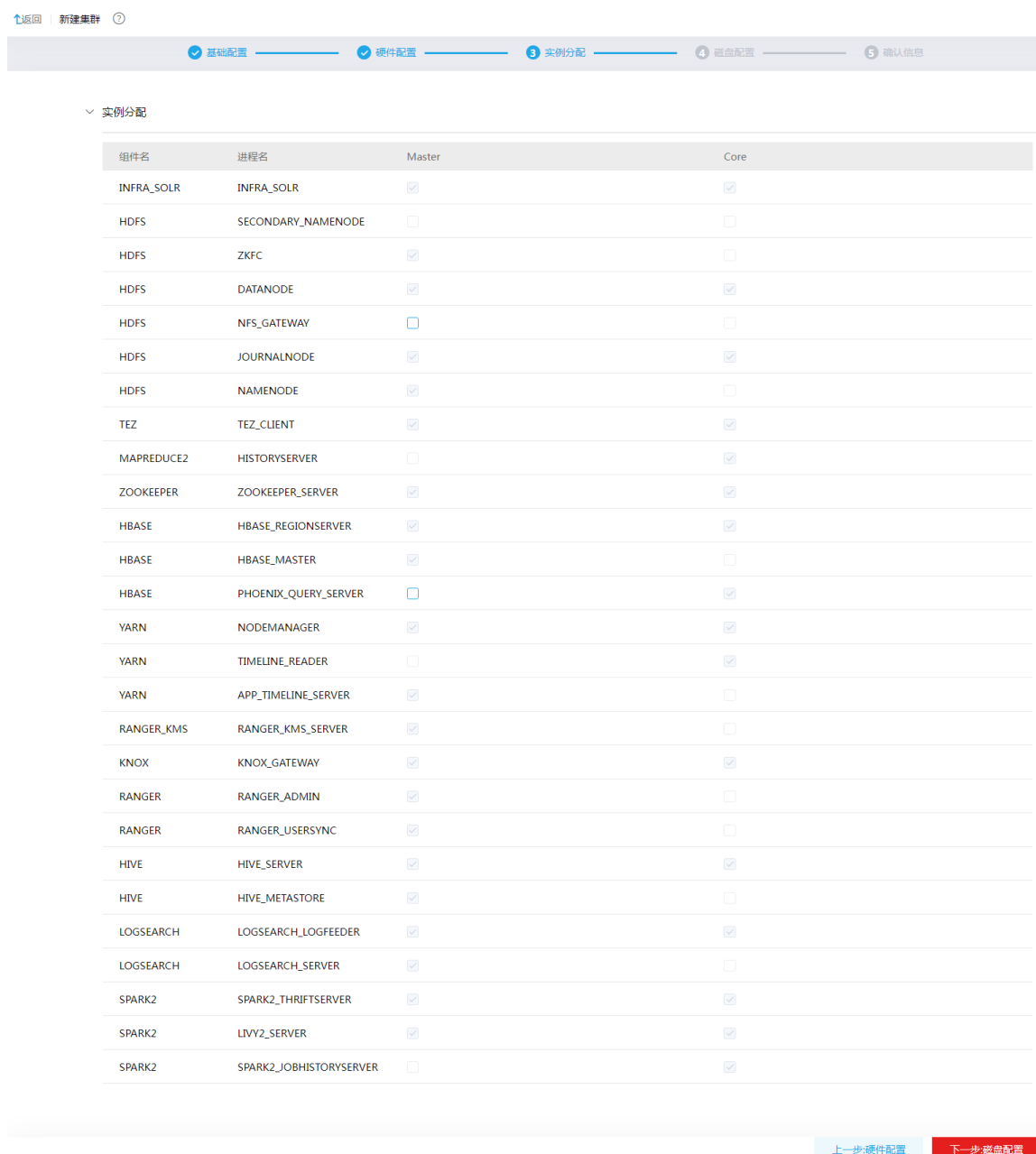
节点类型	是否必选	选型说明	描述
Master实例	必选	即主实例，用来管理集群、进行资源调度的实例，主要部署各组件的Master进程，如NameNode、ResourceManager等 <b>【说明】</b> 若集群未开启高可用，则Master实例个数为1，且不可更改；若集群开启了高可用，则Master实例个数为2，且不可更改	在生产环境中，强烈建议集群开启高可用，此时HDFS、YARN、Hive、HBase等组件也将同步开启HA <b>【注意】</b> 在生产环境中，若在创建集群的硬件配置步骤没有开启高可用，后续在使用过程中集群将再也无法开启高可用
Core实例	必选	即核心实例，用来存储数据和处理数据的实例，主要部署各组件的数据进程等，如DataNode，NodeManager等 <b>【说明】</b> 若集群未开启高可用，则Core实例个数至少为2；若集群开启了高可用，则Core实例个数至少为1	在生产环境中，Core实例的个数需要根据实际数据量大小或计算需求等情况进行规划
专有实例	可选	当前版本中，集群支持的专有实例类型包括：Redis、Zookeeper、Elasticsearch、Solr、Kafka	集群达到一定规模时，可单独部署指定组件的实例

图4-4 硬件配置





**第三步：实例分配**，显示待安装组件的各进程在各节点类型的主机上的部署规则，此时部分进程的部署配置可自定义做出调整，不支持做调整的部署配置将置灰（系统中已内置组件进程的部署规则）。

图4-5 实例分配



**第四步：磁盘配置**，在存储目录下勾选组件后，在操作栏中单击<修改>按钮，会弹出管理配置组窗口，然后在窗口中单击添加配置组+图标，输入配置组名称和描述即可添加配置组，添加成功后即可管理配置组。

- 添加配置组：在配置组列表中，单击+图标，弹出添加配置组窗口，输入配置组名称、描述即可完成添加。
- 编辑配置组：在配置组列表中选择某配置组后，单击图标，弹出修改配置组窗口，可修改该配置组名称或描述。
- 删除配置组：在配置组列表中选择某配置组后，单击图标并在弹窗中进行确认后即可删除该配置组。

- 添加主机：在配置组列表中选择某配置组后，然后在对应的主机列表中单击+图标，弹出增加配置组主机窗口，可为该配置组选择要添加的主机。
- 删除主机：在配置组列表中选择某配置组后，然后在对应的主机列表中选择某主机后，单击-图标并在弹窗中进行确认后即可删除该主机。
- 挂载点列表：若某配置组选择的主机节点对应的磁盘有划分分区，可在挂载点列表勾选其数据盘对应的挂载路径（若无挂载点信息，请尝试单击刷新按钮获取）。

图4-6 磁盘配置

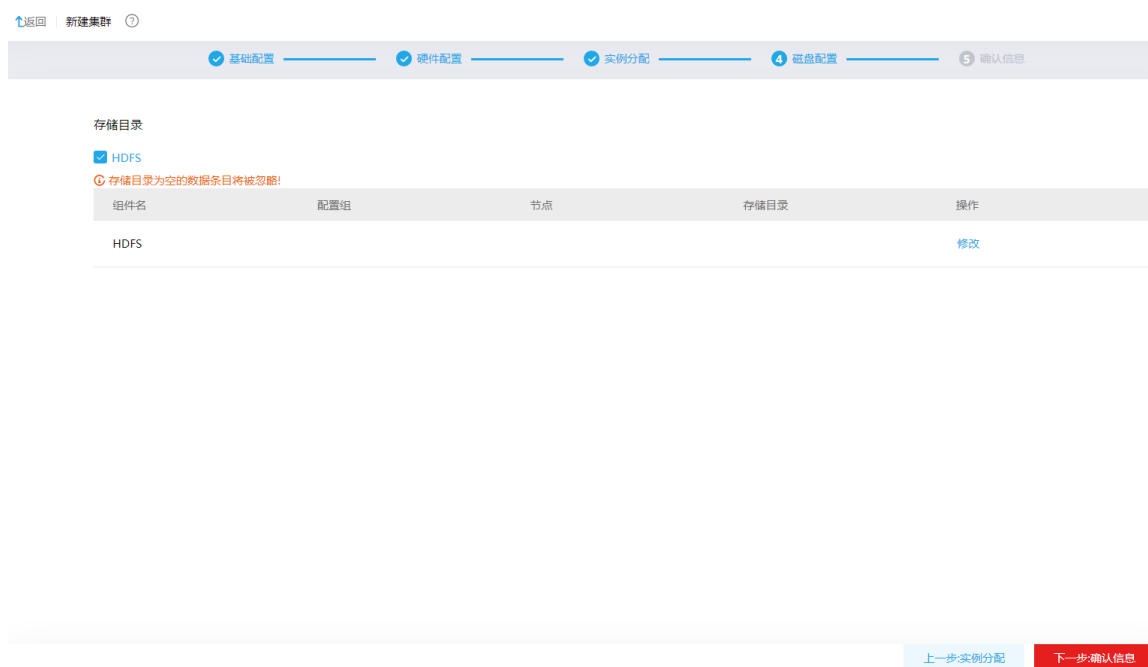
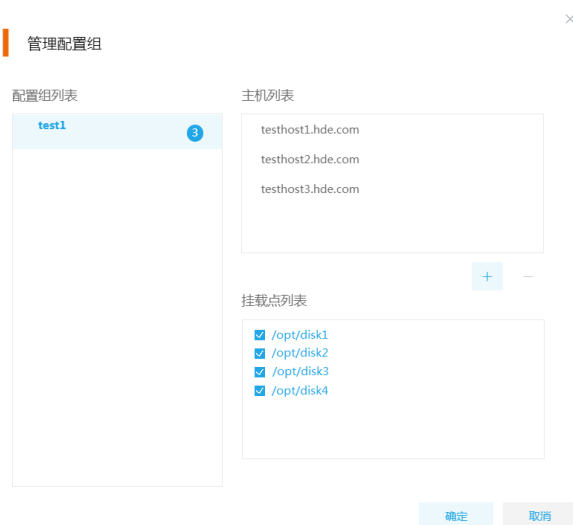


图4-7 管理配置组



**第五步：确认信息**，查看集群的基础配置、硬件配置、实例分配的详细信息，若检查配置无误可单击<确认信息并创建>按钮启动创建集群，若检查配置有误可返回上一步进行修改。

图4-8 确认信息

返回 新建集群

基础配置 硬件配置 实例分配 磁盘配置 确认信息

### 基础配置

集群名称: testcluster 集群类型: Hadoop

集群模式: 独立模式 集群超级用户: superuser

集群描述:

组件名	版本	描述
Hadoop	3.0.0	针对大数据集的分布式数据存储HDFS、高级计算MapReduce、...
ZooKeeper	3.4.5	分布式应用程序协调服务,为集群提供一致性服务
Hive	2.1.1	建立在Hadoop上的数据仓库框架,提供HQL语言进行数据离线...
Spark2	2.4.0	基于内存的分布式计算框架,提供批量处理、流式计算、SQL以及...

Kerberos认证: 开启

审计日志: 开启

权限与密码管理: 开启

组件日志: 开启

存储类型: HDFS

### 硬件配置

高可用: 开启

Master实例: 10.121.65.94:testhost1.hde.com, 10.121.65.95:testhost2.hde.com

Core实例: 10.121.65.96:testhost3.hde.com

### 实例分配

组件名	进程名	Master	Core
INFRA_SOLR	INFRA_SOLR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HDFS	DATANODE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HDFS	NFS_GATEWAY	<input type="checkbox"/>	<input type="checkbox"/>
HDFS	JOURNALNODE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HDFS	NAMENODE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TEZ	TEZ_CLIENT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HBASE	HBASE_MASTER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HBASE	PHOENIX_QUERY_SERVER	<input type="checkbox"/>	<input checked="" type="checkbox"/>
YARN	NODEMANAGER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
YARN	TIMELINE_READER	<input type="checkbox"/>	<input checked="" type="checkbox"/>
YARN	APP_TIMELINE_SERVER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
YARN	RESOURCEMANAGER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RANGER_KMS	RANGER_KMS_SERVER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
KNOX	KNOX_GATEWAY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RANGER	RANGER_ADMIN	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RANGER	RANGER_USERSYNC	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HIVE	HIVE_SERVER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HIVE	HIVE_METASTORE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LOGSEARCH	LOGSEARCH_LOGFEEDER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LOGSEARCH	LOGSEARCH_SERVER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SPARK2	SPARK2_THRIFTSERVER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SPARK2	LIVY2_SERVER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SPARK2	SPARK2_JOBHISTORYSERVER	<input type="checkbox"/>	<input checked="" type="checkbox"/>

### 磁盘配置

组件名	配置组	节点	存储目录
HDFS	test1	testhost1.hde.com, testhost2.hde.com, testhost3.hde.com	/opt/disk1, /opt/disk2, /opt/disk3, /opt/disk4

上一步磁盘配置 确认信息并创建

(5) 创建集群启动后，会跳转至集群列表页面，等待一段时间集群即可创建完成。

## 4.5.2 新建 Elasticsearch 集群

---



注意

- 新建集群前需要提前对节点数量（是否配置专有 Master 实例或 Client 实例）、是否开启安全管理、是否开启高可用等进行规划。
  - 新建集群时，若没有开启安全管理和高可用，则后续在使用过程中将再也无法开启。
  - 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。
- 

新建 Elasticsearch 集群的步骤如下：

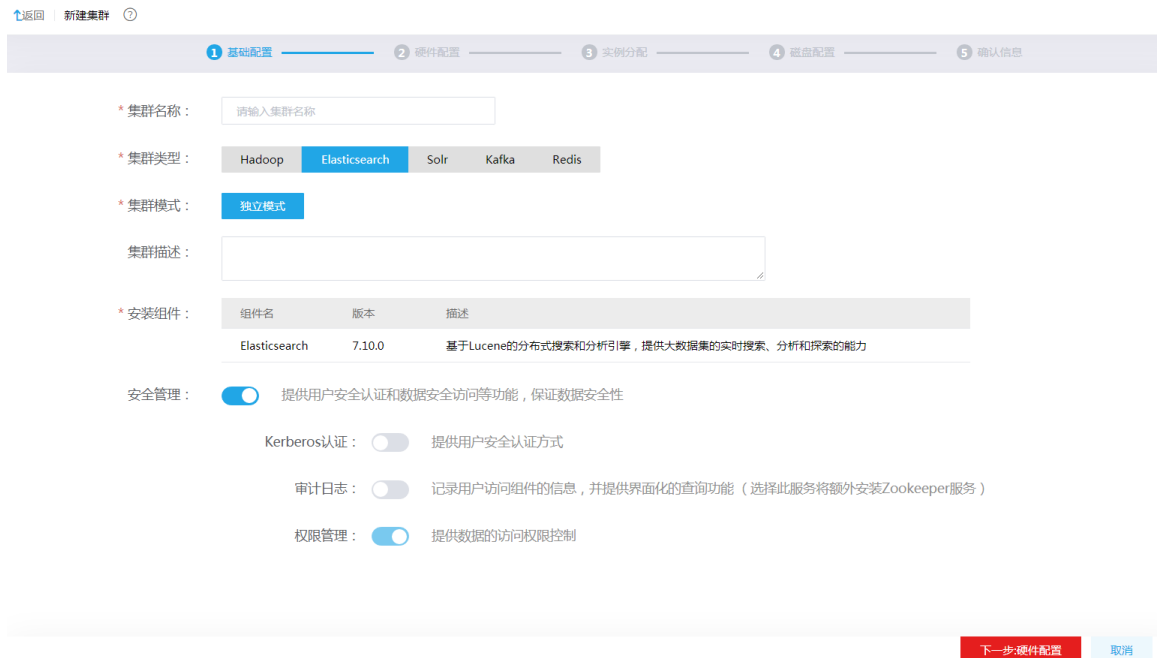
- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击<新建集群>按钮，跳转至新建集群页面。
- (3) 输入集群名称，选择集群类型为 Elasticsearch，即可开始新建 Elasticsearch 集群。
- (4) 新建 Elasticsearch 集群包括 3 个配置步骤，根据提示配置对应参数项的值，如下：

**第一步：基础配置**，参数说明如下：

- 集群名称：自定义输入符合命名规则的集群名称。
- 集群类型：选择 Elasticsearch 类型。
- 集群模式：Elasticsearch 集群仅支持独立模式。
- 集群描述：自定义添加集群的描述信息，以便于快速了解集群相关信息。
- 安装组件：已缺省配置选择 Elasticsearch。
- 安全管理：可选择是否开启安全管理。若选择开启，则同时提供 Kerberos 认证、审计日志、权限管理功能，提供用户安全认证和数据安全访问等功能，保证数据安全性。
  - Kerberos 认证：选择集群是否开启 Kerberos 认证，Kerberos 认证可以提供用户安全认证方式功能。
  - 审计日志：选择集群是否开启审计日志。审计日志可以记录用户访问组件的信息，并提供界面化的查询功能。
  - 权限管理：开启安全管理时默认开启权限管理（不支持关闭），提供数据的权限访问控制。



图4-9 基础配置



**第二步：硬件配置，参数说明如下：**

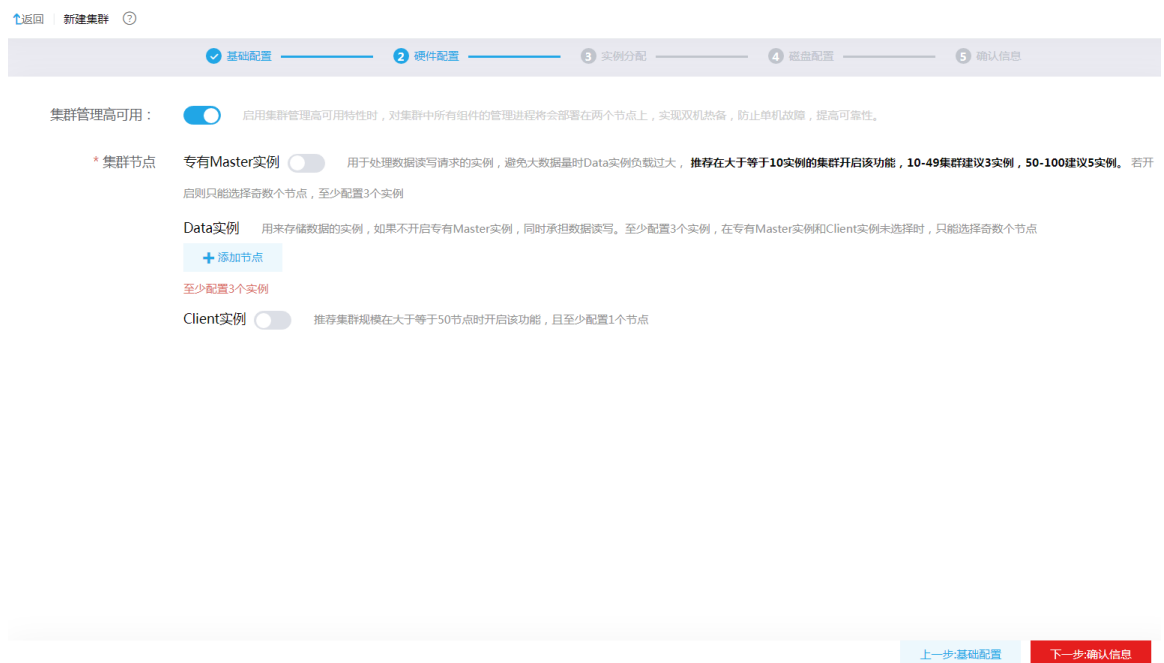
- **高可用：**选择集群管理是否开启高可用。若选择开启，则组件的管理进程将同时部署到两个节点上，实现双机热备；若未开启高可用，则存在单机故障的风险。创建集群时，缺省开启高可用。
- **集群节点：**创建集群时，集群节点包含多种类型，详情请参见[表 4-10](#)。此时，Elasticsearch 集群可选择是否开启专有 **Master** 实例或 **Client** 实例。

表4-10 集群节点说明

节点类型	是否必选	选型说明	描述
专有Master实例	可选	<p>用于处理数据读写请求的实例，可避免大数据量时Data实例负载过大。若开启专有Master实例，则集群的主节点将在专有Master实例中选出，主节点只管理集群的元数据信息，不存储数据。</p> <p><b>【说明】</b>建议在大于等于10实例的集群中开启该功能，且10~49实例的集群建议配置3个专有Master实例，50~100实例的集群建议配置5个专有Master实例</p>	<p>若配置专有Master实例，则实例个数至少配置3个，且只能配置奇数个</p>
Data实例	必选	<p>用来存储数据的实例。如果集群不开启专有Master实例，则Data实例同时承担数据读写请求</p>	<p>在生产环境中，Data实例的个数需要根据实际数据量大小或计算需求等情况进行规划</p> <ul style="list-style-type: none"> <li>● 未开启专有 Master 实例时，</li> </ul>

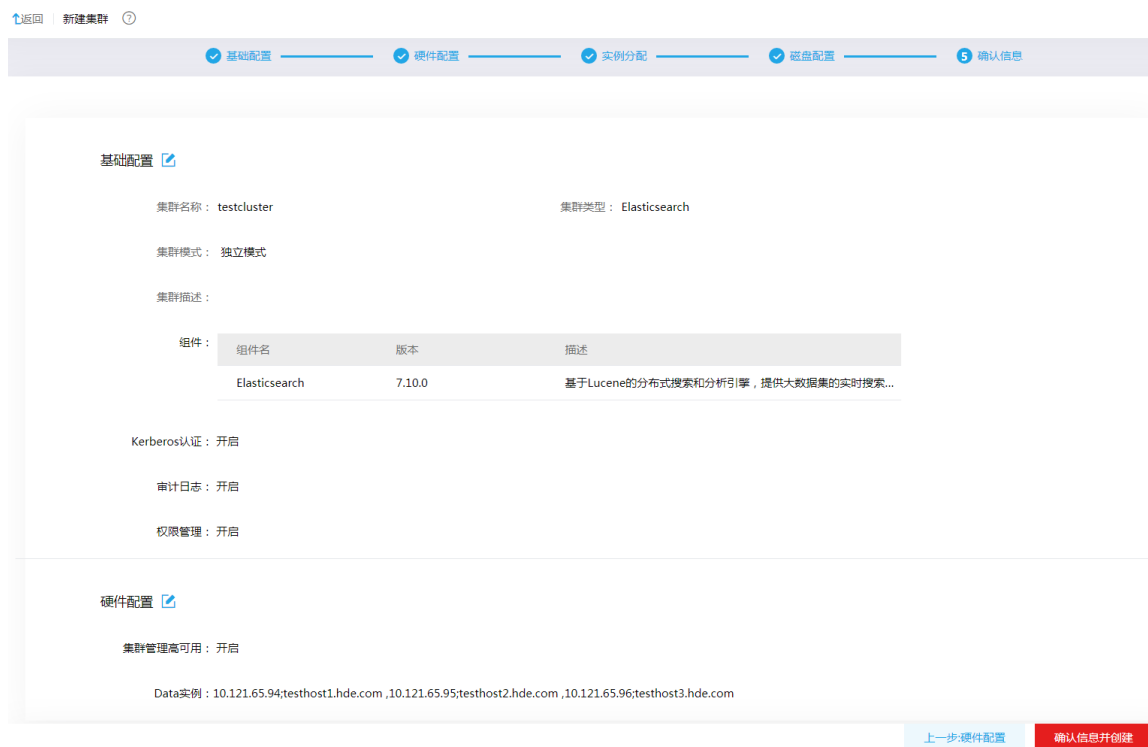
节点类型	是否必选	选型说明	描述
			<p>Data 实例至少配置 3 个。不配置专有 Master 实例和 Client 实例时，Data 实例的节点个数只能为奇数</p> <ul style="list-style-type: none"> <li>若开启专有 Master 实例时，Data 实例个数根据实际需求进行配置即可</li> </ul>
Client实例	可选	<p>用于对读写请求进行负载均衡的实例。Client实例既不参与主节点选举，也不存储数据，仅负责转发读写请求</p> <p>【说明】建议在大于等于50实例的集群中开启该功能，且至少配置1个节点</p>	若配置Client实例，则实例个数至少配置1个

图4-10 硬件配置



**第三步：确认信息**，查看集群的基础配置、硬件配置的详细信息，若检查配置无误可单击<确认信息并创建>按钮启动创建集群，若检查配置有误可返回上一步进行修改。

图4-11 确认信息



(5) 创建集群启动后，会跳转至集群列表页面，等待一段时间集群即可创建完成。

### 4.5.3 新建 Solr 集群



注意

- 新建集群前需要提前对节点数量、是否开启安全管理、是否开启高可用等进行规划。
- 新建集群时，若没有开启安全管理和高可用，则后续在使用过程中将再也无法开启。
- 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。

新建 Solr 集群的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击<新建集群>按钮，跳转至新建集群页面。
- (3) 输入集群名称，选择集群类型为 Solr，即可开始新建 Solr 集群。
- (4) 新建 Solr 集群包括 3 个配置步骤，根据提示配置对应参数项的值，如下：

**第一步：基础配置**，参数说明如下：

- 集群名称：自定义输入符合命名规则的集群名称。
- 集群类型：选择 Solr 类型。
- 集群模式：Solr 集群仅支持独立模式。
- 集群描述：自定义添加集群的描述信息，以便于快速了解集群相关信息。
- 安装组件：已缺省配置选择 Zookeeper、Solr。

- 安全管理：可选择是否开启安全管理。若选择开启，则同时提供 Kerberos 认证、审计日志、权限管理功能，提供用户安全认证和数据安全访问等功能，保证数据安全性。
  - Kerberos 认证：Kerberos 认证可以提供用户安全认证方式功能。开启安全管理时默认开启 Kerberos 认证（不支持关闭）。
  - 审计日志：选择集群是否开启审计日志。审计日志可以记录用户访问组件的信息，并提供界面化的查询功能。
  - 权限管理：开启安全管理时默认开启权限管理（不支持关闭），提供数据的权限访问控制。

图4-12 基础配置

↑返回 | 新建集群

1 基础配置 | 2 硬件配置 | 3 实例分配 | 4 磁盘配置 | 5 确认信息

\* 集群名称：

\* 集群类型： Hadoop Elasticsearch Solr Kafka Redis

\* 集群模式： 独立模式

集群描述：

\* 安装组件：

组件名	版本	描述
ZooKeeper	3.4.5	分布式应用程序协调服务，为集群提供一致性服务
Solr	7.4.0	基于Lucene的高性能全文搜索引擎，具备强大的搜索和近实时的索引能力

安全管理：  提供用户安全认证和数据安全访问等功能，保证数据安全性

Kerberos认证：  提供用户安全认证方式

审计日志：  记录用户访问组件的信息，并提供界面化的查询功能

权限管理：  提供数据的访问权限控制

下一步:硬件配置 | 取消

**第二步：硬件配置，参数说明如下：**

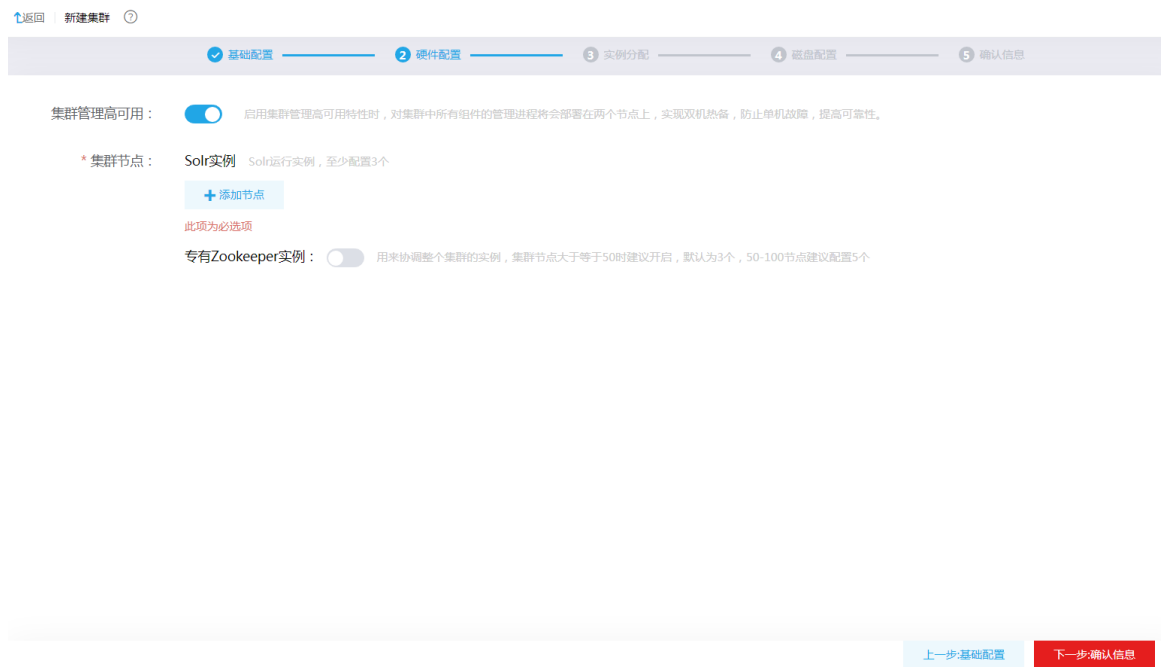
- 高可用：选择集群管理是否开启高可用。若选择开启，则组件的管理进程将同时部署到两个节点上，实现双机热备；若未开启高可用，则存在单机故障的风险。创建集群时，缺省开启高可用。
- 集群节点：创建集群时，集群节点包含多种类型，详情请参见[表 4-11](#)。此时，Solr 集群可选择是否开启专有 Zookeeper 实例。

表4-11 集群节点说明

节点类型	是否必选	选型说明	描述
Solr实例	必选	Solr运行实例	实例个数至少配置3个
专有 Zookeeper 实例	可选	用来协调整个集群的实例 【说明】建议在大于等于50实例的集群中开启该功能，且50~100节点建议配置5个	若配置Zookeeper专有实例，则实例个数至少配置3个，且只能配置奇数个 【说明】 • 若未配置 Zookeeper 专有实例，则

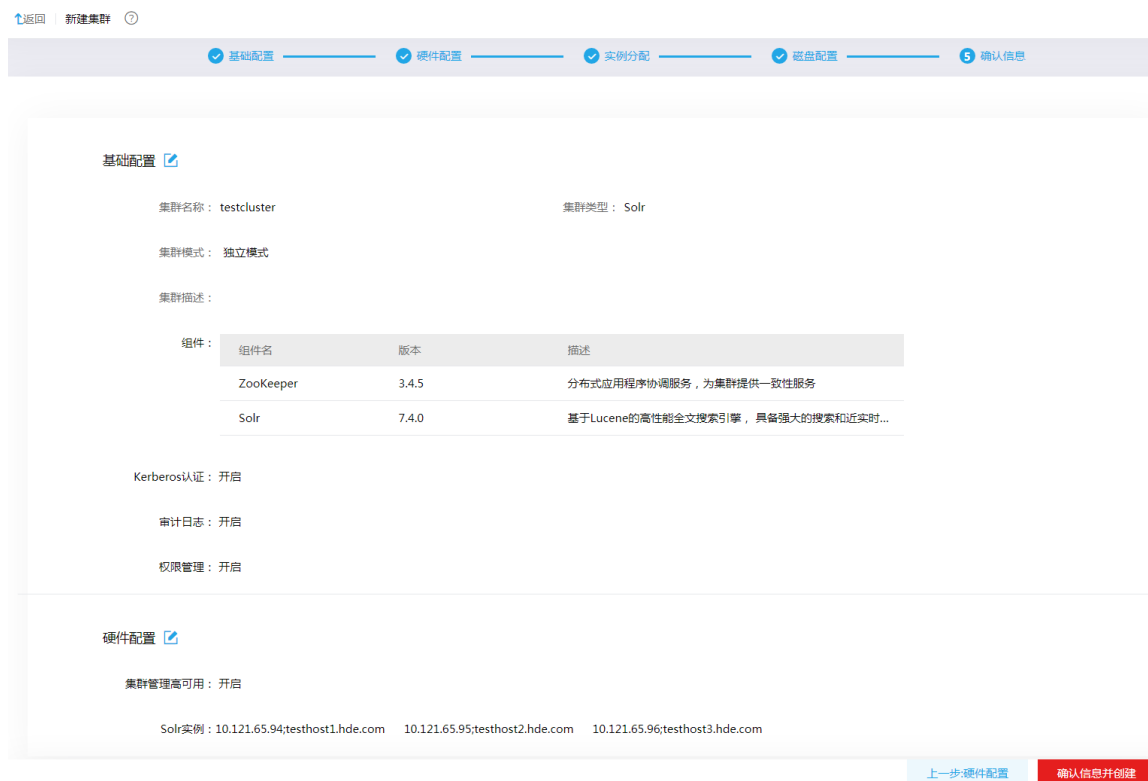
节点类型	是否必选	选型说明	描述
			Zookeeper 与 Solr 部署在相同节点上 <ul style="list-style-type: none"> <li>若配置 Zookeeper 专有实例，则 Zookeeper 与 Solr 分开部署</li> </ul>

图4-13 硬件配置



**第三步：确认信息**，查看集群的基础配置、硬件配置的详细信息，若检查配置无误可单击<确认信息并创建>按钮启动创建集群，若检查配置有误可返回上一步进行修改。

图4-14 确认信息



(5) 创建集群启动后，会跳转至集群列表页面，等待一段时间集群即可创建完成。

#### 4.5.4 新建 Kafka 集群

##### 注意

- 新建集群前需要提前规划集群模式，且同时需要提前对节点数量、是否开启安全管理、是否开启高可用等进行规划。
- 新建集群时，若没有开启安全管理和高可用，则后续在使用过程中将再也无法开启。
- 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。

新建 Kafka 集群的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击<新建集群>按钮，跳转至新建集群页面。
- (3) 输入集群名称，选择集群类型为 Kafka，即可开始新建 Kafka 集群。
- (4) 新建 Kafka 集群包括 3 个配置步骤，根据提示配置对应参数项的值，如下：

**第一步：基础配置**，参数说明如下：

- 集群名称：自定义输入符合命名规则的集群名称。
- 集群类型：选择 Kafka 类型。
- 集群模式：选择新建集群的模式，包括独立模式和租户模式两种。

- 集群描述：自定义添加集群的描述信息，以便于快速了解集群相关信息。
- 安装组件：已缺省配置选择 Zookeeper、Kafka。
- 安全管理：独立集群可选择是否开启安全管理。若选择开启，则同时提供 Kerberos 认证、审计日志、权限管理功能，提供用户安全认证和数据安全访问等功能，保证数据安全性。租户集群缺省开启安全管理功能（不支持关闭）。
  - Kerberos 认证：Kerberos 认证可以提供用户安全认证方式功能。开启安全管理时默认开启 Kerberos 认证（不支持关闭）。
  - 审计日志：选择集群是否开启审计日志。审计日志可以记录用户访问组件的信息，并提供界面化的查询功能。
  - 权限管理：开启安全管理时默认开启权限管理（不支持关闭），提供数据的权限访问控制。

图4-15 基础配置

基础配置

\* 集群名称：

\* 集群类型： Hadoop Elasticsearch Solr **Kafka** Redis

\* 集群模式： **独立模式** 租户模式

集群描述：

组件名	版本	描述
ZooKeeper	3.4.5	分布式应用程序协调服务，为集群提供一致性服务
Kafka	2.7.2	高吞吐量的分布式消息队列系统，具有出色的性能和可靠性

安全管理： 提供用户安全认证和数据安全访问等功能，保证数据安全性

Kerberos认证： 提供用户安全认证方式

审计日志： 记录用户访问组件的信息，并提供界面化的查询功能

权限管理： 提供数据的访问权限控制

下一步:硬件配置 取消

**第二步：硬件配置，参数说明如下：**

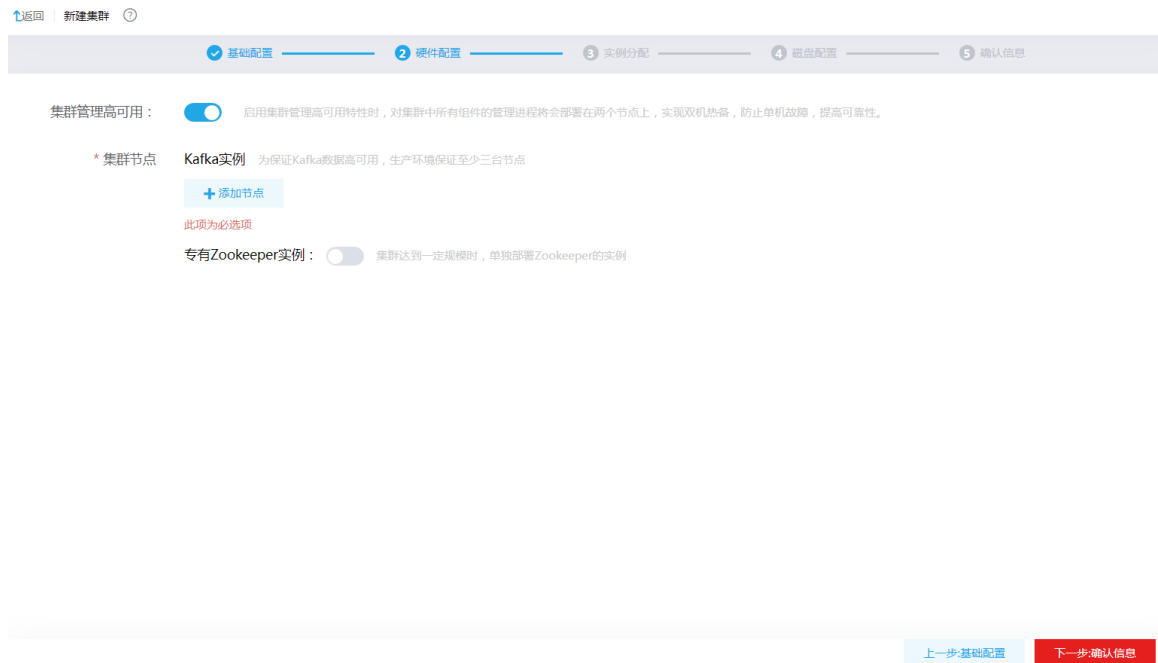
- 高可用：选择集群管理是否开启高可用。若选择开启，则组件的管理进程将同时部署到两个节点上，实现双机热备；若未开启高可用，则存在单机故障的风险。创建集群时，缺省开启高可用。
- 集群节点：创建集群时，集群节点包含多种类型，详情请参见表 4-12。此时，Kafka 集群可选择是否开启专有 Zookeeper 实例。

表4-12 集群节点说明

节点类型	是否必选	选型说明	描述
Kafka实例	必选	Kafka运行实例	为保证Kafka数据高可用，实例个数至少配置3个
专有	可选	用来协调整个集群的实	若配置Zookeeper专有实例，则实例个数至少配置3

节点类型	是否必选	选型说明	描述
Zookeeper实例		例，集群达到一定规模时，可单独部署Zookeeper的实例	个，且只能配置奇数个 <b>【说明】</b> <ul style="list-style-type: none"> <li>若未配置 Zookeeper 专有实例，则 Zookeeper 与 Kafka 部署在相同节点上</li> <li>若配置 Zookeeper 专有实例，则 Zookeeper 与 Kafka 分开部署</li> </ul>

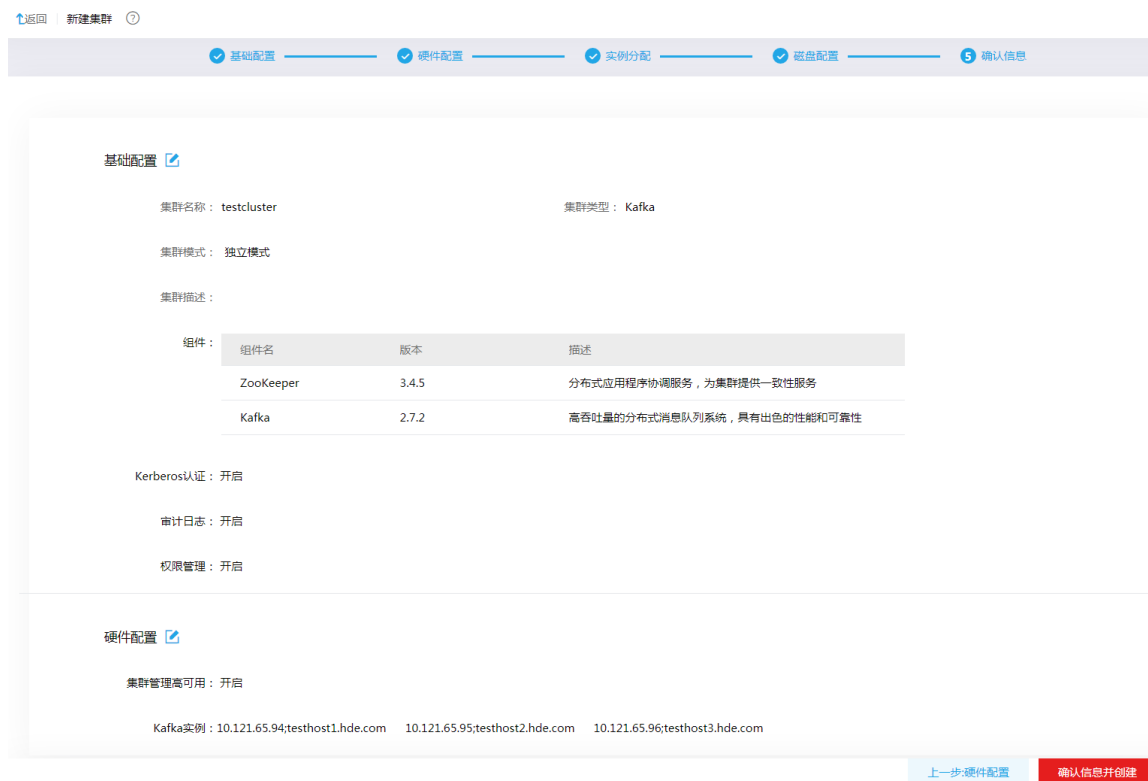
图4-16 硬件配置



**第三步：确认信息**，查看集群的基础配置、硬件配置的详细信息，若检查配置无误可单击<确认信息并创建>按钮启动创建集群，若检查配置有误可返回上一步进行修改。



图4-17 确认信息



(5) 创建集群启动后，会跳转至集群列表页面，等待一段时间集群即可创建完成。

### 4.5.5 新建 Redis 集群



#### 注意

- 新建集群前需要提前对节点数量、是否开启高可用等进行规划。
- Redis 支持单机模式和集群模式，其中：Redis 单机模式的集群节点数为 1，Redis 集群模式的集群节点数大于等于 3（且为奇数）。
- Redis 单机模式不支持开启高可用，Redis 集群模式必须开启高可用。
- 新建集群时，若没有开启安全管理，则后续在使用过程中将再也无法开启。
- 大数据集群创建完成以后，集群中的主机节点不允许修改主机名。

新建 Redis 集群的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击<新建集群>按钮，跳转至新建集群页面。
- (3) 输入集群名称，选择集群类型为 Redis，即可开始新建 Redis 集群。
- (4) 新建 Redis 集群包括 3 个配置步骤，根据提示配置对应参数项的值，如下：

**第一步：基础配置**，参数说明如下：

- 集群名称：自定义输入符合命名规则的集群名称。

- 集群类型：选择 **Redis** 类型。
- 集群模式：**Redis** 集群仅支持独立集群模式。
- 集群描述：自定义添加集群的描述信息，以便于快速了解集群相关信息。
- 安装组件：已缺省配置选择 **Redis**。
- 安全管理：可选择是否开启安全管理。若选择开启，表示开启权限管理（不开启 Kerberos、不开启审计日志），提供用户权限控制功能，保证数据安全性。
- 实例副本数：配置 **Redis** 集群备份模式，支持单副本和双副本两种方式。
  - 单副本机制，单机模式下没有备用节点实时同步数据，各个实例之间相互独立。集群模式下存在一主一从的副本机制，主从实例间数据实时同步，能够在主库出现故障的时候自动进行主备切换。
  - 双副本机制，单机模式下没有备用节点实时同步数据，各个实例之间相互独立。集群模式下存在一主两从的副本机制，主从实例间数据实时同步，能够在主库出现故障的时候自动进行主备切换。

图4-18 基础配置

The screenshot shows a configuration wizard for creating a cluster. The current step is 'Basic Configuration' (基础配置). The wizard has five steps: 1. Basic Configuration, 2. Hardware Configuration, 3. Instance Allocation, 4. Disk Configuration, and 5. Confirmation Information. The configuration options are as follows:

- 集群名称:** 请输入集群名称 (Input field)
- 集群类型:** Hadoop, Elasticsearch, Solr, Kafka, **Redis** (Selected)
- 集群模式:** **独立模式** (Selected)
- 集群描述:** (Text area)
- 安装组件:**

组件名	版本	描述
Redis	6.2.1	基于内存的分布式缓存数据库，满足高性能读写的业务需求
- 安全管理:**  提供用户权限控制功能，保证数据安全性
- 实例副本数:** **单副本** (Selected), 双副本

At the bottom right, there are two buttons: '下一步:硬件配置' (Next Step: Hardware Configuration) and '取消' (Cancel).

**第二步：硬件配置，参数说明如下：**

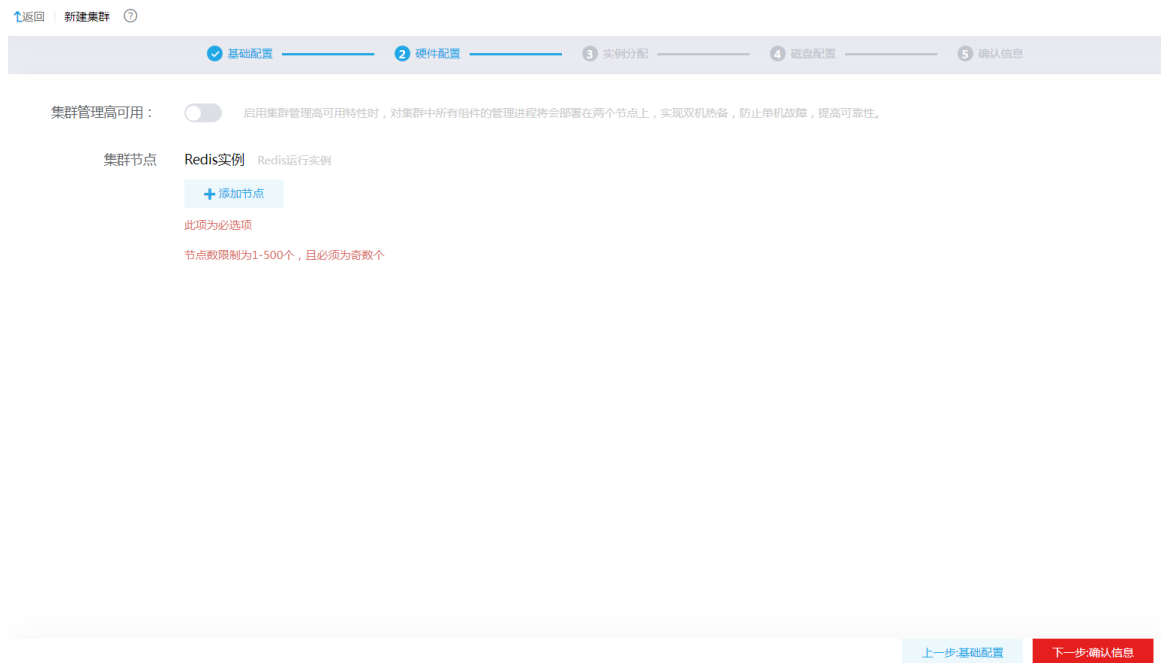
- 高可用：选择集群管理是否开启高可用。单机模式下，缺省关闭集群管理高可用；集群模式下，缺省开启集群管理高可用，此时组件的管理进程将同时部署到两个节点上，实现双机热备，提高可靠性。
- 集群节点：创建集群时，集群节点详情请参见[表 4-13](#)。

表4-13 集群节点说明

节点类型	是否必选	选型说明	描述
Redis实例	必选	Redis运行实例	Redis支持单机模式和集群模式，其中：

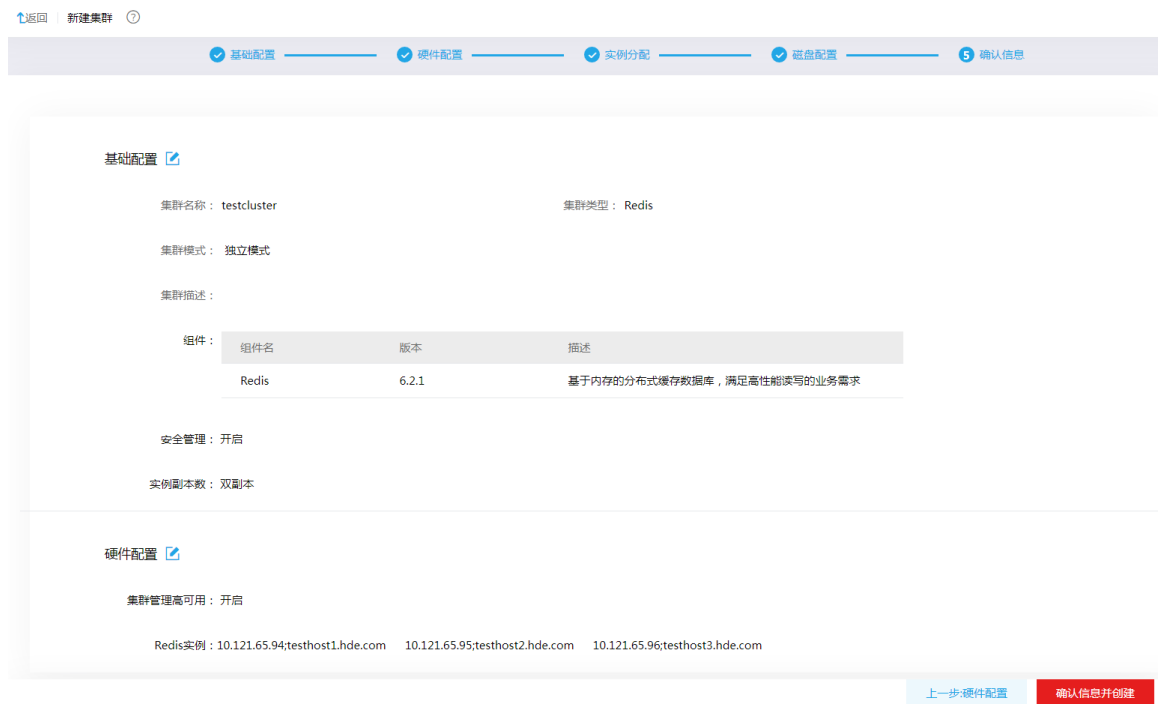
节点类型	是否必选	选型说明	描述
			<ul style="list-style-type: none"> <li>当实例个数为 1 时，为 Redis 单机模式，此时不支持开启高可用，且一旦创建不可横向扩容</li> <li>当实例个数大于等于 3 时，为 Redis 集群模式，此时必须开启高可用，且节点数量必须为奇数个</li> </ul>

图4-19 硬件配置



**第三步：确认信息**，查看集群的基础配置、硬件配置的详细信息，若检查配置无误可单击<确认信息并创建>按钮启动创建集群，若检查配置有误可返回上一步进行修改。

图4-20 确认信息



(5) 创建集群启动后, 会跳转至集群列表页面, 等待一段时间集群即可创建完成。

# 5 大数据平台相关配置

## 5.1 软件授权

大数据集群或数据工厂部署完成后，可在 180 天内试用所有功能。超过试用期限后，需要获取 License 授权才能正常使用。

关于大数据平台 License 授权详情请参见《UniCloud 大数据平台 License 支持情况说明》。

### 5.1.1 License 远程授权操作

大数据平台需通过 License Server 获取授权，在进行大数据平台的 License 配置时，需提前完成 License 远程授权相关操作，详情请参见《UniCloud 大数据平台 License 使用 FAQ》。

### 5.1.2 配置大数据集群的 License

访问管理页面，成功连接到 License Server 的客户端后，大数据集群可以向 License Server 请求授权并将请求结果展示在页面上。

配置大数据集群 License 的步骤如下：

- (1) 访问管理页面，在顶部导航栏选择[系统]菜单项进入系统管理页面。
- (2) 在左侧导航树中选择[软件授权]进入软件授权页面。
- (3) 软件授权页面显示“License Server 配置”和“授权信息”，下面对这两部分进行详细介绍。

图5-1 软件授权



#### o License Server 配置

单击<配置>按钮可进行 License Server 配置，配置完成后可连接到对应的 License Server 客户端自动获取授权信息，且可查看状态信息、授权服务 IP 地址、授权服务端口信息。

License Server 配置参数项如下：

- 授权服务 IP 地址：License Server 客户端所在主机的 IP 地址。
- 授权服务端口：License Server 授权服务端口号，缺省为“5555”。
- 客户端名称：License Server 中设置的客户端名称。
- 客户端密码：License Server 中设置的客户端名称对应的密码。



- License 配置时填写的用户名和密码必须为在 License Server 中创建的客户端的名称和密码。
- 进行 License Server 配置时，单击<确定>按钮后，若无法连接到 License Server，会弹出错误提示信息，此时则需要检查输入是否正确或者 License Server 是否正常运行。
- 当已使用的 License Server 信息（比如：IP 地址、客户端名称等）有变化时，可执行更新配置的操作重新获取授权信息。

---

#### ○ 授权信息

管理页面和 License Server 定期通信更新授权状态，授权信息栏可查看当前系统中授权使用情况。当 License Server 上的授权信息变更时，单击<同步>按钮可手动刷新当前授权信息列表。部分参数说明如下：

- 授权名称：从 License Server 获取到的授权名称。单击>图标可查看此条授权的详细信息（比如：产品条码、授权类型、授权数量、总授权天数、剩余授权时间等）。
- 获得授权：从 License Server 获取到的授权状态。对于数量型授权，该值为实际获取的授权数量；对于功能型授权，该值为 YES（获取授权成功）或 NO（获取授权失败）。
- 使用授权：对于数量型授权，该值表示已经使用的授权数量；对于功能型授权，该值为空。



对于大数据集群的数量型授权，当可用授权不足时，会影响“新建集群”、“集群扩容”等操作的进行。

---

## 5.2 添加浏览器安全证书



### 说明

- 由于大数据平台管理系统仅支持通过 **https** 协议访问，所以需要为浏览器添加授权证书以保证安全访问。如果没有执行此步骤，在浏览器访问时，选择“继续前往（不安全）”，也可以访问大数据平台管理系统。
- UniCloud BDP 证书在下载前和证书安装后，均需要强制清除浏览器缓存及重启浏览器。
- 大数据平台管理系统访问不受信，若安装证书后仍然不受信处理方法请参见 [9.15](#) 章节。

如果浏览器中以前没有导入过 UniCloud BDP 证书或需要更新 UniCloud BDP 证书时，均需要获取最新的证书。

以 Chrome 95 浏览器为例，添加安全证书的步骤如下：

- (1) 在浏览器中输入大数据平台管理系统访问地址，如 [图 5-2](#) 所示，弹出连接不安全的提示，此时建议在浏览器中导入 UniCloud BDP 的安全证书。

图5-2 登录大数据平台管理系统（不安全）



### 您的连接不是私密连接

攻击者可能会试图从 **10.121.65.106** 窃取您的信息（例如：密码、通讯内容或信用卡信息）。[了解详情](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

[隐藏详情](#)

[返回安全连接](#)

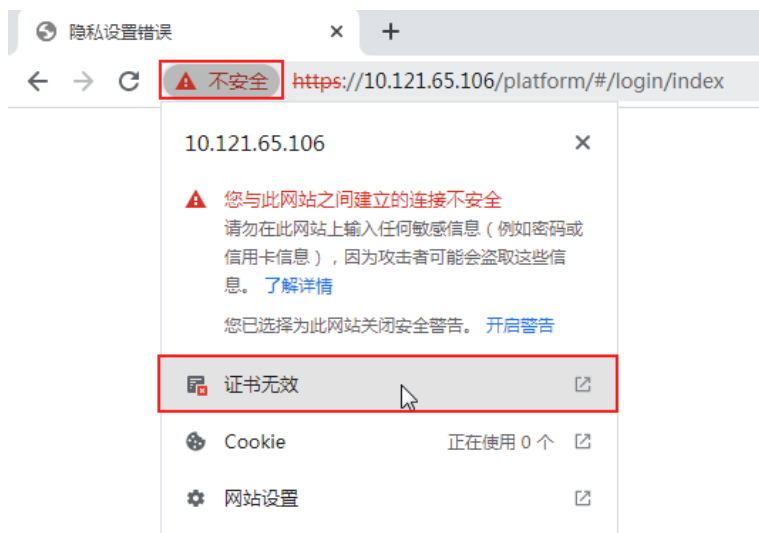
此服务器无法证明它是 **10.121.65.106**；您计算机的操作系统不信任其安全证书。出现此问题的原因可能是配置有误或您的连接被拦截了。

[继续前往10.121.65.106（不安全）](#)

- (2) 下载 UniCloud BDP 安全证书

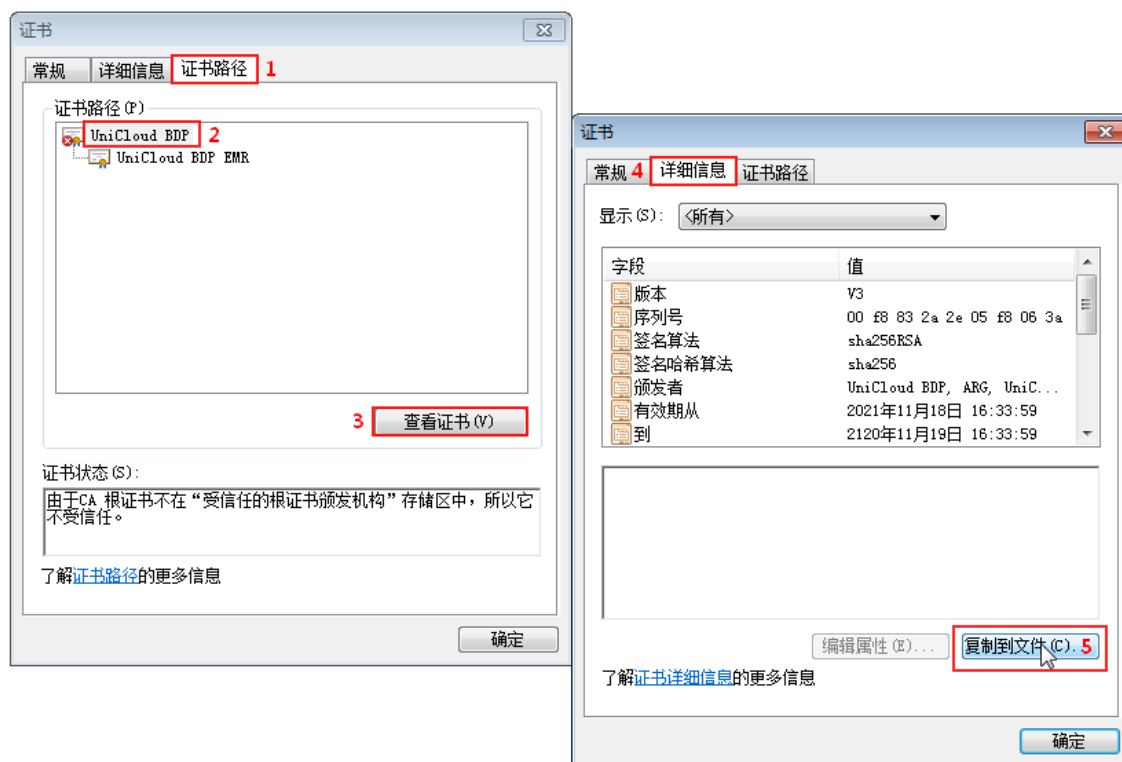
- a. 在浏览器中输入大数据平台管理系统访问地址的位置，查看“不安全”的网站信息，单击“证书（无效）”链接出现证书弹窗，如 [图 5-3](#) 所示。

图5-3 查看访问不安全详请



- b. 在证书弹窗中，查看[证书路径]页签，选择根证书，并单击<查看证书>按钮出现该证书弹窗。在该证书弹窗中选择“详细信息”页签，单击<复制到文件>按钮进入证书导出向导弹窗，如图 5-4 所示。

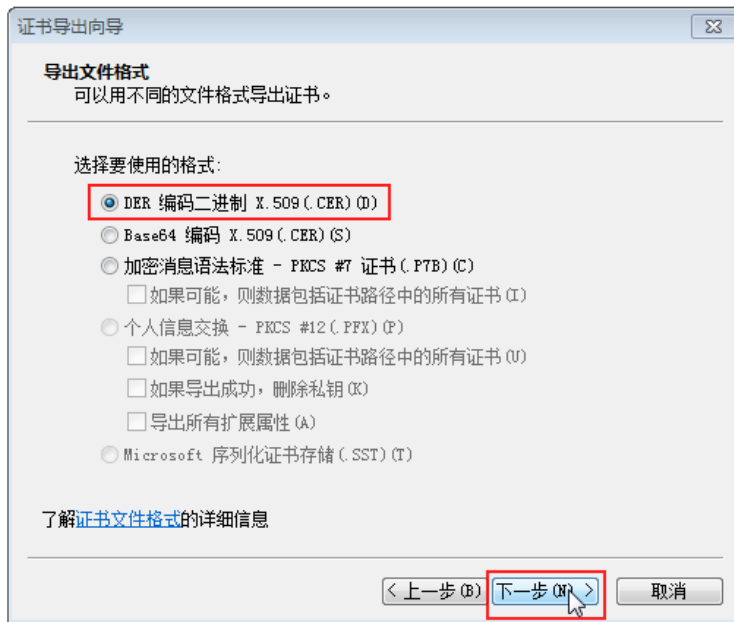
图5-4 查看 UniCloud BDP 根证书详细信息并导出



- c. 在证书导出向导弹窗中，单击<下一步>选择导出文件格式，勾选“DER 编码二进制 X.509(.CER) (D)”，如图 5-5 所示。

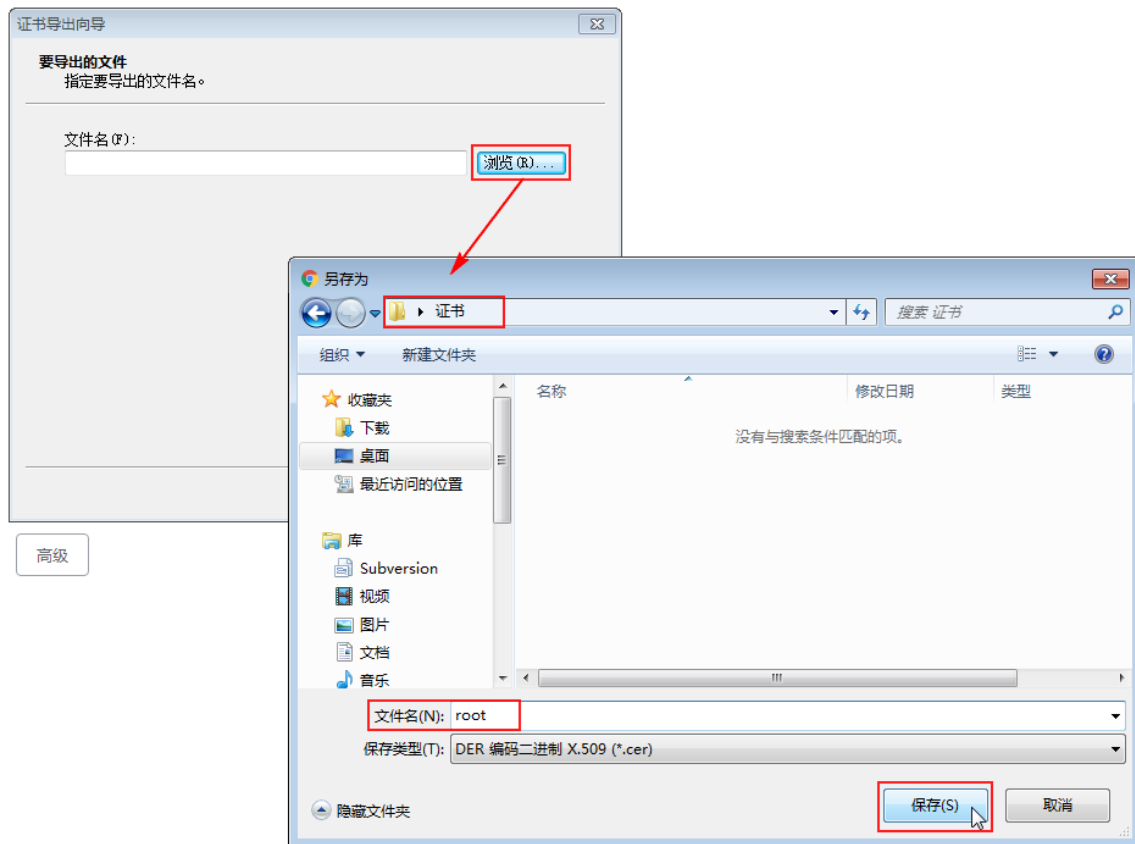


图5-5 配置证书导出后的文件格式



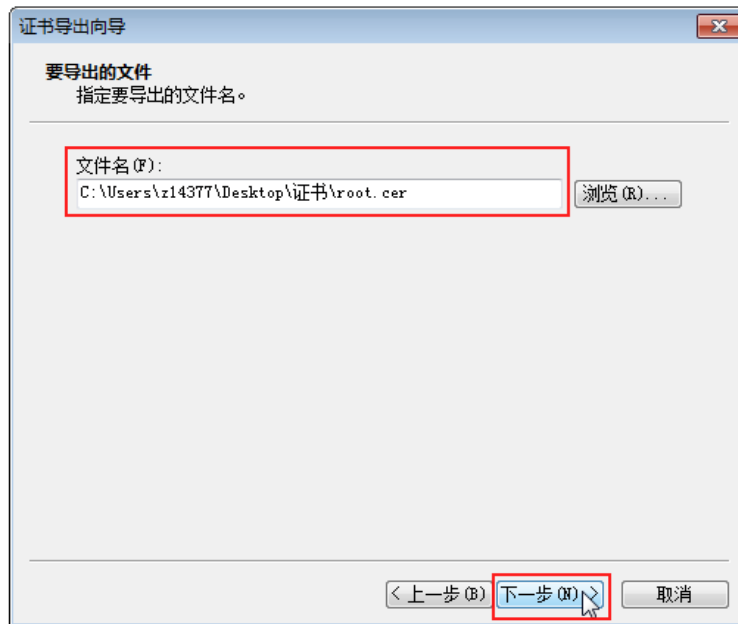
- d. 继续单击<下一步>按钮, 配置要导出的文件名。单击<浏览>按钮, 选择文件的存储位置并输入文件名称, 配置完成后单击<保存>按钮, 如图 5-6 所示。

图5-6 配置要导出的文件名



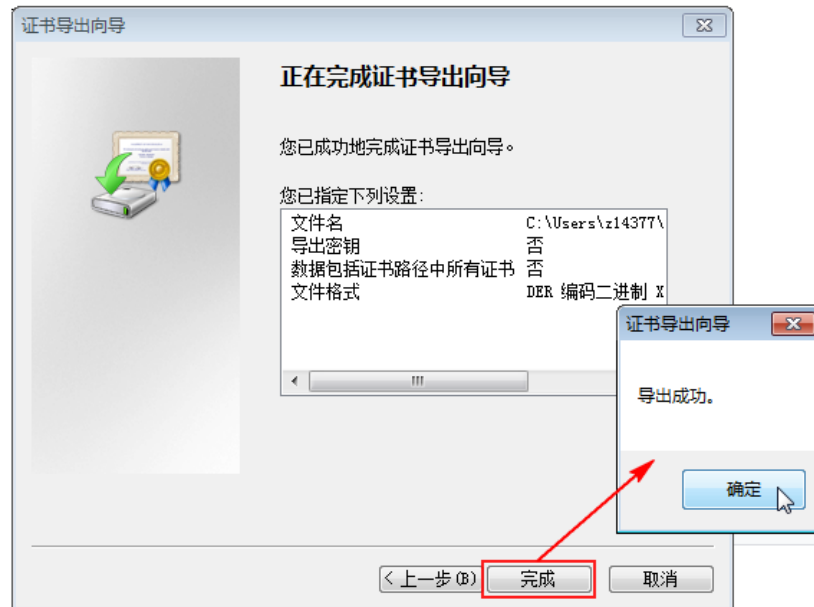
- e. 返回证书导出向导窗口后, 单击<下一步>即可启动证书导出, 若图 5-7 所示。

图5-7 启动证书导出



f. 导出完成后单击<完成>按钮提示“导出成功”，如图 5-8 所示。

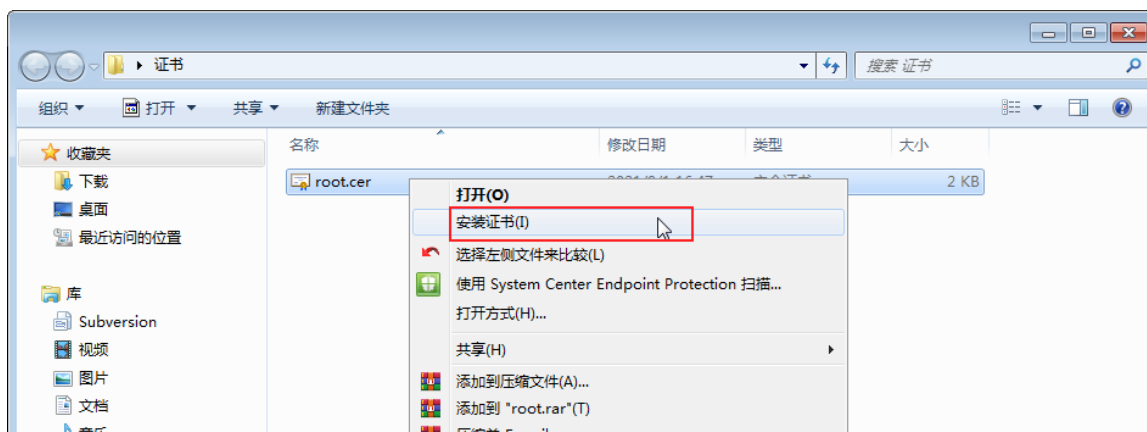
图5-8 UniCloud BDP 证书导出完成



### (3) 导入 UniCloud BDP 安全证书

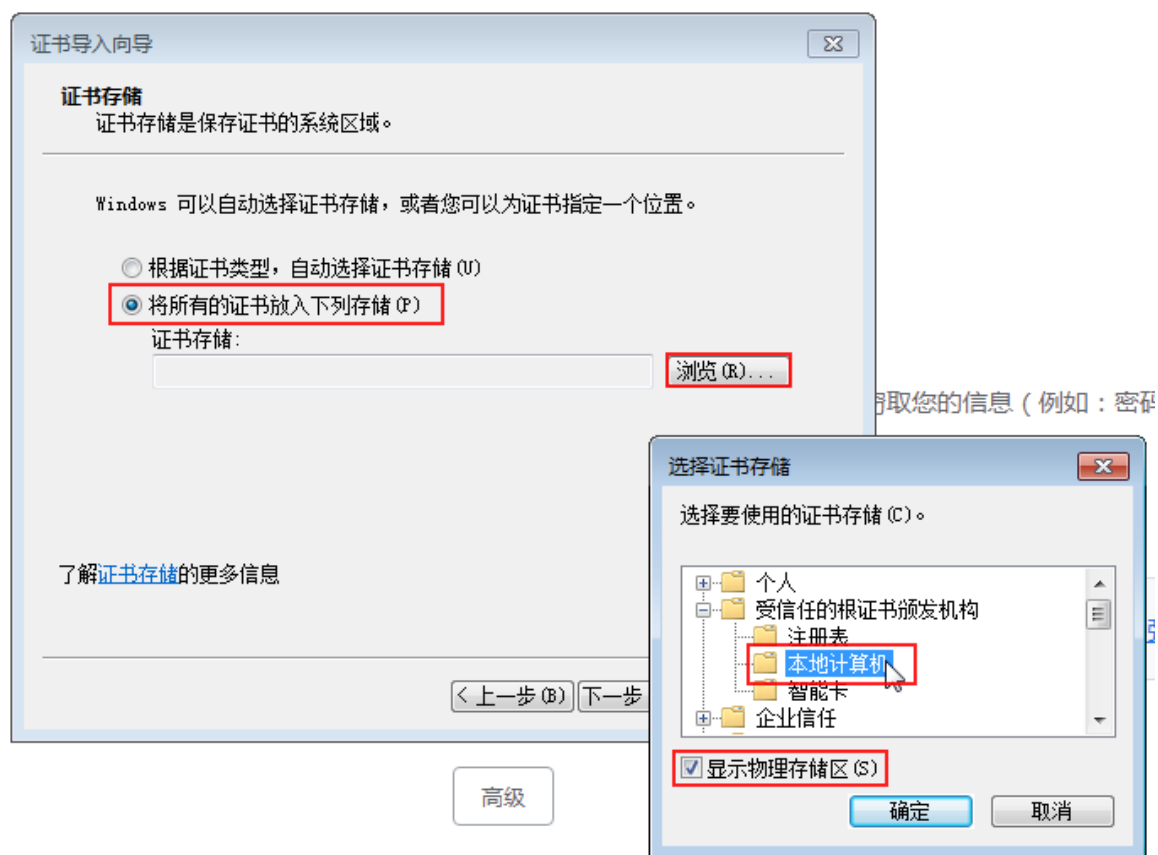
a. 选中导出的根证书，右键选择“安装证书”，进入证书导入向导，如图 5-9 所示。

图5-9 启动安装根证书



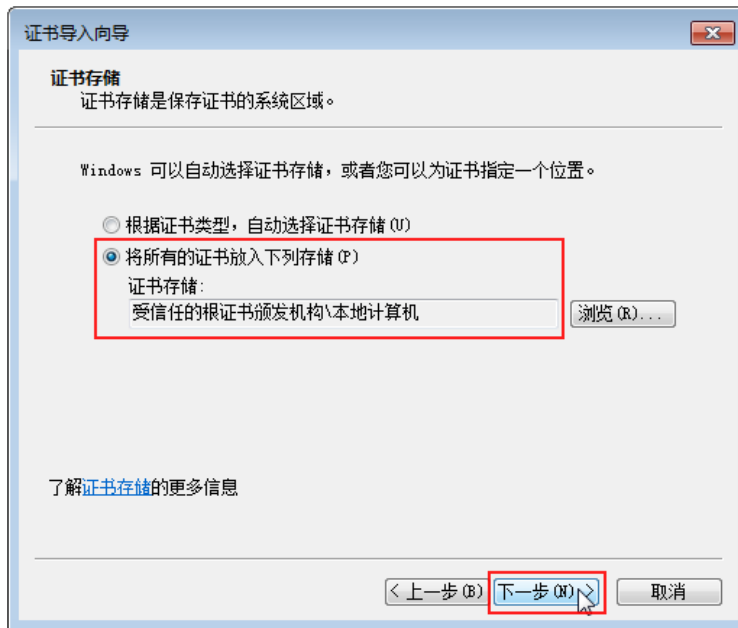
- b. 在证书导入向导弹窗中，单击<下一步>选择证书存储。勾选“将所有的证书放入下列存储”，单击<浏览>按钮进入选择证书存储弹窗，勾选“显示物理存储区”后，选择受信任的根证书颁发机构下的本地计算机，单击<确定>按钮完成选择，如图 5-10 所示。

图5-10 配置证书存储



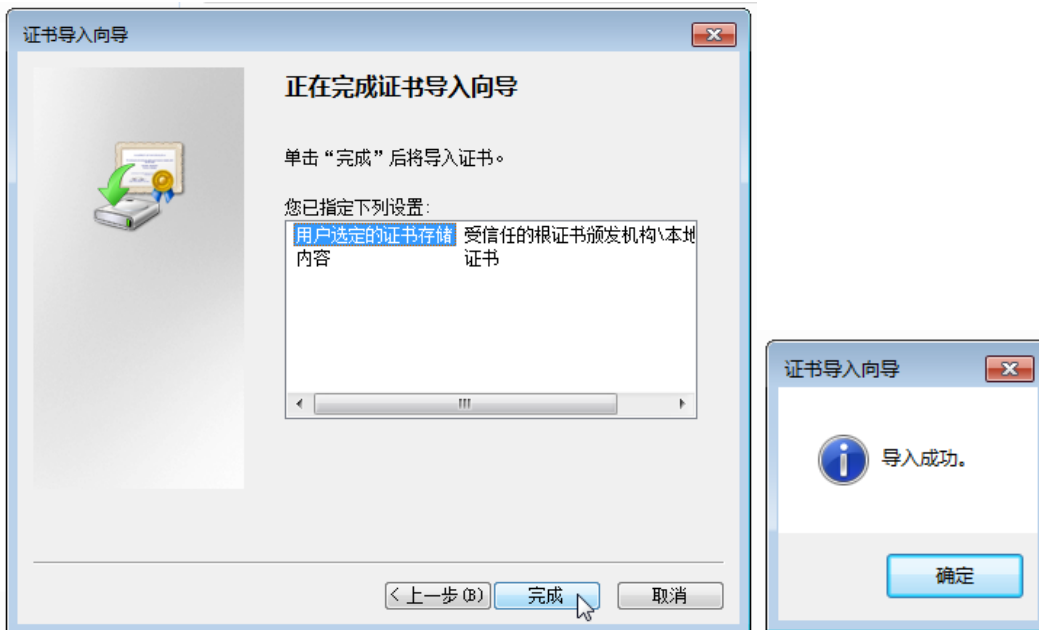
- c. 返回证书导入向导窗口后，单击<下一步>即可启动证书导入，如图 5-11 所示。

图5-11 启动证书导入



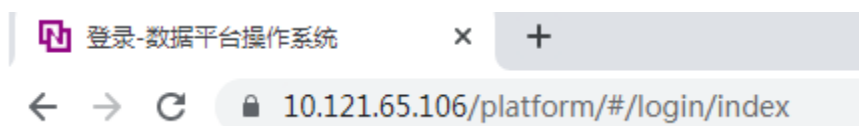
d. 导入完成后单击<完成>按钮提示“导入成功”，如图 5-12 所示。

图5-12 UniCloud BDP 证书导入完成



(4) UniCloud BDP 证书导入成功后，重新启动浏览器，输入大数据平台管理系统访问地址，即可实现受信任的访问进入，如图 5-13 所示。

图5-13 登录大数据平台管理系统（安全）



# 6 集群创建后检查

大数据集群创建完成后，进入集群管理页面，可检查集群、主机和组件的当前情况，以确保大数据集群状态正常。

## 6.1 集群巡检



说明

- 集群巡检支持对集群、主机、组件进行检查，系统内置了多种检查项和检查规则，详情请以实际报告中的检查项为准。
- 同一时期集群仅支持执行一次巡检操作，巡检执行结束后支持在线查看报告或导出报告，报告展示每个检查项的巡检结果、结果状态和修复建议等。

访问管理页面，检查某集群的当前状态，步骤如下：

- (1) 在运维管理的左侧导航树中选择[巡检管理]，进入巡检管理页面。
- (2) 在巡检管理页面，支持手动巡检和自动巡检两种方式，其中：
  - 手动巡检：单击<手动巡检>按钮，会立即对集群执行巡检操作。
  - 自动巡检：单击<自动巡检>按钮，通过“动态巡检”配置项可选择集群是否开启自动巡检功能。若选择为集群开启自动巡检，则需要配置自动巡检的重复策略和调度时间，配置完成后单击<确定>按钮，集群即可启动自动巡检功能，在指定时间对集群执行巡检操作。
- (3) 集群执行巡检操作时，巡检内置多个检查项，依次执行直至全部执行结束后，才可查看或导出巡检报告。

图6-1 集群巡检

#	巡检项	巡检状态	巡检结果	启动方式	开始时间	结束时间	操作
1	sharedevtest_check_2022-04-25-14-58	检查中	----	手动巡检	2022-04-25 14:58:...		导出报告 终止 删除
2	sharedevtest_check_2022-04-25-14-58	已完成	告警	手动巡检	2022-04-25 14:58:...	2022-04-25 14:58:...	查看报告 导出报告 删除
3	sharedevtest_check_2022-04-25-10-06	已完成	告警	手动巡检	2022-04-25 10:06:...	2022-04-25 10:07:...	查看报告 导出报告 删除

- (4) 集群巡检结束后，各个巡检项的结果状态需在巡检报告中查看，巡检报告支持在线查看或导出查看，如图 6-2 和图 6-3 所示。根据本次集群巡检项的结果状态进行综合分析后可得到巡检结果，分为以下 4 种情况：
  - 合格：所有巡检项结果状态全部合格
  - 建议：巡检项结果状态中含有至少 1 条建议，且无告警和错误
  - 告警：巡检项结果状态中含有至少 1 条告警，且无错误

- 错误：巡检项结果状态中含有至少 1 条错误

图6-2 在线查看巡检报告

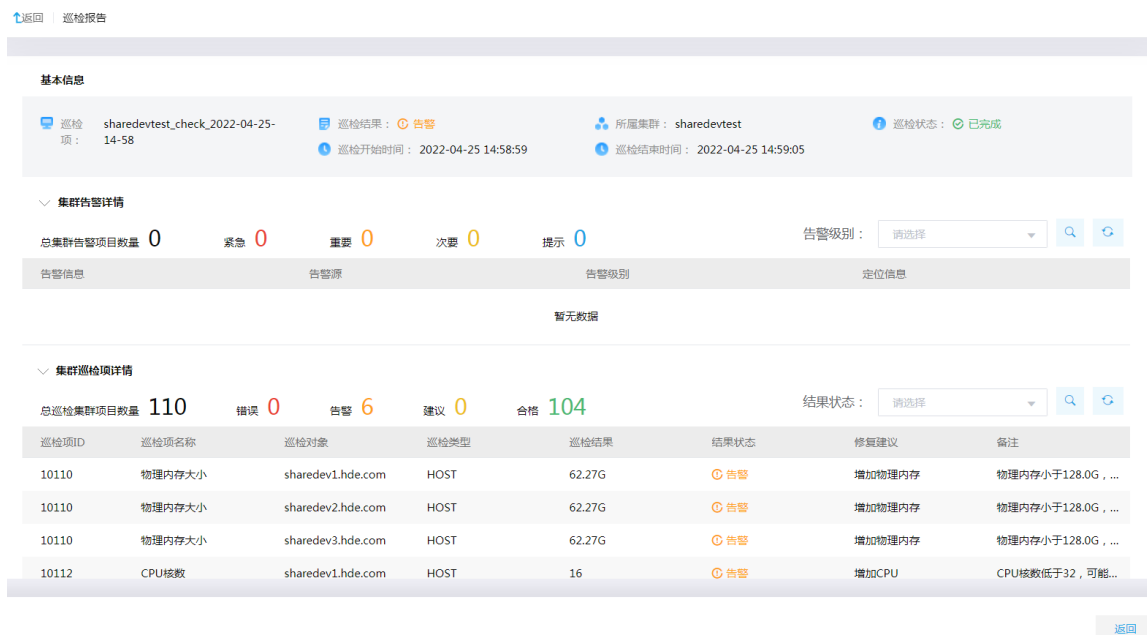


图6-3 导出查看巡检报告

巡检对象	巡检时间	巡检项id	巡检项名称	巡检结果	结果状态	修复建议	备注
HOST: sharedev1.hde.com	2022-04-25 14:59:03	10110	物理内存大小	62.27G	WARN	增加物理内存	物理内存小于128.0G, 可能影响服务性能
HOST: sharedev2.hde.com	2022-04-25 14:59:03	10110	物理内存大小	62.27G	WARN	增加物理内存	物理内存小于128.0G, 可能影响服务性能
HOST: sharedev3.hde.com	2022-04-25 14:59:04	10110	物理内存大小	62.27G	WARN	增加物理内存	物理内存小于128.0G, 可能影响服务性能
HOST: sharedev1.hde.com	2022-04-25 14:59:03	10112	CPU核数	16	WARN	增加CPU	CPU核数低于32, 可能影响服务性能
HOST: sharedev2.hde.com	2022-04-25 14:59:03	10112	CPU核数	16	WARN	增加CPU	CPU核数低于32, 可能影响服务性能
HOST: sharedev3.hde.com	2022-04-25 14:59:04	10112	CPU核数	16	WARN	增加CPU	CPU核数低于32, 可能影响服务性能

总览 集群 主机 组件

## 6.2 检查主机

### 6.2.1 主机运行状态检查

访问管理页面，检查某集群中主机运行状态的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击某集群名称可跳转至对应的集群详情页面。
- (3) 在集群详情页面的[主机]页签，可查看集群中的主机列表及主机运行状态。检查范围包括：
  - 检查部署的大数据集群中所有主机节点是否都在主机列表中。

- 检查所有主机状态是否都正常。
  - 若运行状态为“在线”，则表示主机正常。
  - 若运行状态为“离线”，则表示主机已关机或存在其他故障，需要检查。

图6-4 主机运行状态检查

主机名	主机状态	主机IP	主机用户	CPU...	CPU使用率	内存使用率	磁盘使用率	机架	操作
★ sharedev1.h...	● 在线	10.121.68...	root	16	8%	43.31G/62.27G	69.56% 58.42G/767.19G	7.61%	/default-r... 删除
☆ sharedev2.h...	● 在线	10.121.68...	root	16	7.11%	36.5G/62.27G	58.61% 45.97G/767.19G	5.99%	/default-r... 删除
sharedev3.h...	● 在线	10.121.68...	root	16	6.55%	32.66G/62.27G	52.45% 39.84G/767.19G	5.19%	/default-r... 删除
sharedev4.h...	● 在线	10.121.68...	root	16	6.23%	16.67G/126.27G	13.2% 70.31G/767.19G	9.16%	/default-r... 删除

第1-4条, 共 4 条 << < 1 / 1 > >> 10条/页

## 6.2.2 主机健康检查



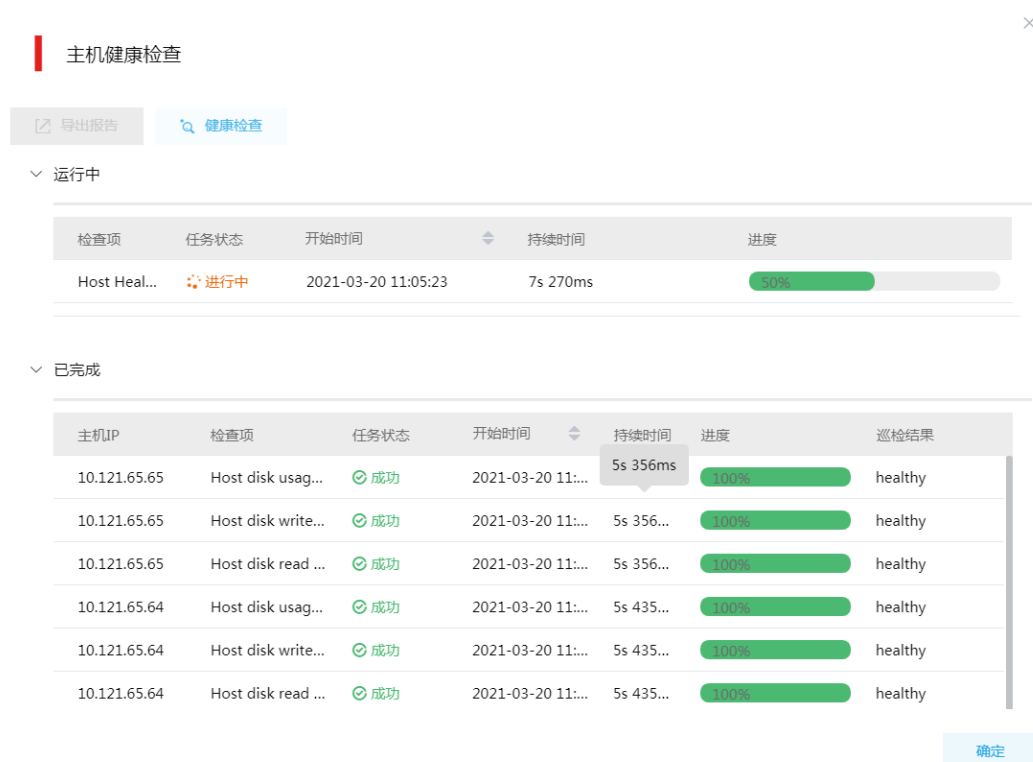
### 说明

- 主机健康检查支持检查主机内存、磁盘使用率、磁盘读写速率、以及偏移量等，详情请以实际报告为准。
- 同一时期主机仅支持执行一次健康检查操作，主机健康检查执行结束后支持导出报告（仅支持导出最近一次健康检查的报告）。

访问管理页面，检查某集群中所有主机的健康状态，步骤如下：

- (1) 在顶部导航树中选择[集群管理]，进入集群管理页面。
- (2) 在集群管理页面，选择[集群列表]页签，单击某集群名称可跳转至对应的集群详情页面。
- (3) 在集群详情页面右上角的集群操作下拉框中选择<主机健康检查>按钮，弹出主机健康检查窗口。
- (4) 单击<健康检查>按钮，启动主机健康检查操作。主机健康检查内置多个检查项，依次执行直至全部执行结束后，才可导出健康检查报告。
- (5) 单击<确定>按钮即可关闭主机健康检查窗口。

图6-5 主机健康检查



## 6.3 检查组件

### 6.3.1 组件存储路径检查

根据现场磁盘分区方案和挂盘方案的不同，组件安装完成后，必须对各组件的数据目录配置结果进行检查，否则组件可能会使用异常。关于各组件的数据目录对应配置项的检查说明，详情请参见 [9.2](#) 章节。

### 6.3.2 组件运行状态检查

访问管理页面，检查某集群中组件运行状态的步骤如下：

- (1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。
- (2) 在集群列表页面，单击某集群名称可跳转至对应的集群详情页面。
- (3) 在集群详情页面的[组件]页签，选择业务组件或系统组件，可查看集群中的组件列表及组件运行状态。检查范围包括：
  - 检查部署的大数据集群中已安装的所有组件是否都在组件列表中。
  - 检查所有组件状态是否都正常。



图6-6 组件运行状态检查

业务组件	系统组件	
组件名	组件状态	操作
 HBASE	● 已启动	停止 重启 删除 组件检查 下载Client
 HDFS	● 已启动	停止 重启 组件检查 下载Client
 HIVE	● 已启动	停止 重启 删除 组件检查 下载Client
 KAFKA	● 已启动	开启 重启 删除 下载Client
 MAPREDUCE2	● 已启动	停止 重启 组件检查 下载Client
 SPARK2	● 已启动	停止 重启 删除 组件检查 下载Client
 TF7	● 已安装	重启 组件检查

### 6.3.3 组件检查

#### 说明

- 大数据集群中可以安装多种类型的大数据组件，支持执行组件检查操作，但是各个组件的检查方案不同，详情请参见大数据平台组件用户手册。
- 本章节以 HDFS 组件检查为例，介绍组件检查方法。

执行 HDFS 组件检查时，会向 HDFS 上传测试文件并检查 HDFS 文件系统的 UI 页面响应，同时检测 HDFS 相关进程的运行状态，若 HDFS 组件检查成功则表示向 HDFS 上传文件和页面响应正常，且各进程运行正常。

- (1) 组件检查的方式有以下三种，任选其一即可：
  - 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面，单击某集群名称可跳转至对应的集群详情页面。
    - 在集群详情页面选择[组件]页签，单击组件列表中某组件对应的<组件检查>按钮。
    - 在集群详情页面选择[组件]页签，单击组件列表中某组件名称进入组件详情页面，在右上角组件操作的下拉框中选择<组件检查>按钮。
  - 在组件管理的组件详情页面右上角组件操作的下拉框中选择<组件检查>按钮。
- (2) 然后在弹窗中进行确定后，即可对该组件进行检查。
- (3) 组件检查结束后，检查窗口中会显示组件检查成功或失败的状态。如图 6-7 所示，表示组件检查成功，可正常使用。

图6-7 组件检查



- (4) 组件检查结束后，在组件详情页面单击<操作历史>按钮，进入操作历史窗口。可查看“HDFS Service Check”组件操作执行的详细信息以及操作日志详情，根据操作日志可判断组件检查的具体情况。

图6-8 组件检查日志详情



# 7 关于集群配置的说明

## 7.1 访问管理



- 禁止直接在后台操作大数据平台管理节点、集群节点的防火墙规则。
- 对于融合部署的集群，若开启了防火墙，则在对应的大数据平台上新建其他集群时，需要将新集群规划的集群节点 IP 提前添加至白名单中，否则新建集群无法成功。

---

集群创建完成后，且集群状态为“运行中”时，在大数据平台管理系统的[运维管理/访问管理/防火墙管理]页面可对集群执行开启或关闭防火墙等相关管理操作。

在生产环境中，开启或关闭防火墙均为高危操作，会对集群的访问产生影响，请谨慎操作。关于防火墙管理的更多详情和注意事项请参见产品在线联机帮助。

## 7.2 禁用/启用root权限



- 禁用或启用 root 权限的功能，仅是针对 root 用户的 ssh 权限，并不会删除 root 用户或更改 root 用户的其他权限。
- 执行禁用 root 权限操作后，系统会自动在集群内所有主机上创建 sysadmin 用户，并为其配置 sudo 权限。
- 注意：部分集群操作必须以 root 用户执行（即 root 权限启用时），比如：系统升级、组件升级。

---

集群创建完成后，且集群状态为“运行中”时，主机节点会被大数据集群占用，为避免主机 root 用户误操作带来的安全风险，根据需要使用，在大数据平台管理系统的[运维管理/访问管理/root 用户管理]页面可对集群内主机执行禁用或启用 root 权限的操作。关于 root 权限的更多操作详情和注意事项请参见产品在线联机帮助。

## 7.3 配置组件快速链接

---



注意

- 在大数据集群中，部分组件支持快速链接功能，可跳转至对应的 UI 页面查看组件详情。
  - 不同组件支持的快速链接数量和类别不同，详情请以实际页面为准。
  - 对于 Kafka 组件，访问其快速链接 Kafka Eagle 的方式与其他组件均不同，即：无论集群是否开启 Kerberos，访问 Kafka 的快速链接时，均只能通过用户名（admin）和密码（CloudOS5#DE3@KE）进行登录，其他用户名/密码均无法访问。
  - 对于 Elasticsearch 组件，访问其快速链接 Kibana 的方式与其他组件均不同，即：无论集群是否开启权限管理，均需要输入用户名和密码进行认证。当集群开启权限管理时，对于集群超级用户，可直接访问 Kibana；对于集群普通用户，需要拥有所有索引的“all”权限，才可访问 Kibana。
- 

大数据集群部署完成后，需要修改本地 hosts 文件，用以确保组件的快速链接页面通过域名访问能够顺利跳转。修改本地 hosts 文件的方法如下：

- (1) 登录大数据集群中任一节点，查看当前集群的 hosts 文件（Linux 环境下位置为/etc/hosts）。
- (2) 将集群的 hosts 文件信息添加到本地 hosts 文件中。若本地电脑是 Windows 环境，则 hosts 文件位于 C:\Windows\System32\drivers\etc\hosts，修改该 hosts 文件并保存。
- (3) 在本地 hosts 文件中配置主机域名信息完成后，此时访问组件（Kafka、Elasticsearch 除外）的快速链接：
  - 若集群没有开启 Kerberos 认证，则此时可直接跳转访问对应的 UI 页面。
  - 若集群开启了 Kerberos 认证，则需要输入用户名和密码进行认证（可以使用集群创建时填写的超级用户，也可以使用用户管理中创建的用户），然后才可跳转访问对应的 UI 页面。

## 7.4 日志管理

---



说明

- 新建大数据集群时，若没有开启“组件日志”，则集群不可使用[日志管理/组件日志]功能。若在新建集群时没有开启组件日志，则后续在使用过程中将再也无法开启，且一旦开启将再也无法关闭。
  - 新建大数据集群时，若没有开启“安全管理/审计日志”，则集群不可使用[日志管理/审计日志]功能。若在新建集群时没有开启审计日志，则后续在使用过程中将再也无法开启，且一旦开启将再也无法关闭。
  - [日志管理/日志配置]功能与创建集群时是否开启组件日志无关。
  - 关于日志管理模块功能的配置或使用详情请参见产品在线联机帮助系统。
- 

大数据平台管理系统的日志管理模块展示大数据平台中已部署的集群中产生的日志信息（包括组件日志和审计日志），支持对日志信息进行搜索，同时还可对集群中对应组件的日志存储目录等进行配置。

## 7.5 安全管理



说明

关于安全管理模块功能的配置或使用详情请参见产品在线联机帮助系统。

表7-1 开启安全管理后提供的功能说明

功能	说明
Kerberos认证	Kerberos认证可以提供用户安全认证方式功能。 【说明】关于Kerberos认证开启后，对使用的影响详情请参见 <a href="#">7.5.1 开启Kerberos</a>
审计日志	审计日志提供操作审计和密钥审计，并提供界面化的查询功能。 【说明】关于审计日志开启后，对使用的影响详情请参见 <a href="#">7.5.2 开启审计日志</a>
权限与密钥管理	权限与密钥管理可以提供数据的权限访问控制和HDFS密钥管理工具。 【说明】关于权限与密钥管理开启后，对使用的影响详情请参见 <a href="#">7.5.3 开启权限和密钥管理</a>

### 7.5.1 开启 Kerberos



注意

- 新建大数据集群时，Kerberos 认证一旦开启将再也无法关闭或卸载。
- 开启 Kerberos 后，业务端需要进行安全认证适配。所以在生产环境中，部署集群前，请务必确认清楚是否要开启 Kerberos。
- 独立集群可选择是否开启 Kerberos 认证。租户集群缺省开启 Kerberos 认证功能（不支持关闭）。

集群开启 Kerberos 认证后，可能受影响的操作如下：

- 对于租户集群，租户的用户需要通过认证才可使用租户中的组件资源。
- 对于独立集群，集群超级用户和普通用户在拥有相关权限的基础上，均需要通过认证才可访问集群。
- 访问集群中某组件的快速链接时，必须通过用户名/密码进行认证。
- 组件使用（管理/业务）方面的影响，详情请参见 UniCloud BDP 相关组件手册。

## 7.5.2 开启审计日志



注意

新建大数据集群时，若没有开启审计日志，则集群不可使用审计日志功能，且后续在使用过程中将再也无法开启。

大数据平台管理系统的[日志管理/审计日志]功能包括操作审计和密钥审计，其中：

- 操作审计页面展示访问 HDFS、YARN、HBase、Kafka、Hive 等组件的日志信息。
- 密钥审计页面展示对密钥的操作日志信息。

### 【示例】

操作审计提供某用户在某时刻以某种操作访问某组件上的某资源，以及访问是否通过的日志信息。比如：

- (1) [图 7-1](#) 中日志显示：2019-10-28 16:19:02，lining 用户在 10.121.36.22 机器上对 HBase 组件的命名空间 Inns1 执行删除操作，操作失败。

图7-1 操作审计日志

用户名	组件名	资源	访问类型	访问结果	客户端IP	创建时间
lining	hbase	Inns1:	deleteNamespace	Denied	10.121.36.22	2019-10-28 16:19:02

- (2) [图 7-2](#) 中日志显示：2019-10-29 19:39:22，keyadmin 用户在 10.121.65.244 机器上通过密钥 key 执行 getmetadata 操作，操作成功。

图7-2 密钥审计日志

用户名	密钥名	访问类型	访问结果	客户端IP	访问时间
keyadmin	key	getmetadata	Allowed	10.121.65.244	2019-10-29 19:39:22

## 7.5.3 开启权限和密钥管理

### 1. 权限管理



说明

- 新建大数据集群时，若没有开启权限与密钥管理，则集群不可使用角色管理功能。
- 新建大数据集群时，若没有开启权限与密钥管理，则后续在使用过程中将再也无法开启。
- 关于权限管理模块功能的配置或使用详情请参见产品在线联机帮助系统。

权限管理是安全管理的重要组成部分，在开启权限与密钥管理的集群中，权限基于角色进行统一管理，角色是权限的集合。一个角色可以同时拥有多个组件的资源权限，例如：HDFS 某些目录的权限、HBase 某个表的权限等。以角色作为权限集合的优势在于：

- 当多个用户对同一组件的同一资源有相同的权限时，只需要为这些用户绑定拥有该资源权限的角色，而不用分别为这些用户重复添加相同的权限。
- 对某一角色的权限进行修改后，所有绑定该角色的用户将会被统一修改权限，这样可以更加灵活方便的对用户进行权限管理。

当前版本提供面向 Hadoop 组件资源的统一权限管理平台，系统中仅部分组件支持权限控制，详情请以实际页面为准。

## 2. 密钥管理

---



- 新建大数据集群时，若没有开启权限与密钥管理，则集群不可使用密钥管理功能。
  - 新建大数据集群时，若没有开启权限与密钥管理，则后续在使用过程中将再也无法开启。
  - 在当前版本中，仅 HDFS 超级用户（hdfs）可创建加密区。
  - 关于密钥管理模块功能的配置或使用详情请参见产品在线联机帮助系统。
- 

密钥管理是将多个集群中的密钥进行统一管理，提供密钥的创建、删除、授权等操作。在 HDFS 中使用密钥创建加密区，可以实现对数据的加密功能。

密钥管理使用指导如[图 7-3](#)所示，流程说明如[表 7-2](#)所示。

图7-3 密钥管理使用指导

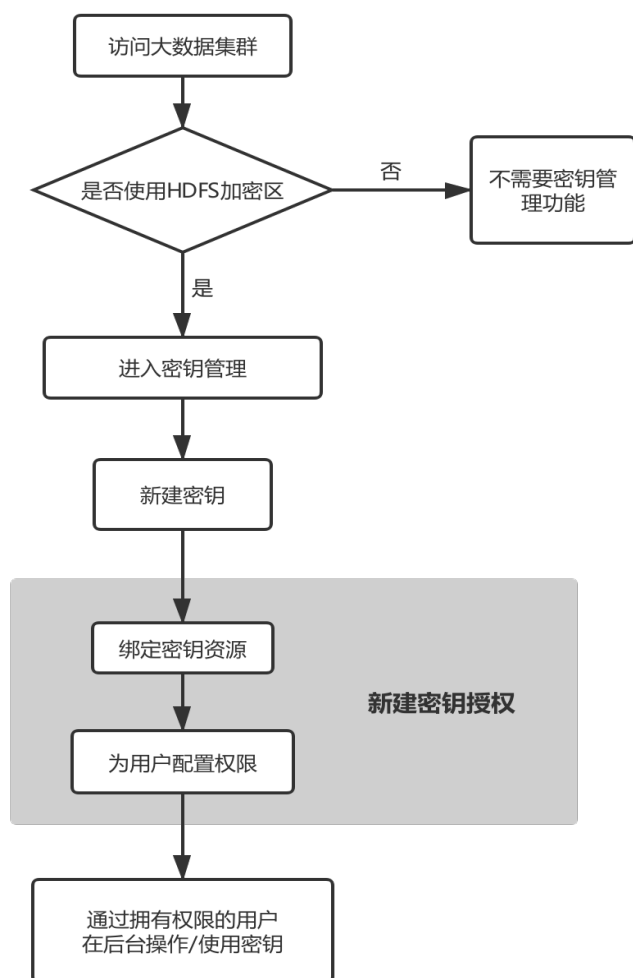


表7-2 密钥管理使用指导说明

步骤		说明
访问大数据集群		用户在后台访问大数据集群（示例用户user01）
是否使用HDFS加密区		若需要创建HDFS加密区（示例加密区/zone）存储需要加密的数据
进入密钥管理		则需要使用“密钥管理”功能
新建密钥		在[密钥管理/密钥]页签，为对应集群新增密钥（示例key01）
新建密钥授权	绑定密钥资源	新增密钥授权时，需要绑定密钥资源（示例密钥key01）
	为用户配置权限	新增密钥授权时，根据需要，可为不同用户配置不同权限（示例为用户user01绑定密钥key01，并为其授予解密加密区的权限）
通过拥有权限的用户在后台操作/使用密钥		拥有密钥权限的用户可在后台执行对应操作，比如通过密钥向加密区上传文件或查看加密文件



步骤	说明
	<p><b>【注意】</b>当前版本中，仅HDFS超级用户（hdfs）可创建加密区</p> <p>示例：hdfs用户可通过密钥key01创建加密区/zone。因用户user01已绑定解密加密区的权限，所以用户user01可通过密钥key01查看加密区/zone的里的文件</p>

## 7.6 租户管理



说明

关于租户管理模块功能的配置或使用详情请参见产品在线联机帮助系统。

多个租户之间共享一套集群，共享网络和集群资源，并且不同租户之间保证资源隔离。

- 新建租户

普通用户在自己创建的租户集群中申请租户时，无需审批，会直接触发新增租户的操作。普通用户在其他用户创建的租户集群中申请租户时，则需要走流程审批，待审批人审批通过后才能触发新增租户的操作。管理员用户新增租户时，无需审批，会直接触发新增租户的操作。

- 租户管理操作

普通用户在自己创建的租户集群中执行租户续期、资源扩缩容、配置 YARN 动态策略管理操作时，无需审批，会直接触发相关操作。普通用户在其他用户创建的租户集群中执行租户续期、资源扩缩容、配置 YARN 动态策略管理操作时，则需要走流程审批，待审批人审批通过后才能触发相关操作。管理员用户执行租户续期或资源扩缩容操作时，无需审批，会直接触发相关操作。

在当前版本中，仅部分组件支持租户操作，支持的组件类型和租户策略如[表 7-3](#)所示。

表7-3 支持的组件类型和资源共享策略

组件	租户的策略
HDFS	资源对应一个或多个限额的存储目录
YARN	资源对应一个资源队列，每个资源队列提供配额的CPU和内存资源
Hive	资源对应一个或多个限额的database，每个database具有独立的存储资源
HBase	资源对应一个或多个限额的命名空间和若干个RegionServer组
Kafka	资源对应一个或多个Topic，Topic可设置副本数和存储空间
Spark	通过YARN的租户来实现对计算资源的控制
Flink	通过YARN的租户来实现对计算资源的控制

租户有时间期限，新建租户成功后，指定用户在指定时间期限内可使用本租户的组件资源。租户内组件资源的具体使用方法，与集群组件资源的使用方式完全一样。

# 8 卸载

卸载包括独立卸载大数据集群、独立卸载数据工厂、卸载大数据平台管理系统（也会同时卸载数据工厂）。

## 8.1 卸载大数据集群

大数据集群的卸载包括删除集群、删除组件、删除进程三种场景。

### 8.1.1 删除集群

删除集群表示删除该集群中包含的所有组件及主机节点。



注意

- **在生产环境中，删除集群为高危操作，且不可回退或暂停，请谨慎操作。**
- 当集群中有正在运行的任务时，删除集群后集群中的所有任务均会被同步删除。
- 若某租户集群中已创建租户，则删除该租户集群时，对应的租户会一起被删除。
- 执行删除集群操作后，当此集群中的主机上所有数据都被删除干净（即在[资源管理/主机管理]的主机列表中这些主机的状态切换为“未使用”时），这些主机的密码会被重置为 Passw0rd@\_。
- 当集群被数据工厂中的数据源所依赖时，删除集群后数据工厂依赖该集群的所有数据源都将被同步删除。
- 融合部署（即大数据平台管理系统和大数据集群部署在相同节点上）的情况下，删除集群操作可能会执行失败，此时请联系紫光云技术支持工程师协助处理。
- 删除集群成功后，该集群所有节点均不可直接用来重新部署大数据平台管理系统。若有此类使用规划，请务必在删除集群后对节点重装操作系统，然后才可新部署大数据平台管理系统。

集群在使用过程中，根据实际需要，可执行删除集群的操作。

(1) 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面。

(2) 在集群列表页面，单击某集群对应的<删除>按钮，根据集群中主机状态不同，分为以下两种情况：

- 若集群中所在主机均在线，则此时删除集群会显示集群总节点个数、所有节点共使用的磁盘容量，执行删除集群操作时可选择是否删除数据。若勾选删除数据，则同时删除节点上的组件和数据；若不勾选删除数据，则此时仅删除组件，该节点若想被其他大数据集群重新使用，可后续在[集群管理/资源管理/主机管理]的主机列表处手动删除对应节点上的数据。
- 若集群中部分主机离线，则此时删除集群会显示集群总节点个数、在线节点已使用的磁盘容量、离线节点个数和离线主机 IP。
  - 对于离线主机，执行删除集群操作时不能删除离线节点上的组件及数据（需等待集群删除操作完成且主机恢复正常后，在[集群管理/主机管理/主机资源]的主机列表处手动删除离线节点上的组件和数据，然后该节点才能被其他大数据集群重新使用）。

- 对于在线主机，执行删除集群操作时可选择是否删除数据。若勾选删除数据，则同时删除节点上的组件和数据；若不勾选删除数据，则此时仅删除组件，该节点若想被其他大数据集群重新使用，可后续在[集群管理/主机管理/主机资源]的主机列表处手动删除对应节点上的数据。

(3) 集群删除的相关信息确认并选择完成后，还需根据弹窗中的提示进行相关操作（比如：输入集群名和主机 root 密码进行二次确认），然后即可删除集群。

图8-1 删除集群

集群名称	集群IP	运行状态	告警状态	集群模式	集群类型	创建者	创建时间	集群描述	操作
sharedevtest	10.121.68.130	运行中		租户模式	Hadoop	admin	2022-04-25 04:4...		编辑 删除

## 8.1.2 删除组件

删除组件表示针对某个组件的完整卸载，即删除该组件在集群所有主机节点上的相关进程。



注意

- 在生产环境中，删除组件功能不可回退或暂停，请谨慎使用。
- 大数据平台中支持多种集群类型，仅部分集群类型支持删除组件，详情请以实际页面为准。
- 在不同状态下，删除组件操作可能处于不可执行状态。比如：处于“已启动”状态下的组件，需要先停止组件后再执行删除组件操作，删除组件后数据不会清理。
- 在大数据集群中，系统组件为创建集群时缺省安装的组件，不支持单独执行添加或删除操作。
- 在大数据集群中，对于业务组件，仅部分组件支持删除操作，详情请以实际页面为准。
- 删除组件时，需要考虑各组件之间的依赖关系。比如：Spark 依赖 Hive，因此删除 Hive 时需要首先删除 Spark。
- 若待删除组件正在被数据工厂的数据源所依赖，则删除组件后数据工厂对应的数据源将同步不可用。

集群在使用过程中，根据实际需要，可执行删除组件的操作。

(1) 删除组件的方式有以下三种，任选其一即可：

- 在集群管理的左侧导航树中选择[集群列表]，进入集群列表页面，单击某集群名称可跳转至对应的集群详情页面。
  - 在集群详情页面选择[组件]页签，单击组件列表中某组件对应的<删除>按钮。
  - 在集群详情页面选择[组件]页签，单击组件列表中某组件名称进入组件详情页面，在右上角组件操作的下拉框中选择<删除>按钮。
- 在组件管理的组件详情页面右上角组件操作的下拉框中选择<删除>按钮。

(2) 然后按照弹窗中的提示进行相关操作后，即可删除该组件。

图8-2 删除组件（方式一）



图8-3 删除组件（方式二&三）



### 8.1.3 删除进程

删除进程表示仅在大数据集群的某个主机节点上删除此进程。



注意

- 在生产环境中，删除进程功能不可回退或暂停，请谨慎使用。
- 在大数据集群中，仅部分组件的部分进程支持删除操作，详情请以实际页面为准。
- 在不同状态下，删除进程操作可能处于不可执行状态，详情请以实际页面为准。比如：处于“已启动”状态下的进程，不可执行删除操作，此时需先停止进程才可执行删除操作。

集群在使用过程中，根据实际需要，可执行删除进程的操作。

(1) 删除进程的方式有以下四种，任选其一即可：

- 在[集群管理/集群列表]页面，单击某集群名称可跳转至对应的集群详情页面。在集群详情页面选择[组件]页签，单击组件列表中某组件名称进入组件详情页面。在组件详情页面选择[部署拓扑]页签，单击进程列表中某进程对应的<删除>按钮。

- 在[集群管理/组件管理]的组件详情页面选择[部署拓扑]页签，单击进程列表中某进程对应的<删除>按钮。
- 在[集群管理/集群列表]页面，单击某集群名称可跳转至对应的集群详情页面。在集群详情页面选择[主机]页签，单击主机列表中某主机名进入主机详情页面。在主机详情页面选择[进程列表]页签，单击进程列表中某进程对应的<删除>按钮。
- 在[集群管理/主机管理/主机监控]页面的[主机列表]页签，单击某主机名可跳转至对应的主机详情页面。在主机详情页面选择[进程列表]页签，单击进程列表中某进程对应的<删除>按钮。

(2) 然后按照弹窗中的提示进行相关操作后，即可删除该组件。

图8-4 删除进程（方式一&二）

进程名	进程状态	主机名	主机IP	机架	操作
DataNode	已启动	sharedev1.hde.com	10.121.68.131	/default-rack	磁盘均衡 停止 重启 删除
DataNode	已启动	sharedev2.hde.com	10.121.68.132	/default-rack	磁盘均衡 停止 重启 删除
DataNode	已启动	sharedev3.hde.com	10.121.68.133	/default-rack	磁盘均衡 停止 重启 删除
DataNode	已启动	sharedev4.hde.com	10.121.68.134	/default-rack	磁盘均衡 停止 重启 删除
DataNode	已停止	sharedev5.hde.com	10.121.68.135	/default-rack	开启 删除

图8-5 删除进程（方式三&四）

进程名	进程状态	组件名	操作
Standby HBase Master	已启动	HBASE	停止 重启
RegionServer	已启动	HBASE	停止 重启 删除
DataNode	已停止	HDFS	开启 删除
HDFS Client	已安装	HDFS	
JournalNode	已启动	HDFS	停止 重启 删除

## 8.2 卸载数据工厂

---



注意

若系统中已安装了数据工厂，在后续使用过程中数据工厂不再需要，则可以单独执行卸载数据工厂的操作。

---

卸载数据工厂的步骤如下：

- (1) 登录安装大数据平台管理系统的节点，在解压文件夹中，单独执行卸载数据工厂的脚本，命令如下：

```
sh uninstall_df.sh
```

---



说明

- 卸载数据工厂时，若数据工厂中存在数据源则卸载不会被允许。
  - 卸载脚本执行过程中，会出现相关的询问信息（比如：输入主机 root 密码），请根据提示输入信息后继续执行。
- 

- (2) 卸载成功后，仅数据工厂模块功能将不可用，大数据集群等其他功能均可正常使用。此时在解压文件夹下重新执行 **sh install\_df.sh** 即可重新启动安装。

## 8.3 卸载大数据平台管理系统

---



注意

- 在生产环境中，卸载大数据平台管理系统为高危操作，且不可回退或暂停，请务必谨慎使用。
  - 执行卸载大数据平台管理系统时，要求管理系统各节点密码相同（主机 root 密码禁止在后台修改），且没有配置免密。另外，卸载脚本仅存在安装节点上，其他节点无法执行卸载操作。
  - 卸载大数据平台管理系统时，若平台中存在大数据集群则卸载不会被允许。
  - 若系统中已安装了数据工厂，则在执行卸载大数据平台管理系统的操作时会将数据工厂一起卸载。
- 

卸载大数据平台管理系统的步骤如下：

- (1) 登录安装大数据平台管理系统的节点（注意：卸载脚本仅存在安装节点上，其他节点无法执行卸载操作），在解压文件夹中，执行卸载脚本，命令如下：

```
sh uninstall.sh
```

---



说明

卸载脚本执行过程中，会出现相关的询问信息（比如：输入主机 root 密码），请根据提示输入信息后继续执行。

---

(2) 卸载成功后，恢复到大数据平台安装前的状态，此时在解压文件夹下执行 **sh install.sh** 即可重新启动安装。

---

 注意

大数据平台管理系统卸载完成后，对应的管理节点不能直接被其他大数据平台中的集群使用。若有此类使用规划，请务必在大数据平台管理系统卸载之后对节点重装操作系统，然后才可将其添加至其他大数据平台中供集群使用。

---



# 9 常见问题解答

## 1. 大数据集群可部署的业务组件有哪些？

表9-1 大数据集群业务组件列表

组件名	版本号
HDFS	3.0.0
MapReduce	3.0.0
YARN	3.0.0
ZooKeeper	3.4.5
Hive	2.1.1
Spark	2.4.0
Presto	1.5.0
DLH	1.0.0
Sqoop	1.4.7
HBase	2.1.0
HBase Indexer	1.5
Oozie	5.1.0
Redis	6.2.1
Storm	1.2.1
Kafka	2.7.2
Flink	1.13.6
Flume	1.9.0
Elasticsearch	7.10.0
Solr	7.4.0

## 2. 根据现场磁盘分区方案和挂盘方案的不同，安装组件时，可能受影响的组件以及各组件必须检查的配置项有哪些？

由于现场磁盘分区方案和挂盘方案的不同，组件安装完成后，必须按照[表 9-2](#) 所示要求进行检查，否则组件可能使用异常。

表9-2 安装组件后需要检查的配置项

组件	是否需要检查	被影响的配置项	如何解决
HDFS	是（配置项的参数值默认选择3个挂载路径）	dfs.namenode.name.dir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
	是（配置项的参数值默认使用全部挂载路径）	dfs.datanode.data.dir	
	未开启高可用时，需要检查该配置项（配置项的参数值默认使用全部挂载路径）	dfs.namenode.checkpoint.dir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
	开启高可用时，需要检查该配置项（配置项的参数值默认选择1个挂载路径）	dfs.journalnode.edits.dir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
YARN	是（配置项的参数值默认使用全部挂载路径）	yarn.nodemanager.local-dirs	此目录为数据目录，用于存放应用程序的运行依赖包等信息。检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
		yarn.nodemanager.log-dirs	
	是（配置项的参数值默认使用某一个挂载路径）	yarn.timeline-service.leveldb-state-store.path	此目录为数据目录，用于记录应用程序运行状态等信息。检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
		yarn.timeline-service.leveldb-timeline-store.path	
Kafka	是（配置项的参数值默认使用全部挂载路径）	log.dirs	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
ElasticSearch	是（配置项的参数值	path.data	此目录为数据目录，检查此配置项的值时，需

组件	是否需要检查	被影响的配置项	如何解决
	默认使用全部挂载路径)		关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> <li>请确保 <b>Elasticsearch</b> 用户具备数据目录的读写权限</li> </ul>
Solr	是（配置项的参数值默认使用某一个挂载路径）	solr.data.home	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> <li>仅支持单路径挂载使用，所以只允许配置一个数据目录</li> </ul>
Zookeeper	是（配置项的参数值默认使用某一个挂载路径）	dataDir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
Storm	是（配置项的参数值默认使用某一个挂载路径）	storm.local.dir	此目录为 <b>Storm</b> 使用的本地文件系统目录，用于保存少量状态信息。检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> <li>建议此目录为 <b>Storm</b> 服务独立使用。如果该目录同时被其他服务使用，需手动修改为其他路径</li> </ul>
Redis	是（配置项的参数值默认使用某一个挂载路径）	redis.dir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> <li>仅支持单路径挂载使用，所以只允许配置一个数据目录</li> </ul>
Oozie	是（配置项的参数值	oozie_data_dir	此目录为数据目录，检查此配置项的值时，需

组件	是否需要检查	被影响的配置项	如何解决
	默认使用某一个挂载路径)		关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>
Infra Solr	是（配置项的参数值默认使用某一个挂载路径)	infra_solr_datadir	此目录为数据目录，检查此配置项的值时，需关注： <ul style="list-style-type: none"> <li>不允许存在非数据目录</li> <li>若现场数据目录是自定义的，则需要配置为对应的数据目录</li> </ul>

### 3. 组件的日志信息在哪里查看？

表9-3 组件日志路径说明

组件	日志路径
HDFS	/var/de_log/hadoop/user_hdfs
MapReduce2	HistoryServer日志路径：/var/de_log/hadoop-yarn/user_mapred/和 /var/de_log/hadoop-mapreduce/mapred/
YARN	/var/de_log/hadoop-yarn/user_yarn 【说明】上述的日志是YARN本身的日志。另外： <ul style="list-style-type: none"> <li>执行在 YARN 上的应用日志，可以通过 YARN 的 UI 界面查看，日志文件实际存储位置默认是在 HDFS 上，默认路径为/app-logs</li> <li>如果日志不聚合，可以配置 yarn.log-aggregation-enable 为 false</li> <li>内嵌的 HBase 日志路径为： /var/de_log/hadoop-yarn/embedded-yarn-ats-hbase，在 timeline 安装的节点上可看到（前提条件：配置项 use_external_hbase、is_hbase_system_service_launch 的值均为 false）</li> </ul>
Spark	/var/de_log/spark2和/var/de_log/spark2/user_spark/ 【说明】上述的日志是Spark的HistoryServer和ThriftServer的日志。另外： <ul style="list-style-type: none"> <li>使用 Spark 客户端（如使用 spark-sql）执行任务时，日志存放路径为 /var/de_log/spark2/user_\${user.name}/，其中\${user.name}是指执行任务的用户名</li> </ul>
Presto	Presto跨源分析及交互式查询服务日志路径：/var/de_log/presto
Atlas	Atlas元数据服务日志路径：/var/de_log/atlas

组件	日志路径
DLH	<ul style="list-style-type: none"> <li>DLH Server 服务的日志路径: /var/de_log/dlh/hive</li> <li>DLH 流 SQL 服务的日志路径: /var/de_log/flink-sql-gateway/user_hdfs</li> </ul>
Hive	/var/de_log/hive
Ranger	/var/log/ranger/和/var/de_log/ranger/ <b>【说明】</b> 开启权限和密钥管理时, 集群内部会安装该组件
Knox	/var/log/knox/ <b>【说明】</b> 在Hadoop集群中, 开启Kerberos认证时, 创建的集群时会安装该组件, 用于组件Web的单点登录
Elasticsearch	/var/de_log/elasticsearch
Solr	/var/de_log/solr
Redis	/var/de_log/redis
HBase	/var/de_log/hbase/user_hbase
HBase Indexer	/var/de_log/hbase-indexer/user_hbase
Kafka	/var/de_log/kakfa/user_\${user.name}/, 其中\${user.name}是指执行任务的用户名
ZooKeeper	/var/de_log/zookeeper/user_(user.name)/, 其中\${user.name}是指执行任务的用户名
Storm	/var/de_log/storm
Flink	<ul style="list-style-type: none"> <li>Flink 启动日志路径: /var/de_log/flink/user_\${user.name}/, 其中\${user.name}是指执行任务的用户名</li> <li>Flink 任务运行日志路径, 可以通过 YARN 的 UI 界面查看</li> </ul> <b>【说明】</b> Flink是Client服务, 如果在上述路径未找到日志, 请在客户端控制台获取
Sqoop	/var/log/sqoop <b>【说明】</b> Sqoop是Client服务, 如果在上述路径未找到日志, 请在客户端控制台获取
Infra Solr	/var/log/ambari-infra-solr
Kerberos	/var/log/krb5kdc.log 和 /var/log/kadmind.log
Oozie	/var/de_log/oozie
Flume	/var/de_log/flume

#### 4. 常用组件的数据存放位置在哪里？

表9-4 组件数据的存放位置

组件	存放位置	说明
ZooKeeper	配置项dataDir的值	存放ZooKeeper数据
HDFS-JournalNode	配置项dfs.journalnode.edits.dir的值	存放HDFS的JournalNode数据
HDFS-NameNode	配置项dfs.namenode.name.dir的值	存放HDFS的NameNode数据
HDFS-DataNode	配置项dfs.datanode.data.dir的值	<ul style="list-style-type: none"><li>• 推荐把每个物理磁盘挂载在/opt/disknn (nn 为 1 至 2 位的数字) 上不同的挂载点</li><li>• 存放 HDFS 的数据</li></ul>
Elasticsearch	配置项path.data的值	<ul style="list-style-type: none"><li>• 推荐把每个物理磁盘挂载在/opt/disknn (nn 为 1 至 2 位的数字) 上不同的挂载点</li><li>• 存放 Elasticsearch 的数据</li><li>• 推荐使用 SSD, 并且每个分区下的大小要相等, 否则盘剩余空间较大的 I/O 压力会过大</li></ul>
Solr	配置项solr.data.home值	<ul style="list-style-type: none"><li>• 基于性能考虑, Solr 的索引数据可以存放在本地磁盘; 每个节点上的 Solr 实例将各自的 home 目录放置到独立磁盘上, 用以存放 Core 的元数据和索引数据</li><li>• Solr 的索引数据和元数据存放在 HDFS, 通过设定 solr.in.sh 的配置参数的值来决定是否存放在 HDFS 上, 默认不存放。如选择存放在 HDFS 中, 则 Solr 会依赖 HDFS(在此场景下, Solr 无需配置数据盘), 否则不依赖</li></ul>
Storm	配置项storm.local.dir的值	存放少量的中间状态数据
Kafka	配置项log.dirs的值	存放Kafka的数据目录
Redis	配置项redis.dir的值	存放Redis的业务数据, 数据存储目录默认为/var/redis, 用户可根据实际情况进行修改 (但不建议存储在系统盘上)

#### 5. 大数据集群与 NTP 服务器出现时间不同步情况时的排查方案

安装大数据平台管理系统时, 支持自定义配置 NTP 服务器, 详情请参见 [3.4.2 3. \(1\)](#) 章节。大数据集群中的所有节点通过 chrony 基于 NTP 协议向此 NTP 服务器进行时钟校准, 建议集群中所有节点与现场统一 NTP 服务器保持时钟校准。

- (1) `chrony` 的配置文件有如下两个：
  - `/etc/chrony.conf`: 负责 `chrony ntp` 配置项
  - `/etc/sysconfig/chronyd`: 负责系统 `system` 启动 `chrony` 时的传入参数
- (2) `chrony` 常用命令如下：
  - 查看版本: `chronyd --version`
  - 查看运行状态: `systemctl status chronyd`
  - 查看同步状态 (更多参数参见 `man` 手册): `chronyc sourcestats`
- (3) 若出现时间不同步的情况, 排查方案如下:
  - a. 本机硬件时间问题, 本机硬件时间会影响主机重启后的系统软件时间。若出现时间不同步的情况, 请排查是否有主机重启。下面命令可校准本机硬件时间:

```
timedatectl set-timezone "Asia/Shanghai"
timedatectl status
date -s "20191119 19:35:00"
hwclock --systohc
hwclock --show
```
  - b. 大数据集群安装后的配置可以稳定准确校时, `chrony` 配置保存安装后, 配置值即可无需修改。若出现时间不同步的情况, 请排查是否修改过 `chrony` 配置。
  - c. 如果自定义配置需要考虑: `ntp` 校时算法会根据时钟差异决定校时步长, 步长决定出现差异时重新回归同步需要的时间大小, 过大的时钟差异会被认为异常不被校准。若出现时间不同步的情况, 请排查 `chrony` 的配置文件修改是否合理。
  - d. 通常会配置 `chronyc -a makestep` 辅助 `chrony` 校准时间, `chronyc -a makestep` 为一次性校准时间, 作为定时任务, 在主机重启后或 `chronyd` 启动前执行, 但是 `chronyc -a makestep` 任务无法解决 `chrony` 任务时间不同步问题。

**6. 安装大数据平台管理系统前, 若用户已有的网络与系统默认占用的网段冲突, 则需要修改系统容器网络, 如何操作?**



修改大数据平台管理系统 `docker` 容器的网络时要求仅可使用私网地址, 私网地址范围如下:

- 10.0.0.0-10.255.255.255
- 172.16.0.0-172.31.255.255
- 192.168.0.0-192.168.255.255

若无私网地址可使用, 请咨询紫光云技术支持工程师。

---

安装大数据平台管理系统前, 进行网络规划需注意: 系统默认占用了一个网段作为内部使用地址, 即: `172.17.0.1/16` (缺省 `docker` 网桥网段, 即 `docker0` 所在网段), 此网段必须单独预留供 `docker` 容器使用。若用户已有的网络与该地址段冲突, 则需要修改系统 `docker` 容器网络, 修改步骤如下:

- (1) 登录待执行安装大数据平台管理系统的管理节点 (即大数据平台的产品软件包解压路径所在节点, 参见 [3.4.2](#) 章节)。

- (2) 进入解压文件夹中，修改/conf目录下的配置文件default.json。修改说明如[图9-1](#)所示，将services.docker.bip的值修改为新规划网段，修改完成后保存退出。

注意：bip的格式是（172.17.0.1/16）网关/掩码，而不是（172.17.0.0/16）网段/掩码。

图9-1 修改系统 docker 容器网络地址

```
{
  "product": "BDP",
  "version": "E6102",
  "isBigdata" : "true" ,
  "services": {
    "docker": {
      "bip": " 172.17.0.1/16"
    }
  },
}
```

- (3) 进入解压文件夹中，修改/ansible/roles/init/docker/templates/docker.service.j2文件。修改说明如[图 9-2](#)所示，将该文件中的 172.17.0.0/16（网段/掩码）修改为新规划的网段/掩码，修改完成后保存退出。

图9-2 修改系统 docker 服务防火墙网络地址

```
[Unit]
Description=Docker Application Container Engine
Documentation=http://docs.docker.io

[Service]
ExecStart=/usr/bin/dockerd
ExecStartPre=/sbin/iptables -t nat -A POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
ExecStartPost=/sbin/iptables -I FORWARD -s 0.0.0.0/0 -j ACCEPT
ExecStopPost=/sbin/iptables -t nat -D POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
ExecReload=/bin/kill -s HUP $MAINPID
Restart=always
RestartSec=5
LimitNOFILE=65536
LimitNPROC=infinity
LimitCORE=infinity
Delegate=yes
KillMode=process

[Install]
WantedBy=multi-user.target
```

- (4) 然后，根据部署流程启动大数据平台管理系统的安装即可。



## 7. 安装大数据平台管理系统后，才发现用户已有的网络与系统默认占用的网段冲突，此时需要修改系统容器网络，如何操作？



注意

修改大数据平台管理系统 docker 容器的网络时要求仅可使用私网地址，私网地址范围如下：

- 10.0.0.0-10.255.255.255
- 172.16.0.0-172.31.255.255
- 192.168.0.0-192.168.255.255

若无私网地址可使用，请咨询紫光云技术支持工程师。

- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 config.json 中配置的管理节点）。
- (2) 修改/etc/docker/daemon.json 文件。修改说明如[图 9-3](#)所示，将 bip 的值修改为新规划网段，修改完成后保存退出。

注意：bip 的格式是（172.17.0.1/16）网关/掩码，而不是（172.17.0.0/16）网段/掩码。

图9-3 修改 docker 容器网段默认地址

```
{
  "bip": "172.17.0.1/16",
  "max-concurrent-downloads": 10,
  "log-driver": "json-file",
  "log-level": "warn",
  "log-opts": {
    "max-size": "10m",
    "max-file": "3"
  },
  "data-root": "/var/lib/docker"
}
```

- (3) 修改/etc/systemd/system/docker.service 文件。修改说明如[图 9-4](#)所示，将该文件中的 172.17.0.0/16（网段/掩码）修改为新规划的网段/掩码，修改完成后保存退出。

图9-4 修改系统 docker 服务防火墙网段默认地址

```
[Unit]
Description=Docker Application Container Engine
Documentation=http://docs.docker.io

[Service]
ExecStart=/usr/bin/dockerd
ExecStartPre=/sbin/iptables -t nat -A POSTROUTING -s 172.17.0.0/16 ! -o docker0
-j MASQUERADE
ExecStartPost=/sbin/iptables -I FORWARD -s 0.0.0.0/0 -j ACCEPT
ExecStopPost=/sbin/iptables -t nat -D POSTROUTING -s 172.17.0.0/16 ! -o docker0
-j MASQUERADE
ExecReload=/bin/kill -s HUP $MAINPID
Restart=always
RestartSec=5
LimitNOFILE=65536
LimitNPROC=infinity
LimitCORE=infinity
Delegate=yes
KillMode=process

[Install]
WantedBy=multi-user.target
```

(4) 重启 docker 容器，命令如下：

```
systemctl restart docker
```

(5) docker 容器重启完成后，再次查看 docker 容器的网络是否修改成功，命令如下：

```
ip addr show dev docker0
```

图9-5 验证 docker 容器网段是否更改成功（示例修改为 192.168.0.1/24）

```
[root@management0 ~]# ip addr show dev docker0
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether 02:42:2e:53:b8:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:2eff:fe53:b859/64 scope link
        valid_lft forever preferred_lft forever
```

## 8. 安装大数据平台管理系统的配置文件说明

在大数据平台管理系统的[安装过程](#)中，配置文件分为 config.json 和 default.json 文件组成。

- 配置文件 config.json 中，可配置大数据平台管理系统的管理节点 IP 和虚拟 IP（访问 IP）。
- 配置文件 default.json 中，可配置是否安装数据工厂（请根据实际情况进行选择），还可配置大数据平台管理系统的默认端口、数据库配置、Redis 配置等信息（默认不需要修改）。关于 default.json 文件中部分配置项的说明详情请参见[表 9-5](#)。

表9-5 配置文件 default.json 中部分配置项说明

配置项	默认值	是否可修改	说明
product	BDP	否	产品名

配置项	默认值	是否可修改	说明
version	E6102	否	版本号信息
services.docker.bip	172.17.0.1/16	是	Docker0使用的网段，安装前务必进行检查是否与业务网冲突，参见2.5章节。若出现冲突，请修改此配置项的值
services.hostname.host_prefix	management	是	管理节点的主机名前缀
services.host_prefix.domain	hde.com	是	管理节点的主机的域（即主机名后缀）
services.mysql.port	3306	是，不建议修改	MySQL端口
services.mysql.proxy_port	3307	是，不建议修改	MySQL负载代理端口
services.mysql.root_password	UGFzc3cwcmRAXw==	是，不建议修改	MySQL的root用户密码（已加密）
services.mysql.admin_user	admin	是，不建议修改	MySQL管理用户
services.mysql.admin_password	UGFzc3cwcmRAXw==	是，不建议修改	MySQL管理用户密码（已加密）
services.redis.password	UGFzc3cwcmRAXw==	是，不建议修改	Redis登录密码（已加密）
services.redis.port	["7101","7102"]	是，不建议修改	Redis占用端口
services.rocketmq.port	10911	是，不建议修改	Rocketmq端口，真实端口随broker个数+10。比如：2节点部署时，每台机器上占用启动2个broker，则端口分别是10921和10931
services.rocketmq.ha_port	10912	是，不建议修改	Rocketmq HA端口，真实端口随broker个数+10。比如：2节点部署时，每台机器上占用启动2个broker，则端口分别是10922和10932
services.rocketmq.namesrv_port	9876	是，不建议修改	Rocketmq NameServer端口
services.kong.admin_http_port	28001	是，不建议修改	Kong注册服务http端口

配置项	默认值	是否可修改	说明
services.kong.admin_https_port	28002	是，不建议修改	Kong注册服务https端口
services.kong.proxy_http_port	28003	是，不建议修改	KongAPI服务http端口
services.kong.proxy_https_port	28004	是，不建议修改	Kong API服务https端口
services.kong.mysql_database	kong	是，不建议修改	Kong 数据库名
services.kong.haproxy_proxy_admin_port	28005	是，不建议修改	Kong 注册服务代理端口
services.kong.haproxy_proxy_proxy_port	28006	是，不建议修改	Kong API代理端口
services.keystone.admin_port	28007	是，不建议修改	Keystone管理端口
services.keystone.http_port	28008	是，不建议修改	Keystone页面端口
services.keystone.api_port	28009	是，不建议修改	Keystone API端口
services.keystone.mysql_database	keystone	是，不建议修改	Keystone 数据库名
services.keystone.haproxy_proxy_aip_port	28010	是，不建议修改	keystone API 代理端口
services.haproxy.port	28011	是，不建议修改	haproxy监控端口
services.Keepalived.vip_route	111	是，不建议修改	组播路由ID
services.yum.port	29001	是，不建议修改	yum源端口
services.yum.proxy_port	29002	是，不建议修改	yum代理端口
services.openresty.port	29003	是，不建议修改	openresty端口
services.openresty.proxy_port	29004	是，不建议修改	openresty代理端口
services.deployment.port	29005	是，不建议修改	deployment端口
services.deployment.proxy_port	29006	是，不建议修改	deployment代理端口

配置项	默认值	是否可修改	说明
services.omc.port	29007	是，不建议修改	omc端口
services.omc.proxy_port	29008	是，不建议修改	omc代理端口
services.alertmanager.port	29009	是，不建议修改	alertmanager端口
services.alertmanager.peer_port	29010	是，不建议修改	alertmanager集群端口
services.alertmanager.proxy_port	29011	是，不建议修改	alertmanager代理端口
services.alertrule.port	29012	是，不建议修改	alertrule端口
services.thanos.port	29013	是，不建议修改	thanos端口
services.thanos.proxy_port	29014	是，不建议修改	thanos代理端口
services.league.port	29015	是，不建议修改	league端口
services.league.proxy_port	29016	是，不建议修改	league代理端口
services.league.dbname	bigdata_cluster	是，不建议修改	League数据库名
services.license.port	28012	是，不建议修改	License端口
services.license.proxy_port	28013	是，不建议修改	License代理端口
services.license.mysql_database	license	是，不建议修改	License数据库名
services.webserver.http_port	28014	是，不建议修改	Webserver http端口
services.webserver.proxy_http_port	80	是，不建议修改	Webserver http代理端口
services.webserver.proxy_https_port	443	是，不建议修改	Webserver https代理端口
services.svcmgmt.port	28018	是，不建议修改	svcmgt端口
services.svcmgmt.proxy_port	28019	是，不建议修改	svcmgt代理端口
services.svcmgmt.mysql_database	usrmgt	是，不建议修改	svcmgt数据库名
services.sorb.port	28020	是，不建议修改	sorb端口
services.sorb.proxy_port	28021	是，不建议修改	sorb代理端口

配置项	默认值	是否可修改	说明
services.sorb.mysql_database	bpm	是，不建议修改	sorb数据库名
services.operlog.port	28022	是，不建议修改	operlog端口
services.operlog.proxy_port	28023	是，不建议修改	operlog代理端口
services.operlog.mysql_database	aquarius	是，不建议修改	operlog数据库名
services.notify.port	28024	是，不建议修改	notify端口
services.notify.proxy_port	28025	是，不建议修改	notify代理端口
services.notify.mysql_database	pisces	是，不建议修改	notify数据库名
services.sso.port	28026	是，不建议修改	sso端口
services.sso.proxy_port	28027	是，不建议修改	sso代理端口
services.sso.mysql_database	sso	是，不建议修改	sso数据库名
services.zepelin.port	28580	是，不建议修改	Zeppelin端口
services.azkaban.web_server_port	28581	是，不建议修改	Azkaban管理系统端口
services.azkaban.exec_server_port	28588	是，不建议修改	Azkaban执行服务端口
service.merged_svc.port	28553	是，不建议修改	数据工厂端口
service.merged_svc.proxy_port	28554	是，不建议修改	数据工厂代理端口
service.merged_svc.dbname	datafactory	是，不建议修改	数据工厂数据库名
service.merged_svc.datasource_list	hdfs,hbase,hive,spark,phoenix,livy	否	数据工厂数据库连接列表
service.merged_svc.datasource_type_list	Hive,SparkSQL,Phoenix,HBase	否	数据工厂连接支持类型
service.merged_svc.datasource_query_type_list	Hive,SparkSQL,Phoenix	否	数据工厂查询支持类型

配置项	默认值	是否可修改	说明
service.ldap.user	cn=Manager,dc=hde,dc=com	是，不建议修改	LDAP默认用户
service.ldap.password	Q2xvdWRPUzUjREUzQEFtYmFyaQ==	是，不建议修改	LDAP默认密码（已加密）
service.ambari.user	admin	是，不建议修改	Ambari默认用户
service.ambari.password	Q2xvdWRPUzUjREUzQEFtYmFyaQ==	是，不建议修改	Ambari默认密码（已加密）
service.df.install	false	是	根据是否选择安装数据工厂进行配置，其中： <b>false</b> 表示不安装数据工厂， <b>true</b> 为安装数据工厂
service.upgrade.port	28030	是，不建议修改	upgrade服务端口
service.upgrade.proxy_port	28031	是，不建议修改	upgrade服务代理端口
service.upgrade.mysql_database	upgrade	是，不建议修改	upgrade服务数据库实例名

9. 若安装大数据平台管理系统时，没有同步选择安装数据工厂，在后续使用过程中又有数据工厂的需求，则补充安装数据工厂的方式是什么？

#### 说明

如果此时集群采用的是融合部署，且集群禁用了 root 权限（参见 [7.2](#) 章节），则后续再部署数据工厂时会提示请使用 root 用户进行部署。

(1) 进入大数据平台管理系统的解压文件夹中，修改配置文件 `default.json`。修改说明如 [图 9-6](#) 所示，将 `df.install` 的值由 `false` 改为 `true`，修改完成后保存退出即可。

```
cd BDP-<version>
```

```
vi default.json
```

表9-6 配置文件 default.json 修改说明

参数	说明
df.install	<code>false</code> 表示不安装数据工厂， <code>true</code> 表示安装数据工厂

图9-6 配置文件 default.json 修改后

```
"df":{
  "install": "true"
}
```

(2) 配置文件 default.json 修改完成后，在解压文件夹中，单独执行安装数据工厂的脚本，命令如下：

```
sh install_df.sh
```



说明

安装脚本执行过程中，会出现相关的询问信息（比如：输入主机密码），请根据提示输入信息后继续执行。

## 10. 若安装大数据平台管理系统时，没有配置外部 NTP 服务器，在后续使用过程中又有配置外部 NTP 服务器的需求，则配置方式是什么？



说明

- 安装大数据平台管理系统后，若还未新建大数据集群，则可直接按照本章节步骤配置外部 NTP 服务器即可。
- 安装大数据平台管理系统后，若已经创建大数据集群并且上线了业务，则再配置外部 NTP 服务器会存在较大的风险，比如：时间跳变导致组件服务状态异常、业务数据的时间不一致、监控指标异常等。此时，若仍需要配置，则建议先下线业务、停止集群全部组件，待集群时钟同步后再进行集群组件启动、业务上线、监控指标异常恢复等操作，此情况可联系紫光云技术支持工程师协助处理。

**示例：**安装大数据平台管理系统完成后，新增配置外部 NTP 服务器（示例：NTP 服务器的 IP 地址为 10.121.73.136），操作步骤如下：

- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 config.json 中配置的管理节点。示例：第一个管理节点为 10.121.68.161，第二个管理节点为 10.121.68.162）。
- (2) 在第一个管理节点上（即在 [3.4.2](#) [3.\(1\)](#) 步骤中配置文件 config.json 的 node 配置项中配置的第一个主机节点 IP），修改 /etc/chrony.conf 文件。修改说明如 [图 9-7](#) 所示，在第一行下面增加一行“server 10.121.73.136 iburst trust prefer minpoll 1 maxpoll 3 mindelay 1 maxdelay 3”，修改完成后保存退出。

图9-7 修改第一个管理节点的/etc/chrony.conf 文件（红框新增）

```
# Use public servers from the pool.ntp.org project.
server 10.121.73.136 iburst trust prefer minpoll 1 maxpoll 3 mindelay 1 maxdelay 3
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
```



- (3) 重启第一个管理节点上的 `chronyd` 服务，命令如下：  
`systemctl restart chronyd`
- (4) 在第二个管理节点上（即在 [3.4.2 3.\(1\)](#) 步骤中配置文件 `config.json` 的 `node` 配置项中配置的第二个主机节点 IP），修改 `/etc/chrony.conf` 文件。修改说明如 [图 9-8](#) 所示，在第一行下面新增增加一行“`server 10.121.73.136 iburst trust prefer minpoll 1 maxpoll 3 mindelay 1 maxdelay 3`”，修改完成后保存退出。

图9-8 修改第二个管理节点的/etc/chrony.conf 文件（红框新增）

```
# Use public servers from the pool.ntp.org project.  
server 10.121.73.136 iburst trust prefer minpoll 1 maxpoll 3 mindelay 1 maxdelay 3  
server 10.121.68.161 iburst trust minpoll 1 maxpoll 3 mindelay 1 maxdelay 3
```

- (5) 重启第二个管理节点上的 `chronyd` 服务，命令如下：  
`systemctl restart chronyd`
- (6) 然后，新增配置的外部 NTP 服务器即可生效，之后大数据集群中的所有节点将通过 `chrony` 基于 NTP 协议向此外部 NTP 服务器进行时钟校准。

11. 安装大数据平台管理系统后，才发现大数据平台需要开启内外网映射访问，此时需要配置外网访问虚拟 IP，如何操作？



当大数据平台管理系统开启 SSO 配置时，才需修改外网访问虚拟 IP；若未开启，则可忽略此步骤。

---

- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 `config.json` 中配置的管理节点）。
- (2) 在 2 个管理节点上分别修改 `/data/BDP/system/sso/scripts/restart_sso.sh` 文件。修改说明如 [图 9-7](#) 所示，将文件中 `VIP_HOST` 的值修改为外网访问虚拟 IP，修改完成后保存退出。

图9-9 修改 SSO 服务的 VIP\_HOST

```
if [ ! -n "$1" ] || [ ! -n "$2" ];then
    echo "you need input this mysql password and redis password,for example:sh restart_sso.sh <mysql password>
    <redis password>"
else
    MYSQL_ADMIN_PASSWD=$1
    REDIS_PWD=$2

    dockerid=$(docker ps -a --no-trunc --filter name=~/BDP-system-sso|grep -v CONTAINER|awk '{print $1}')

    if [[ -n "$dockerid" ]];then
        docker stop $dockerid && docker rm $dockerid
    fi

    docker run -d --name BDP-system-sso \
    -v /etc/localtime:/etc/localtime \
    -v /etc/sysctl.conf:/etc/sysctl.conf \
    --env REDIS_SVC_HOST=10.121.47.235 \
    --env REDIS_SVC_PORT=7101 \
    --env X86=single \
    --env JAVA_OPTS="-Drocketmq.client.name=sso1" \
    --env REDIS_PWD=${REDIS_PWD} \
    --env MYSQL_SVC_HOST=10.121.47.235 \
    --env MYSQL_SVC_PORT=3307 \
    --env MYSQL_ADMIN_USER=admin \
    --env MYSQL_ADMIN_PASSWD=${MYSQL_ADMIN_PASSWD} \
    --env DB_USERNAME=admin \
    --env DB_PASSWORD=${MYSQL_ADMIN_PASSWD} \
    --env DB_NAME=dataengine_sso \
    --env ROCKET_NAME_SERVER="10.121.47.236:9876;10.121.47.237:9876" \
    --env KEYSTONE_DATABASE=dataengine_keystone \
    --env VIP_HOST=10.121.47.235 \
    --env USE_RZT=False \
    --env APP_ID=rsFL9gjG \
    --env APP_SECRET=269e1d2f3ec747f2aa986b6ae9f33b12ed9a3f4e \
    --env WEB_SERVER_PORT=443 \
    --env KONG_SVC_HOST=http://10.121.47.235:28006 \
    --env LOG_SVC_HOST=http://10.121.47.235:28023 \
    --env KS_SVC_HOST=http://10.121.47.235:28010 \
    --env SVCMGT_SVC_HOST=http://10.121.47.235:28019 \
    --env PRODUCT_NAME=DataEngine \
    --env IP=10.121.47.236 \
    --volume /etc/localtime:/etc/localtime \
    -p 28026:16660 \
    --restart=always \
    -m 2Gi \
    --memory-reservation 512Mi \
    --cpus 1 \
    -c 1024 \
    --health-cmd "curl --fail http://localhost:16660/health || exit 1" \
    --health-interval 10s \
    --health-start-period 60s \
    --health-timeout 30s \
    --health-retries 5 \
    bdp_sso:E6102
fi
```

(3) 重启 bdp-sso 容器，命令如下：

```
/data/BDP/system/sso/scripts/restart_sso.sh <mysql_password> <redis_password>
```

其中：<mysql\_password>为系统数据库 Mysql 的密码，<redis\_password>为系统数据库 Redis 的密码。若有重启 bdp-sso 容器的需求，密码请联系紫光云技术支持工程师获取。

## 12. 安装大数据平台管理系统后，才发现大数据平台需要对接认证通，此时需要配置认证通相关参数，如何操作？

---

### 注意

- 当大数据平台管理系统需对接认证通时，才需修改认证通参数；若不对接，则可忽略此步骤。
  - 若大数据平台管理系统需对接认证通，则部署前需在认证通应用管理中添加 BDP 应用，添加完成后获取应用的 appID 和 appSecret 参数。关于在认证通中添加 BDP 应用以及获取应用相关参数的方法详情请参见认证通相关使用手册。
- 
- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 config.json 中配置的管理节点）。
  - (2) 在 2 个管理节点上分别修改/data/BDP/system/sso/scripts/restart\_sso.sh 文件。修改说明如[图 9-8](#)所示，将文件中 USE\_RZT 的值修改为 True，APP\_ID 和 APP\_SECRET 参数修改为认证通中 BDP 应用具体的参数，修改完成后保存退出。

图9-10 修改 SSO 服务的认证通参数

```
if [ ! -n "$1" ] || [ ! -n "$2" ];then
    echo "you need input this mysql password and redis password,for example:sh restart_sso.sh <mysql password>
    <redis password>"
else
    MYSQL_ADMIN_PASSWD=$1
    REDIS_PWD=$2

    dockerid=$(docker ps -a --no-trunc --filter name=~BDP-system-sso|grep -v CONTAINER|awk '{print $1}')

    if [[ -n "$dockerid" ]];then
        docker stop $dockerid && docker rm $dockerid
    fi

    docker run -d --name BDP-system-sso \
    -v /etc/localtime:/etc/localtime \
    -v /etc/sysctl.conf:/etc/sysctl.conf \
    --env REDIS_SVC_HOST=10.121.47.235 \
    --env REDIS_SVC_PORT=7101 \
    --env X86=single \
    --env JAVA_OPTS="-Drocketmq.client.name=sso1" \
    --env REDIS_PWD=${REDIS_PWD} \
    --env MYSQL_SVC_HOST=10.121.47.235 \
    --env MYSQL_SVC_PORT=3307 \
    --env MYSQL_ADMIN_USER=admin \
    --env MYSQL_ADMIN_PASSWD=${MYSQL_ADMIN_PASSWD} \
    --env DB_USERNAME=admin \
    --env DB_PASSWORD=${MYSQL_ADMIN_PASSWD} \
    --env DB_NAME=dataengine_sso \
    --env ROCKET_NAME_SERVER="10.121.47.236:9876;10.121.47.237:9876" \
    --env KEYSTONE_DATABASE=dataengine_keystone \
    --env VIP_HOST=10.121.47.235 \
    --env USE_RZT=False \
    --env APP_ID=rsFl9gjG \
    --env APP_SECRET=269e1d2f3ec747f2aa986b6ae9f33b12ed9a3f4e \
    --env WEB_SERVER_PORT=443 \
    --env KONG_SVC_HOST=http://10.121.47.235:28006 \
    --env LOG_SVC_HOST=http://10.121.47.235:28023 \
    --env KS_SVC_HOST=http://10.121.47.235:28010 \
    --env SVCMGT_SVC_HOST=http://10.121.47.235:28019 \
    --env PRODUCT_NAME=DataEngine \
    --env IP=10.121.47.236 \
    --volume /etc/localtime:/etc/localtime \
    -p 28026:16660 \
    --restart=always \
    -m 2Gi \
    --memory-reservation 512Mi \
    --cpus 1 \
    -c 1024 \
    --health-cmd "curl --fail http://localhost:16660/health || exit 1" \
    --health-interval 10s \
    --health-start-period 60s \
    --health-timeout 30s \
    --health-retries 5 \
    bdp_sso:E6102
fi
```

(3) 重启 bdp-sso 容器，命令如下：

```
/data/BDP/system/sso/scripts/restart_sso.sh <mysql_password> <redis_password>
```

其中:<mysql\_password>为系统数据库 Mysql 的密码,<redis\_password>为系统数据库 Redis 的密码。若有重启 bdp-sso 容器的需求，密码请联系紫光云技术支持工程师获取。

### 13. 在物理机环境中安装大数据集群时，若出现组件启动时间过长，CPU 占用率异常过高的情况，如何处理？

在物理机环境中安装大数据集群时，若出现组件启动时间过长，CPU 占用率异常过高的情况，可能是因为主机的 CPU 策略设置不为 performance 模式，处理步骤如下：

(1) 查看当前主机的 CPU 策略是否为 performance，命令如下：

```
cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

(2) 若查看结果不为 performance，则需要修改 cpu 的资源策略为 performance，命令如下：

```
for i in $(ls /sys/devices/system/cpu/*/cpufreq/scaling_governor);do echo performance >
$i;done
```

#### 14. 若大数据平台管理系统被扫描出存在 CSRF（跨站点请求伪造）漏洞，如何处理？

---



修复 CSRF（跨站点请求伪造）漏洞后，第三方调用 BDP 接口时，需要在 HTTP 请求 Header 中增加“Referer:https://vip/”配置，其中 vip 为大数据平台管理系统的虚拟 IP。

---

修复 CSRF（跨站点请求伪造）漏洞的步骤如下：

- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 config.json 中配置的管理节点）。
- (2) 在 2 个管理节点上分别修改/data/bdp/system/webserver/configs/nginx.conf 文件。修改说明如[图 9-11](#)所示，在 nginx.conf 文件的 server 模块中增加如下内容：
  - 增加 valid\_referers 配置，配置值为大数据平台管理系统的虚拟 IP 和 2 个管理节点 IP（IP 之间以空格分隔）。
  - 在 location 模块中增加 invalid\_referer 判断（注意：只修改 location，新增的 invalid\_referer 判断内容与[图 9-11](#)所示严格保持一致）。
- (3) nginx.conf 文件修改完成后，保存退出。

图9-11 修改 nginx.conf 配置文件

```
server {
    listen      28014;
    server_name management0.hde.com;
    client_max_body_size 5000m;
    client_body_timeout 6500s;

    limit_req zone=dataengine burst=100;

    add_header X-Frame-Options 'SAMEORIGIN';
    add_header X-XSS-Protection '1; mode=block';
    add_header X-Content-Type-Options 'nosniff';

    valid_referers 10.121.68.160 10.121.68.161 10.121.68.162;

    location ~* "^/client/login(/|$)(.*)" {
        if ($invalid_referer) {
            return 403;
        }
        proxy_pass http://sso_server;
        proxy_set_header Host $host:80;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }

    location ~* "^/messages/logDownload" {
        if ($invalid_referer) {
            return 403;
        }
        rewrite /messages/logDownload/(.*) /$1 break;
        proxy_pass http://operlog_server;
        proxy_set_header Host $host:443;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }

    location ~* "^/api/sso(/|$)(.*)" {
        if ($invalid_referer) {
            return 403;
        }
        rewrite "(?i)/api/sso(/|$)(.*)" /$2 break;
        proxy_pass http://sso_server;
        proxy_set_header Host $host:80;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }

    location ~* "^/api" {
        if ($invalid_referer) {
            return 403;
        }
        rewrite /api/(.*) /$1 break;
        proxy_pass http://kong_server;
        proxy_set_header Host $host:443;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
```

(4) 重启 bdp-webserver 容器，命令如下：

/data/BDP/system/webserver/scripts/restart\_webserver.sh

## 15. 大数据平台管理系统访问不受信，且安装证书后仍然不受信处理方法

【现象描述】

大数据平台安装成功之后，因大数据平台使用的是自签证书，用户访问大数据平台管理系统时，浏览器不信任该证书信息，认为访问的是不安全的私密连接，从而对请求进行拦截，接口出现：**failed net::ERROR\_CERT\_AUTHORITY\_INVALID** 错误，导致无法访问。根据 [5.2](#) 章节导入浏览器安全证书并重启浏览器后，再次访问仍然提示不安全连接，访问接口出现该错误。

#### 【解决方法】

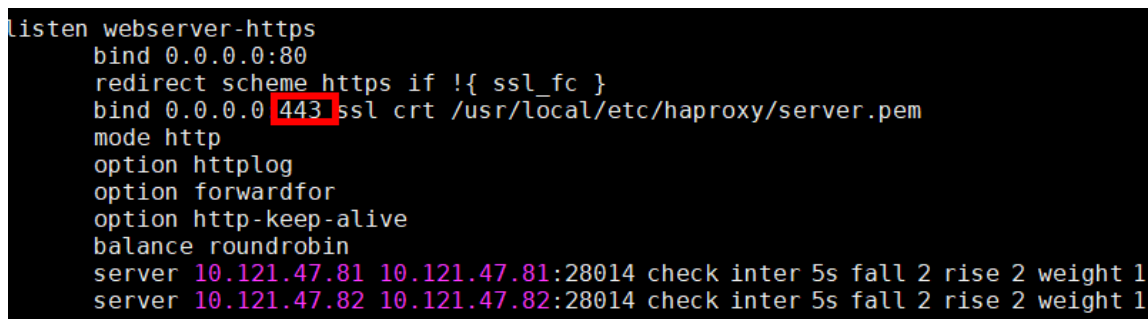
大数据平台管理系统访问地址的默认端口为：**443**，**443** 作为 **https** 协议的标准端口，但是因大数据平台使用的自签证书，可能环境中存在拦截或对 **443** 端口限制，导致安装根证书后，浏览器仍然不信任该证书。因此，此时可在大数据平台安装成功之后，通过修改大数据平台管理系统访问地址的默认端口号的方式进行解决。

#### 【处理步骤】

- (1) 分别登录安装大数据平台管理系统的 2 个管理节点（即 [3.4.2](#) 章节中在 `config.json` 中配置的管理节点）。在两个管理节点，分别执行以下操作（两个节点均需执行）。
- (2) 修改 `system.cfg` 文件中的 **443** 端口号为自定义端口（例如 **18443**），修改完成后保存，然后重启 `haproxy` 服务。命令如下：

```
vi /data/BDP/haproxy/conf/conf.d/system.cfg
sh /data/BDP/haproxy/restart_haproxy.sh
```

图9-12 修改 `system.cfg` 文件中的 **443** 端口号为自定义端口



```
listen webserver-https
    bind 0.0.0.0:80
    redirect scheme https if !{ ssl_fc }
    bind 0.0.0.0 443 ssl crt /usr/local/etc/haproxy/server.pem
    mode http
    option httplog
    option forwardfor
    option http-keep-alive
    balance roundrobin
    server 10.121.47.81 10.121.47.81:28014 check inter 5s fall 2 rise 2 weight 1
    server 10.121.47.82 10.121.47.82:28014 check inter 5s fall 2 rise 2 weight 1
```

- (3) 修改 `nginx.conf` 文件中的 **443** 端口号为自定义端口号（例如 **18443**，注意此端口必须与步骤(1)中自定义端口号保持一致），修改完成后保存，然后重启 `webserver` 服务。命令如下：

```
vi /data/BDP/system/webserver/configs/nginx.conf
sh /data/BDP/system/webserver/scripts/restart_webserver.sh
```

图9-13 修改 nginx.conf 文件中的 443 端口号为自定端口号

```
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}

location ~* "^/messages/logDownload" {
    rewrite /messages/logDownload/(.*) /$1 break;
    proxy_pass http://operlog_server;
    proxy_set_header Host $host:443;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}

location ~* "^/api/sso(/|$)(.*)" {
    rewrite "(?i)/api/sso(/|$)(.*)" /$2 break;
    proxy_pass http://sso_server;
    proxy_set_header Host $host:80;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}

location ~* "^/api" {
    rewrite /api/(.*) /$1 break;
    proxy_pass http://kong_server;
    proxy_set_header Host $host:443;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}

location = / {
    proxy_set_header Host $host:443;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    return 301 https://$host:443/platform/;
}

location ~* "/" {
    root /etc/static/dist;
    expires 168h;
    proxy_set_header Host $host:443;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    try_files $uri $uri/ /index.html?&args;
}
```

- (4) 以上配置全部修改完成后，通过大数据平台管理系统的 URL 新地址：<https://<管理系统访问的虚ip>:自定义端口号>（例如：[18443](https://18443)）重新访问大数据平台管理系统，此时访问连接将变为安全的连接。