

虚谷实时数据服务平台V2.0安装部署手册

本文面向实施工程师和平台运维人员，说明如何准备安装环境、配置离线整包、部署平台、验证服务，并完成后续扩容与升级。当前平台采用 Kubernetes 和 Helm；可由安装器初始化集群，也可部署到已准备好的Kubernetes 集群。

文档信息	内容
编制日期	2026年6月17日
文档版本	1.0
适用范围	与本次核对脚本接口一致的离线整包；具体产品版本以交付包签名清单为准

1 部署组成与边界

系统采用典型B/S微服务架构，容器化通过K8S部署，用户通过浏览器访问入口服务，入口将请求转发至网关和相应业务服务。虚谷数据库、Redis、Nacos 等提供基础支撑；对象存储、元数据目录、血缘、质量、调度和计算组件随所选功能域及依赖关系部署。

平台管理是必装基座。数据治理、数据开发、数据应用及 AI 智能按交付范围选择；知识库与智能问数分别控制。完整离线包负责提供相应架构的二进制、镜像、Chart、初始化与安装脚本及第三方许可证。

单节点初始化便于首次交付，但不代表高可用。增加工作节点也不会自动形成多控制平面、数据库高可用或共享存储。并发量、吞吐量与恢复目标应按现场容量规划和测试结果单独确认。

2 安装环境准备

2.1 服务器操作系统兼容范围

平台支持以下服务器操作系统环境，可根据项目基础设施选择相应环境。

操作系统	支持版本
统信（UOS）	V25

麒麟	V10 SP2 / SP3
openEuler	24.03 LTS-SP3
麒麟信安	V6 / V6 SP1
CentOS	7.4
Ubuntu	22.04 LTS

服务器架构应与交付制品一致，按实际提供的 amd64 （x86-64）或 arm64 安装包选择。本文后续安装命令采用 Linux Kubernetes 部署示例。

2.2 客户端浏览器兼容范围

平台通过浏览器访问，客户端无需安装平台业务服务。支持的浏览器及版本如下。

浏览器	支持版本
Google Chrome	130 及以上
Microsoft Edge	130 及以上
Mozilla Firefox	128 及以上
奇安信浏览器	V1.1.45966.52 及以上

浏览器应允许平台正常使用 JavaScript、登录会话所需的 Cookie 或本地存储，以及授权场景下的上传、下载和新窗口操作。部署 HTTPS 时，应确保客户端信任平台证书及其证书链。

2.3 Linux Kubernetes 部署资源与基础要求

项目	要求与核对方式
操作系统与架构	服务器操作系统兼容范围见第2.1节；选择与目标部署环境及 CPU 架构匹配的交付包。
账号与工具	具备 root 或 sudo 权限。准备 Bash、Python 3、OpenSSL；按整包预检补齐离线工具。Kubernetes、Helm 等使用包内匹配版本。
CPU 与内存	安装器预检下限为2核、MemAvailable不低于4096MB。这只是初始预检门槛，不能作为全模块运行配置或并发承诺。
数据盘	DATA_ROOT 所在文件系统可用空间硬下限100GB；默认低于400GB告警。按数据、对象、向量、日志、备份增长额外规划容量。

其他磁盘	分别检查 /var/lib/containerd、/opt/datagolden/images 和临时目录；脚本包含30GB、20GB、10GB及 inode 阈值，按文件系统去重检查。
节点基础	固定 IP 和唯一主机名；时间同步；关闭 swap。DATA_ROOT 使用独立业务目录，不能指向系统根目录或受保护系统目录。
容量确认	结合所选模块的 Chart requests/limits、运行副本、计算任务和升级滚动余量确定资源；全域上线前应另做容量测试。

2.4 部署前检查命令

cat /etc/os-release

uname -m

uname -r

nproc

free -h

df -h

df -i

swapon --show

timedatectl status

ip -br addr

自建集群安装会调整宿主机运行配置，包括容器运行时、内核网络参数、swap 和防火墙服务。现行脚本含关闭并屏蔽 firewalld 的处理；生产部署前应由运维明确主机与网络边界策略，避免在共享业务主机上直接运行。已有集群路径不执行此类宿主机初始化。

3 网络与安装参数

通信范围	端口及用途
用户到平台入口	HTTP 80；HTTPS 443 仅在证书及 TLS 入口正确配置后使用。仅监听443不等于HTTPS已经可用。
运维与节点通信	SSH通常为TCP 22；Kubernetes API为TCP 6443，kubelet为TCP 10250。仅向必要管理网段和节点开放。
集群内部	

	按控制平面及 CNI 实际配置放通；etcd 2379–2380仅限必要内部访问，Calico 网络和DNS须互通。
可选 NodePort	只按实际服务开放所用端口；范围通常为30000–32767，不建议整体向用户网络开放。
外部依赖	放通业务数据源、模型API、邮件或其他已配置服务的目标地址和端口。离线安装不代表AI推理无需模型服务。

配置安装文件

解压正式交付的整包，进入包含 install.sh 的目录，编辑 config/install.conf。安装配置会被脚本读取，应仅接受可信配置文件。不要将密码写入手册、工单或共享日志。

参数	配置说明
NODE_IP / DOMAIN	填写实际节点或入口地址、平台访问域名；多网卡及非交互场景明确指定地址。
DATA_ROOT	默认 /data/datagolden；安装前核对挂载点与容量。
NAMESPACE / RELEASE_NAME	默认均为 datagolden；以下示例沿用默认值。
STORAGE_CLASS / INGRESS_CLASS	默认 datagolden-local-path / traefik；已有集群使用已就绪的存储类和入口控制器。
DEPLOY_DOMAINS	常用值 platform,governance,data_dev,consumer,ai_smart；all表示按包内范围全域启用，platform始终启用。不得选包内未交付模块。
AI 子功能	AI_KNOWLEDGE_BASE_ENABLED 和 AI_ASK_DATA_ENABLED 分别控制知识库和问数；模型地址及密钥按现场服务设置。
管理员及密钥	ADMIN_USERNAME默认admin；ADMIN_PASSWORD留空随机生成。其他秘密按模板或安装器生成流程管理，升级必须保留已有身份与密钥。
MASTER_AUTO_ENROLL	当前默认false。确需自动纳管时设置true并配置专用SSH凭据；也可安装后在平台手工纳管。

4 首次安装操作

4.1 接收并核对安装包

核对交付版本、CPU架构、功能域组合及发布摘要。将安装包上传至专用目录；检查交付渠道提供的校验值。安装器还会校验包内发布签名和相关内容，校验失败应停止并取得正确制品。

```
tar -xzf <安装包文件名>.tar.gz
```

```
cd <解压后的安装包目录>
```

```
vi config/install.conf
```

```
chmod 600 config/install.conf
```

```
./install.sh --help
```

4.2 填写站点配置

以下为平台、治理、开发及应用组合示例。地址仅为示意，应替换为真实地址；凭据由安全交付渠道管理。已有安装禁止用空白初始配置覆盖现场配置。

```
NODE_IP=192.0.2.10
```

```
DOMAIN=datagolden.example.internal
```

```
DATA_ROOT=/data/datagolden
```

```
NAMESPACE=datagolden
```

```
RELEASE_NAME=datagolden
```

```
DEPLOY_DOMAINS=platform,governance,data_dev,consumer
```

```
MASTER_AUTO_ENROLL=false
```

4.3 执行安装

```
sudo ./install.sh --bootstrap-cluster
```

阶段	主要结果
preflight	完成预检与宿主机准备。
cluster	初始化 kubeadm 集群，准备节点与网络基础。
storage	配置存储与持久化目录。
images	校验并准备离线镜像与扩容物料。
platform	提交 Helm Release，执行所需初始化并等待核心服务。
verify	验证部署资源、依赖健康、入口认证和适用业务只读接口。

默认入口 `sudo ./install.sh` 同样执行自建集群安装。cgroup v2 使用 `systemd`，v1/hybrid 使用 `cgroupfs`；安装器在初始化前校验一致性。初始化失败保留现场，不应直接手工 `reset` 或反复全量重装。

5 部署到已有 Kubernetes 集群

本章适用于已由运维准备的集群。安装器通过 `kubeconfig` 访问目标集群，不初始化节点、不替换 CNI，也不按节点数量自动决定存储或调度配置。

5.1 核对前置条件

确认 `kubeconfig` 指向正确环境且权限满足部署需求；核对 Kubernetes 与包内 Chart 的兼容性。存储类、Ingress Controller、DNS、节点容量以及所需 Operator 等基础条件应已满足。涉及 AI/Ray 时，须确认相应 CRD 与 Operator 依赖。

```
kubectl --kubeconfig=<配置文件> get nodes
```

```
kubectl --kubeconfig=<配置文件> get storageclass
```

```
kubectl --kubeconfig=<配置文件> get ingressclass
```

```
helm --kubeconfig=<配置文件> list -A
```

在所有可调度节点准备好所需镜像，或配置各节点均可访问的镜像仓库及凭据。只向安装机导入镜像不足以满足多节点部署。核对实际调度架构、镜像摘要、PVC及已有资源归属。

5.2 执行部署

在 `config/install.conf` 中填写站点域名、部署模块和已有入口类别。下面命令中的地址须为真实访问入口；`--skip-images` 是已有集群路径的必要确认，不能用来跳过尚未完成的镜像准备。

```
sudo ./install.sh \
```

```
--kubeconfig=/secure/target-cluster.conf \
```

```
--storage-class=<已就绪的存储类> \
```

```
--node-ip=<实际入口IP> \
```

```
--skip-images
```

随后按第6章执行验证。`--bootstrap-cluster` 与 `--kubeconfig` 不能同时使用。`--dry-run` 可用于只渲染 Helm 清单，但渲染成功不证明镜像、存储、凭据或业务接口可用。渲染文件可能包含敏感配置，应限制访问。

5.3 存量环境保护

已有 DataGolden 环境应使用正式升级流程，不把整包初装当作升级。接管旧资源前核对 Helm 所属、不可变字段、PVC绑定、Nacos配置及Secret；不得通过删除卷、重新生成数据库密码或强制替换资源解决冲突。

配置覆盖顺序为公共 values.yaml、环境配置、站点或发布参数。离线环境使用 environments/offline.yaml，并由安装器生成现场参数。不得直接套用 local、dev、test 的地址、节点标签及资源预算。

部署方式选择

现场情况	使用方式
新服务器首次安装	第4章初始化集群后安装。
已有可用Kubernetes集群	本章已有集群路径。
已有DataGolden待升级	第8章正式升级包。
需要增加工作节点	第7章平台节点纳管与扩容。

6 安装验证与首次登录

6.1 检查资源和入口

```
kubectl get nodes
kubectl get pods -n datagolden
kubectl get deploy,statefulset -n datagolden
kubectl get pvc -n datagolden
kubectl get ingress,svc -n datagolden
helm status datagolden -n datagolden
```

节点应为 Ready，预期工作负载达到目标就绪副本数，使用中的 PVC 为 Bound。初始化 Job 成功后显示 Completed 属于正常现象；不应要求所有 Pod 永久为 Running。

将 DOMAIN 解析至实际入口地址。无 DNS 时，在访问端 hosts 中添加“入口IP 域名”。浏览器使用该域名访问平台；HTTPS需另确认有效证书、信任链和入口路由。

6.2 执行完整快速自检

```
sudo ./install.sh --only-stage=verify
```

整包安装会自动执行本阶段。重复验收可单独运行，无需重装。SELF_CHECK_BASE_URL 可设置正式入口，SELF_CHECK_CA_FILE 可指定私有CA。管理员凭据可通过权限为600的JSON文件提供，并由SELF_CHECK_CREDENTIALS_FILE 引用。

结果	含义
退出码0	通过本次适用的基础部署检查。
退出码1	检查失败。
退出码2	凭据、验证码、权限等必要条件阻塞。
退出码3	运行、报告或超时故障。

报告位于 diagnostics/self-check/self-check-<run_id>.json。自检覆盖适用部署资源、部分依赖健康、登录身份及已登记模块的只读API，并注销本轮会话。基础 healthcheck.sh 仅供诊断，不能代替完整验收。

6.3 获取初始凭据并登录

```
sudo ./install.sh --show-credentials
```

在受控交互终端查看凭据，不重定向到共享日志。完整凭据保存在 config/install.conf.resolved，应受限保管。使用管理员账号登录并按提示修改初始密码，再检查租户、角色、数据源及所选模块入口。

基础自检通过不代表任务执行、数据写入、AI推理、权限隔离、性能或故障切换验收通过。上线前应按交付范围另做代表性业务验证，记录实际版本及结果。

7 日常运维与节点扩容

7.1 配置与数据管理

普通部署参数由 Chart、环境和站点文件分层管理；应用参数通过 Nacos 管理；密码与令牌使用 Kubernetes Secret。凭据轮换需同步所有依赖方，不能只改 Secret 而不更新数据库角色或外部服务。

默认本地存储依赖所在节点，不能自动跨节点恢复。保留原PVC身份和数据目录；监控数据库、对象存储、向量数据、容器镜像与日志空间。SeaTunnel驱动缓存使用独立PVC，存量卷模板变更需执行专门

迁移，不能强制更新。

7.2 日志与健康查询

```
kubectrl get events -n datagolden --sort-by=.lastTimestamp
```

```
kubectrl describe pod <Pod名称> -n datagolden
```

```
kubectrl logs <Pod名称> -n datagolden --tail=200
```

```
kubectrl logs <Pod名称> -n datagolden --previous --tail=200
```

多容器Pod需追加 -c <容器名>。平台自有服务主要输出 stdout/stderr；新集群 kubelet 日志轮转配置为单文件10Mi、每容器5个文件，不能据此推导全节点容量或保留天数。已有集群需单独核对节点实际配置。

7.3 扩容工作节点

扩容前准备与主节点同发行版、同大版本、同架构的机器，设置独立主机名、固定IP、时间同步及SSH访问。确认节点间网络、主节点扩容二进制和镜像物料可用；默认关闭自动纳管时，先在平台纳管主节点。

在平台管理的运维中心进入资源管理，新增机器并测试连接。保存后选择目标机器执行“加入集群”，核对目标及影响后确认。平台分发运行组件和镜像、执行加入流程并等待节点就绪。以实际页面任务结果和集群状态共同判定成功。

```
kubectrl get nodes -o wide
```

```
kubectrl get pods -A -o wide --field-selector spec.nodeName=<新节点名>
```

节点Ready后仍需核对镜像、存储、节点选择条件及实际工作负载调度。加节点不会自动增加全部业务副本，也不会迁移本地持久化数据。反向代理需要支持扩容进度使用的SSE长连接，关闭响应缓冲并设置匹配的超时。

7.4 备份安排

按恢复目标建立定期备份，涵盖数据库、对象存储、必要向量及持久卷数据、配置中心、站点配置和受控凭据。保存异机副本并进行恢复演练。升级内置备份不等同于覆盖所有数据组件的长期容灾方案。

8 升级恢复与卸载

8.1 升级准备与执行

取得与当前源版本、功能域Profile和CPU架构匹配的正式升级包，核对签名、源与目标版本以及现场镜像。增量升级只处理已部署且被选中的模块，不承担新增、移除功能域或降级。

安排维护窗口，确认备份空间、运行作业和外部写入的处理方式。升级前数据库dump及可读性检查、对象备份与部署事实快照须成功。需要跨存储一致恢复点时，应先停止业务写入。

```
tar -xzf <升级包文件名>.tar.gz
```

```
cd <升级包解压目录>
```

```
sudo ./install-upgrade.sh
```

由升级入口编排备份、镜像准备、配置及数据库变更、Helm更新和检查。多节点场景确认实际调度节点均有目标镜像。升级完成后重新执行基础检查和关键业务验证，记录发布版本、结果及备份位置。

8.2 恢复条件

备份目录应包含 backup-complete.json 和 backup.sha256；缺失完整性标记的备份不能直接作为自动恢复依据。Helm回滚只恢复应用与配置，不撤销数据库迁移。Flyway历史脚本不得修改或删除。

必须先停止应用、调度器和外部写入，再按升级包恢复合同操作。以下命令仅在已确认写入停止、备份目标正确且维护窗口获准后使用；环境变量是操作声明，不能替代实际停写。

```
sudo env RESTORE_WRITES_STOPPED=true \  
bash steps/99-restore.sh <已验证的备份目录>
```

恢复会校验摘要、Release及revision，恢复数据库和对象并回到备份对应的应用revision。对象恢复可能移除备份后新增的对象。任一步失败都应保留现场，完成业务核验后才能恢复写入。

8.3 卸载范围

命令	影响
sudo ./uninstall.sh	默认卸载Helm Release，保留集群、命名空间及数据。
--purge	删除命名空间及其资源；PVC和存储回收策略可能导致数据删除。
--reset-node	额外执行节点 kubeadm reset，影响该节点集群运行。
--all	删除平台、集群以及DATA_ROOT数据，属于不可逆清理。

卸载前核对Release、命名空间、节点及绝对数据目录，完成备份并取得相应清理授权。升级或排障不能以卸载重装作为默认处理。

9 常见问题与故障排查

现象	优先检查与处置
签名或摘要校验失败	核对交付包是否完整、架构与版本是否匹配；从可信发布渠道重新获取，不能关闭校验继续安装。
预检失败	检查OS、内核、CPU、可用内存、磁盘、inode、时间与工具依赖。资源不足先补齐，不将告警接受参数作为容量达标证明。
kubeadm 初始化失败	保留日志，检查containerd、CRI、cgroup及端口占用；--reset-partial-kubeadm会清理未完成现场，仅在确认目标与风险后使用。
Pod Pending 或 PVC Pending	查看Pod事件、requests、节点选择条件及StorageClass；核对PV容量、目录和绑定，不删除旧PVC强行重建。
ImagePullBackOff	检查镜像名称、架构、摘要、节点导入结果和仓库访问凭据；已有集群检查所有实际调度节点。
CrashLoopBackOff	查看当前及previous日志；检查数据库、Secret、Nacos和Flyway失败原因。不禁用迁移或伪造成功状态。
页面无法访问	依次检查域名解析、80或已配置TLS入口、Ingress、Service、网关和业务Pod；请求域名需与入口规则一致。
登录或自检阻塞	检查有效管理员凭据、首次改密状态、验证码和角色授权；不通过关闭认证或补造权限绕过验收。
AI页面可见但调用失败	检查部署子功能、模型地址、API密钥、网络和模型兼容性；组件就绪不代表模型调用成功。
扩容进度停止更新	区分SSE显示中断与后端执行失败，检查平台任务及节点真实状态、代理缓冲和超时；避免重复提交加入任务。

阶段恢复命令

```
./install.sh --status
./install.sh --list-stages
sudo ./install.sh --resume
sudo ./install.sh --only-stage=platform
sudo ./install.sh --from-stage=platform
```

修复原因后再选择恢复入口。--reset-state 会清除已有阶段记录，不是常规重试方式。排障材料应提供失败阶段、时间、包版本和脱敏日志，避免携带凭据。

10 交付验收与文档依据

10.1 交付验收清单

验收项	应保存的结果
环境与制品	OS及SP版本、架构、节点、资源、包版本、功能域组合、签名或摘要核对记录。
浏览器兼容性	Chrome 130及以上、Edge 130及以上、Firefox 128及以上、奇安信浏览器 V1.1.45966.52及以上的约定测试版本和核心功能验证记录。
配置与入口	域名、IP、证书、存储类、命名空间、Release和站点配置；秘密通过单独受控渠道移交。
资源与基础自检	节点和工作负载就绪、PVC绑定、自检JSON及安装报告。
登录与模块	管理员首登改密、租户及角色检查、已部署模块可访问。
业务与性能	代表性同步或质量任务、所选AI功能等实际结果；并发和性能另附测试报告。
运维与恢复	监控、日志、备份位置、恢复演练或计划、维护责任人及支持渠道。

10.2 关键文件位置

位置	用途
config/install.conf	安装输入参数。
config/install.conf.resolved	最终解析凭据与参数，按敏感文件管理。
install.state	包目录阶段状态；系统副本位于 /var/lib/datagolden/install.state。
/var/log/datagolden-install.log	安装全量日志。
install-report.log	安装交付报告。
diagnostics/	阶段失败诊断及 self-check 下的自检报告。

10.3 编制依据与适用说明

本文以现行安装脚本及Chart为主要依据。历史单机指南中的“只支持新建集群”“主节点默认自动纳管”和“本地Compose”描述已不沿用；使用 --kubeconfig、MASTER_AUTO_ENROLL=false 及当前Kubernetes运行规范。

deploy/package/install-templates/install.sh.tpl

deploy/package/install-templates/install.conf.tpl

deploy/package/install-templates/lib/os-pkg.sh

deploy/package/install-templates/install-upgrade.sh.tpl

deploy/package/install-templates/steps/00b-backup.sh 与 99-restore.sh

deploy/charts/datagolden/values.yaml 与 environments/offline.yaml

deploy/package/README.md 与 deploy/README.md

docs/deployment/zh-CN/scale-out.md（扩容流程参考）

本文件是安装操作说明，不是本次现场安装或性能验收报告。交付前须将实际产品版本、环境参数和验收记录与目标安装包再次对应核对。