天翼云科技有限公司

云日志服务

用户手册

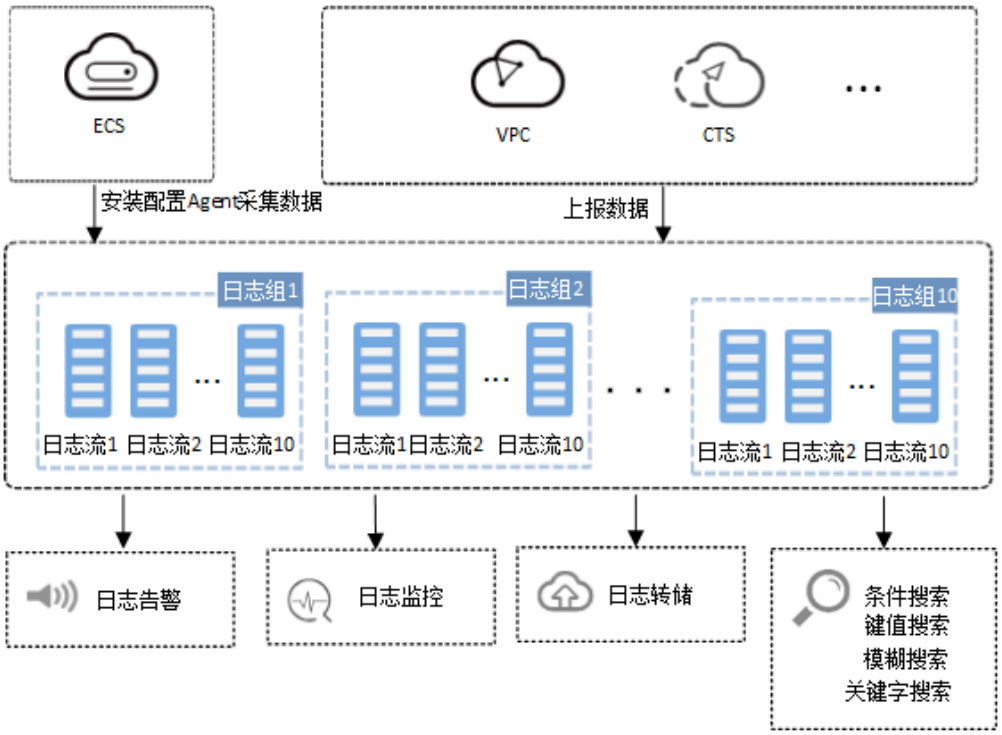
目 录

1 产品介绍

1.1 云日志服务

云日志服务（Log Tank Service，简称 LTS），用于收集来自主机和云服务的日志数据，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为您提供一个实时、高效、安全的日志处理能力，帮助您快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

图1-1 云日志服务示意图



日志采集与分析

云日志服务可以采集主机和云服务的日志数据，采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

1.2 基本功能

实时采集日志

云日志服务提供实时日志采集功能，采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。

日志查询与实时分析

对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

日志转储

主机和云服务的日志数据上报至云日志服务后，默认存储时间为 7 天，可以在 1-30 天之间进行设置。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至对象存储服务（OBS）中长期保存。

1.3 应用场景

日志采集与分析

主机和云服务的日志数据，不方便查阅并且会定期清空，云日志服务采集日志后，日志数据可以在云日志控制台以简单有序的方式展示、方便快捷的方式进行查询，并且可以长期存储。对采集的日志数据，可以通过关键字查询、模糊查询等方式简单快速地进行查询，适用于日志实时数据分析、安全诊断与分析、运营与客服系统等，例如云服务的访问量、点击量等，通过日志数据分析，可以输出详细的运营数据。

合理优化业务性能

网站服务（数据库、网络等）的性能和服务质量是衡量用户满意度的关键指标，通过用户的拥塞记录日志发现站点的性能瓶颈，以提示站点管理者改进网站缓存策略、网络传输策略等，合理优化业务性能。例如：

- 分析历史网站数据，构建业务网络基准。
- 及时发现业务性能瓶颈，合理扩容或流量降级。
- 分析网络流量，优化网络安全策略。

快速定位网络故障

网络质量是业务稳定的基石，将日志上报至云日志服务，确保问题发生时能及时查看、定位问题，助力您快速定位网络故障，进行网络回溯取证。例如：

- 快速定位问题根源的云服务器，例如带宽过度使用的云服务器。
- 通过分析访问日志，判断业务是否遭到了攻击、非法盗链和不良请求等，及时定位并解决问题。

2 日志组

2.1 创建日志组

操作场景

该任务指导用户创建日志组。目前每个账号在一个区域下最多可以创建 100 个日志组。

前提条件

已获取控制台的登录账号与密码。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 单击“创建日志组”。
5. 在“创建日志组”页面中，输入日志组名称。
6. 单击“确定”，完成日志组的创建。

2.2 查看日志组

操作场景

对于已经创建的日志组，用户可以在日志管理页面进行查看。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已创建日志组。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中查看日志组相关信息。

2.3 删除日志组

操作场景

该任务指导用户删除日志组。

说明

日志组删除后无法恢复，请谨慎操作。

前提条件

- 已获取控制台的登录账号与密码。
- 确认日志组关联的日志转储任务已删除。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中，单击待删除日志组所在行的“删除”。
5. 单击“确定”，完成日志组删除。

3 日志流

3.1 创建日志流

操作场景

该任务指导用户在日志组下创建日志流。

前提条件

- 已获取控制台的登录账号与密码。
- 已创建日志组。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 单击已创建的日志组名称，进入该日志组页面。
5. 单击“创建日志流”。
6. 在“创建日志流”页面中，输入日志流名称。
7. 单击“确定”，完成日志主题的创建。

3.2 查看日志流

操作场景

对于已经创建的日志流，用户可以在日志管理页面进行查看。

前提条件

- 已获取控制台的登录账号与密码。
- 日志组已创建。
- 日志流已创建。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中单击日志流对应的日志组，进入该日志组下的日志流列表页面。
5. 查看日志流相关信息。

3.3 删除日志流

操作场景

该任务指导用户对不再使用的日志流进行删除。

说明

用户删除日志流时，需确保该日志流下没有关联的日志转储任务。日志流删除后无法恢复，请谨慎操作。

前提条件

- 已获取控制台的登录账号与密码。
- 已确认日志流关联的日志转储任务已删除。
- 删除云审计服务相关的日志组时，需要先删除该日志组在云审计中对应的追踪器。

操作步骤

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中单击该日志流对应的日志组，进入该日志组下的日志流列表页面。
5. 在日志流列表中，单击待删除日志流所在行的“删除”。

6. 单击“确定”，完成日志流删除。

3.4 日志接入

3.4.1 主机接入

将主机待采集日志的路径配置到日志流中，ICAgent 将按照日志采集规则采集日志，并将多条日志进行打包，以日志流为单位发往云日志服务，您可以在云日志服务控制台实时查看日志。

LTS 目前只支持 ECS 日志采集，暂不支持容器化日志采集，如果需要采集容器化日志，可以使用 AOM 服务。

前提条件

- 已创建日志组。
- 已创建日志流。
- 已安装 ICAgent。

操作步骤

1. 在云日志服务管理控制台，单击日志组名称，日志将被采集至该日志组。
2. 单击日志流名称，日志将被采集至该日志流。
3. 在左侧导航栏单击“日志接入-主机接入”
4. 单击“新增路径”，进入“新增采集配置”页面。
5. 在“添加主机”步骤，选择“Linux 主机”或“Windows 主机”，然后勾选您需要收集日志的主机名，单击“下一步”。
6. 在“配置采集路径”步骤，添加您需要收集日志路径，LTS 按照配置的路径进行日志采集。
   - **采集路径支持递归路径，**表示递归 5 层目录。**

     示例：采集路径配置为 /var/logs/**/a.log，日志匹配如下：

     ```
     /var/logs/1/a.log
     /var/logs/1/2/a.log
     /var/logs/1/2/3/a.log
     /var/logs/1/2/3/4/a.log
     /var/logs/1/2/3/4/5/a.log
     ```

说明

- Windows 环境日志采集路径暂不支持递归路径，配置样例：C:\var\service\a.log。
- 以上示例中的/1/2/3/4/5/，表示/var/logs 目录中，往里递归的 5 个目录层级，在这 5 个目录层级中只要存在 a.log，都能进行日志匹配。
- 采集路径中只能出现一次**，不能出现两个及以上。正确示例：/var/logs/**/a.log；错误示例：/opt/test/**/log/**。
- 采集路径中第一个层级不允许为**（避免误采集系统文件），错误示例：/**/test。

   - **采集路径支持模糊匹配，匹配目录或文件名中的任何字符**。

说明

- Windows 环境日志采集路径暂不支持模糊匹配，配置样例：C:\var\service\a.log。
- 如果配置了 C:/windows/system32 类似的日志采集路径，但无法采集日志，请尝试打开 WAF 物理防火墙后重新配置。
  - 示例 1：采集路径配置为 /var/logs/*/a.log，表示/var/logs/目录下，任何一个目录中存在 a.log，都能进行日志匹配，例如：
    /var/logs/1/a.log
    /var/logs/2/a.log
  - 示例 2：采集路径配置为 /var/logs/service-*/a.log，日志匹配示例：
    /var/logs/service-1/a.log
    /var/logs/service-2/a.log
  - 示例 3：采集路径配置为 /var/logs/service/a*.log，日志匹配示例：
    /var/logs/service/a1.log
    /var/logs/service/a2.log

- 采集路径如果配置的是目录，示例：/var/logs/，则只采集目录下后缀为“.log”、“.trace”和“.out”的文件；
  如果配置的是文件名，则直接采集对应文件，只支持文本类型的文件。

说明

- 请注意您的敏感信息是否在收集范围内。
- 当主机选择“Windows 主机”时，如需采集系统日志，需要在“配置采集路径”环节，开启“采集 windows 系统日志”。
- LTS 暂不支持采集 PostgreSQL（数据库）实例的日志，目前只支持采集安装在 ECS（主机）实例的日志。
- **日志采集路径不能重复配置**，即相同主机的同一个日志采集路径不能在不同的日志流重复配置，否则可能会导致日志采集异常。
- 相同主机的同一个日志采集路径，如果在 AOM 进行了配置，则不能在 LTS 重复配置。
- 只支持文本类文件的采集。
- 配置的文件的最后修改时间和当前时间差如果已超过 12 小时，则不会采集。

7. 单击“下一步”，进入“配置采集信息”步骤。

表3-1 日志采集信息

名称	说明
日志格式	• 单行日志：采集的日志文件中，如果您希望每一行日志在 LTS 界面中都显示为一条单独的日志数据，则选择单行日志。 • 多行日志：采集的日志中包含像 java 异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志则每一行都显示为一条单独的日志数据，则选择多行日志，方便您查看日志并且定位问题。
日志时间	系统时间：表示系统当前时间，默认为日志采集时间，每条日志的行首显示日志的采集时间。 说明 日志打印时间：系统产生并打印日志的时间；日志采集时间：Agent 采集

名称	说明
	日志，并且发送到云日志服务的时间。 Agent 采集日志并发送日志到云日志平台的频率为 1 秒钟。

	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。
	• 如果日志中的时间格式为：2019-01-01 23:59:59，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss。
	• 如果日志中的时间格式为：19-1-1 23:59:59，时间通配符应该填写为：YY-M-D hh:mm:ss。
	说明
	如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。
	填写示例：
	`YY - year (19)`
	`YYYY - year (2019)`
	`M - month (1)`
	`MM - month (01)`
	`D - day (1)`
	`DD - day (01)`
	`hh - hours (23)`
	`mm - minutes (59)`
	`ss - seconds (59)`
	`hpm - hours (03PM)h:mmpm`
	`- hours:minutes (03:04PM)h:mm:sspm`
	`- hours:minutes:seconds (03:04:05PM)`
	`hh:mm:ss ZZZZ (16:05:06 +0100)`
	`hh:mm:ss ZZZ (16:05:06 CET)`
	`hh:mm:ss ZZ (16:05:06 +01:00)`

分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

说明

时间通配和正则表达式均是从每行日志的开头进行严格匹配，如果匹配不上，则会默认使用系统时间上报，这样可能会和文件内容中的时间不一致。例如：时间通配符配置为：YYYY-MM-DD hh:mm:ss，日志内容为[2019-01-01 23:59:59]，将会匹配失败。**如果没有特殊需求，建议使用单行日志-系统时间模式即可**。

8. 单击“确认”，完成日志采集规则配置。此时，云日志服务将按照设定的采集规则进行日志采集。

   日志成功采集后，如果您的日志采集路径等发生变化，还可以修改日志采集配置。

4 Agent

4.1 安装 ICAgent

ICAgent 是云日志服务进行日志采集的工具，运行在需要采集日志的服务器中。首次使用云日志服务采集日志时，需要安装 ICAgent，并配置日志采集规则。

前提条件

在进行 ICAgent 安装前，需要先确保本地浏览器时间与服务器时区、时间都一致。若有多个服务器，则要保证本地浏览器、多个服务器的时区、时间都一致。否则，可能会导致安装后不能在界面上准确查看日志信息。

安装方式说明

ICAgent 有两种安装方式，您可以按照您的场景进行选择。

表4-1 安装方式

方式	适用场景
首次安装	当满足以下条件时，您需要按照该方式安装： 该服务器上未安装过 ICAgent。
继承安装	当满足以下条件时，您需要按照该方式安装： 您有多个服务器需要安装 ICAgent，其中一个服务器已经通过首次安装方式装好了 ICAgent，对于没有安装 ICAgent 的服务器，您可以采用该安装方式。

首次安装

您可以通过以下操作在弹性云服务器上安装 ICAgent。

步骤 1 通过新增访问密钥获取永久 AK/SK，请参考 8.1 如何获取 AK/SK？章节获取 AK/SK。

步骤 2 选择“管理与部署 > 云日志服务”，进入云日志服务界面。

步骤 3 在左侧导航栏，单击“Agent 管理”，进入“Agent 管理”页面。

步骤 4 单击“安装 ICAgent”。

步骤 5 生成 ICAgent 安装命令。

在文本框中输入已获取的 AK/SK，生成 ICAgent 安装命令。单击“复制命令”，复制 ICAgent 安装命令。

说明

请确保输入正确的 AK/SK，否则将无法安装 ICAgent。

步骤 6 使用 PuTTY 等远程登录工具，以 **root** 用户登录待安装 ICAgent 的服务器，执行 ICAgent 安装命令进行安装。

说明

- 当显示“ICAgent install success”时，表示安装成功，ICAgent 已安装在了/opt/oss/servicemgr/目录。安装成功后，在云日志服务左侧导航栏中选择“Agent 管理”，查看该服务器 ICAgent 的状态。
- 如果安装失败，请参考 4.3 卸载 ICAgent 章节卸载 ICAgent 后重新安装，如果还未安装成功，请联系技术支持。

----结束

继承安装

您有多个服务器需要安装 ICAgent，其中一个服务器已经通过首次安装方式装好了 ICAgent，且该服务器“/opt/ICAgent/”路径下存在 ICAgent 的安装包 **ICProbeAgent.tar.gz**，对于没有安装 ICAgent 的服务器，可以通过该方式对服务器进行一键式继承安装。

步骤 1 在已安装 ICAgent 的服务器上执行如下命令，其中 *x.x.x.x* 表示待安装 ICAgent 服务器的 IP 地址。

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -ip x.x.x.x

步骤 2 根据提示输入待安装 ICAgent 的服务器 root 用户密码。

说明

- 如果已安装 ICAgent 的服务器安装过 expect 工具，执行上述命令后，即可完成安装。如果已安装 ICAgent 的服务器未安装 expect 工具，请根据提示输入密码，进行安装。
- 请确保已安装 ICAgent 的服务器可以使用 root 用户执行 SSH、SCP 命令，来与待安装 ICAgent 的服务器进行远端通信。

- 当显示“ICAgent install success”时，表示安装成功，ICAgent 已安装在了/opt/oss/servicemgr/目录。安装成功后，在云日志服务左侧导航栏中选择“Agent 管理”，查看该服务器 ICAgent 的状态。
- 如果安装失败，请参考 4.3 卸载 ICAgent 章节卸载 ICAgent 后重新安装，如果还未安装成功，请联系技术支持。

----结束

继承批量安装

您有多个服务器需要安装 ICAgent，其中一个服务器已经通过首次安装方式装好了 ICAgent，且该服务器“/opt/ICAgent/”路径下存在 ICAgent 的安装包 **ICProbeAgent.tar.gz**，对于没有安装 ICAgent 的服务器，可以通过该方式对服务器进行一键式继承批量安装。

须知

批量安装的服务器需同属一个 VPC 下，并在同一个网段中。

前提条件

已收集需要安装 Agent 的所有服务器的 IP 地址、密码，按照 iplist.cfg 格式整理好，并上传到已安装过 ICAgent 机器的/opt/ICAgent/目录下。iplist.cfg 格式示例如下所示，IP 地址与密码之间用空格隔开：

192.168.0.109 密码（请根据实际填写）

192.168.0.39 密码（请根据实际填写）

说明

- iplist.cfg 中包含您的敏感信息，建议您使用完之后清理一下。
- 如果所有服务器的密码一致，iplist.cfg 中只需列出 IP，无需填写密码，在执行时输入此密码即可；如果某个 IP 密码与其他不一致，则需在此 IP 后填写其密码。

操作步骤

步骤 1 在已安装 ICAgent 的服务器上执行如下命令。

bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -batchModeConfig /opt/ICAgent/iplist.cfg

根据脚本提示输入待安装机器的 root 用户默认密码，如果所有 IP 的密码在 iplist.cfg 中已有配置，则直接输入回车键跳过即可，否则请输入默认密码。

```
batch install begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
2 tasks running, please wait...
2 tasks running, please wait...
End of install agent: 192.168.0.39
```

```
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

请耐心等待，当提示 All hosts install icagent finish.时，则表示配置文件中的所有主机安装操作已完成。

步骤 2 安装完成后，在云日志服务左侧导航栏中选择“Agent 管理”，查看服务器的 4.4 Agent 状态。

----结束

4.2 升级 ICAgent

为了更好的采集体验，LTS 会不断更新 ICAgent 版本。当系统提示您有新的 ICAgent 版本时，您可以按照如下操作步骤进行升级。

1. 在云日志服务管理控制台，单击“Agent 管理”。
2. 在主机列表中选中一个或多个待升级 ICAgent 前的复选框，单击“升级 ICAgent”。
3. 在“升级 ICAgent”对话框中单击“确定”。

   ICAgent 开始升级，升级 ICAgent 预计需要 1 分钟左右，请耐心等待。待 ICAgent 的状态由“升级中”变为“运行”时，表示升级成功。

说明

如果升级后，界面显示 ICAgent 状态异常或者其它升级失败场景，请直接登录节点使用安装命令重新安装 ICAgent 即可（覆盖式安装，无需卸载操作）。

4.3 卸载 ICAgent

服务器上的 ICAgent 被卸载后，会影响该服务器的日志采集能力，请谨慎操作！

卸载方式，您可以按照需要进行选择：

- 通过界面卸载：此操作适用于正常安装 ICAgent 后需卸载的场景。
- 登录服务器卸载：此操作适用于未成功安装 ICAgent 需卸载重装的场景。
- 远程卸载：此操作适用于正常安装 ICAgent 后需远程卸载的场景。
- 批量卸载：此操作适用于正常安装 ICAgent 后需批量卸载的场景。

通过界面卸载

步骤 1 选择“管理与部署 > 云日志服务”，进入云日志服务界面。

步骤 2 在左侧导航栏，单击“Agent 管理”，进入“Agent 管理”页面。

步骤 3 勾选一个或多个待卸载 ICAgent 的服务器的复选框，单击“卸载 ICAgent”。

步骤 4 在“卸载 ICAgent”对话框中单击“确定”。

ICAgent 开始卸载，卸载 ICAgent 预计需要 1 分钟左右，请耐心等待。

待 ICAgent 的状态由“卸载中”变为“未安装”时，表示卸载成功。

说明

通过界面卸载 ICAgent 后如果需要再次安装，请等待 5 分钟后执行安装操作，否则可能出现被再次自动卸载的情况。

----结束

登录服务器卸载

步骤 1 以 **root** 用户登录需卸载 ICAgent 的服务器。

步骤 2 执行如下命令卸载 ICAgent。

bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;

步骤 3 当显示“ICAgent uninstall success”时，表示卸载成功。

----结束

远程卸载

除了上述登录服务器上执行 uninstall.sh 命令卸载 ICAgent 的方式，还可以对服务器进行远程卸载。

步骤 1 在已安装 ICAgent 的服务器上执行如下命令，其中 *x.x.x.x* 表示待卸载 ICAgent 的服务器的 IP 地址。

bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x

步骤 2 根据提示输入待卸载 ICAgent 的服务器 root 用户密码。

说明

- 如果已安装 ICAgent 的服务器安装过 expect 工具，执行上述命令后，即可完成卸载。如果已安装 ICAgent 的服务器未安装 expect 工具，请根据提示输入密码，进行卸载。
- 请确保已安装 ICAgent 的服务器可以使用 root 用户执行 SSH、SCP 命令，来与待卸载 ICAgent 的服务器进行远端通信。
- 当显示“ICAgent uninstall success”时，表示卸载成功。 卸载完成后，可在云日志服务左侧导航栏中选择“Agent 管理”，查看该服务器 ICAgent 的状态。

----结束

批量卸载

当您已有服务器安装过 ICAgent，且该服务器“/opt/ICAgent/”路径下存在 ICAgent 安装包 **ICProbeAgent.zip**，通过该方式可对多个服务器进行一键式继承批量卸载。

须知

批量卸载的服务器需同属一个 VPC 下，并在同一个网段中。

前提条件

已收集需要卸载 Agent 的所有服务器的 IP 地址、密码，按照 iplist.cfg 格式整理好，并上传到已安装过 ICAgent 机器的/opt/ICAgent/目录下。iplist.cfg 格式示例如下所示，IP 地址与密码之间用空格隔开：

192.168.0.109 密码（请根据实际填写）

192.168.0.39 密码（请根据实际填写）

说明

- iplist.cfg 中包含您的敏感信息，建议您使用完之后清理一下。
- 如果所有服务器的密码一致，iplist.cfg 中只需列出 IP 地址，无需填写密码，在执行时输入此密码即可；如果某个 IP 密码与其他不一致，则需在此 IP 地址后填写其密码。

操作步骤

步骤 1 在已安装 ICAgent 的服务器上执行如下命令。

bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -batchModeConfig /opt/ICAgent/iplist.cfg

根据脚本提示输入待卸载机器的 root 用户默认密码，如果所有 IP 地址的密码在 iplist.cfg 中已有配置，则直接输入回车键跳过即可，否则请输入默认密码。

```
batch uninstall begin
Please input default passwd:
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
End of uninstall agent: 192.168.0.109
End of uninstall agent: 192.168.0.39
All hosts uninstall icagent finish.
```

请耐心等待，当提示 All hosts uninstall icagent finish.时，则表示配置文件中所有服务器的卸载操作已完成。

步骤 2 卸载完成后，在云日志服务左侧导航栏中选择“Agent 管理”，查看该服务器 ICAgent 的状态。

----结束

4.4 Agent 状态

ICAgent 状态说明详见下表。

表4-2 ICAgent 状态

状态	说明
运行	该服务器的 ICAgent 运行正常。
未安装	该服务器未安装 ICAgent。安装 ICAgent，详细操作请参见 4.1 安装 ICAgent。

状态	说明
安装中	正在为该主机安装 ICAgent。安装 ICAgent 预计需要 1 分钟左右，请耐心等待。
安装失败	该主机的 ICAgent 安装失败，请登录服务器卸载后重新安装。
升级中	正在升级该服务器的 ICAgent。升级 ICAgent 预计需要 1 分钟左右，请耐心等待。
升级失败	该服务器的 ICAgent 升级失败。请登录服务器卸载后重新安装。
离线	输入的 AK/SK 错误或 ECS 委托设置错误导致该主机的 ICAgent 功能异常。请获取正确的 AK/SK 或正确设置 ECS 委托。
异常	该主机 ICAgent 功能异常，请联系技术支持。

5 查看日志

5.1 实时查看日志

您可以通过本操作实时查看当前时间点之后上报至 LTS 的日志。

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中，单击待查看的日志组，进入日志流列表页面。
5. 在日志流列表中，单击待查看的日志流，进入日志流页面。
6. 单击“实时日志”，查看实时日志

   日志每隔大约 10 分钟上报一次，在日志消息区域，您最多需要等待 10 分钟，即可查看实时上报的日志。

   同时，您还可以通过页面右上方的“清屏”、“暂停”对日志消息区域进行操作。

   - 清屏：清除日志消息区域已经显示出来的日志。
   - 暂停：暂停日志消息的实时显示，页面定格在当前已显示的日志。

     暂停后，“暂停”会变成“继续”，再次单击“继续”，日志消息继续实时显示。

说明

如果您正在使用实时查看功能，请停留在实时查看页面，请勿切换页面。如果您离开实时查看页面，实时查看功能将会被关闭。

5.2 通过关键字查询日志

关键字搜索语法及样例

表5-1 搜索语法

条件	说明
关键字精确搜索	针对日志中的关键字进行精确搜索，关键词指相邻两分词符之间的单词，大小写敏感。
短语精确搜索	针对日志中的短语进行精确搜索，大小写敏感。
&&	搜索结果的交集。
||	搜索结果的并集。
*	模糊搜索能力，*用于替代 0 到 n 个字符。
?	模糊搜索能力，？放在关键字中间或末尾，用于替代一个字符。

关键字搜索样例：

- 含有 Start 的所有日志：Start。
- 含有 Start to refresh 的所有日志：Start to refresh。
- 同时包含 Start 和 Unexpected 的日志数据：Start && Unexpected。
- 包含 Start 或者 Unexpected 的日志数据：Start || Unexpected。
- 含有 error 的所有日志：error*。
- 以“er”开头，以“or”结尾，并且中间有一个字符的所有日志：er?or。

说明

- 使用短语精确搜索时，如果在短语中使用“_”连接符，会默认“_”两边的字符为一个单词，不会进行分词。
- 输入关键字查询日志时，关键字区分大小写。
- 全文搜索时，模糊搜索 “*”，“?” 不匹配特殊字符，例如：“-”、空格。

搜索日志

您可以通过本操作设置关键字和时间范围搜索日志。

1. 登录控制台。
2. 在控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 单击待查询的日志组名称，进入日志流列表。
5. 单击待查询的日志流名称，进入日志流详情页面。

您还可以在待查询日志流“操作”列中，单击“搜索日志”进入日志流详情页面。

6. 在日志详情页面的搜索区域，参考关键字搜索语法及样例，输入待搜索的关键字。
7. 单击 ，开始搜索。

   显示包含搜索关键字的日志。

设置快速查询语句

当您需要重复使用某一关键字语句搜索日志时，可以将其设置为快速查询。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 在日志组列表中，单击待搜索日志的日志组名称，进入日志流列表页面。
5. 单击待查询的日志流名称，进入日志流详情页面。

   您还可以在待查询日志流“操作”列中，单击“搜索日志”进入日志流详情页面。
6. 参考关键字搜索语法及样例，设置搜索条件。

   例如，输入“error*”。
7. 单击“新增快速查询”。
8. 输入快速查询名称。

   用户可自定义快速查询名称，规范如下：
   - 名称长度限制在 1~64 个字符之间。
   - 名称只能由汉字、英文大小写字母、数字、特殊字符“_”“-”“.”组成，且不能以小数点开头或结尾。
   - 同一日志流中，快速查询名称不能重复。
9. 单击“确认”，完成快速查询条件的创建。
10. 单击“新增快速查询”按钮旁边已创建的快速查询标签，可进行快速查询并显示查询结果详情。

查看上下文

您可以通过本操作查看指定日志生成时间点前后的日志，用于在运维过程中快速定位问题。

1. 登录控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”，进入“日志管理”页面。
4. 单击待查看的日志组名称，进入日志流列表。
5. 在日志流列表中，单击查看的日志流名称，进入日志流详情页面。

您还可以在待查询日志流“操作”列中，单击“搜索日志”进入日志流详情页面。

6. 单击待查看日志右侧的“查看上下文”。

   在查看上下文结果中，可以查看该日志的前后若干条日志详细信息。

6 过滤器

6.1 通过自定义指标查询日志

每个日志流允许创建 5 个过滤器。本操作指导用户按需配置需要过滤的关键指标，并且通过云监控对过滤的指标进行监控及告警。

1. 登录控制台。
2. 在左上角单击 ，选择区域和项目。
3. 选择“服务列表 > 管理与部署 > 云日志服务”。
   进入云日志服务界面，默认进入日志管理页面。
4. 在日志组列表中单击需要查看的日志所在的日志组名称。
   进入该日志组下的日志流列表页面。
5. 单击“创建自定义指标过滤”，进行配置。
6. 参考表 6-1，过滤指标参数配置完成后，单击“确定”，完成过滤器的创建。

表6-1 指标过滤参数解释

名称	说明
过滤器名称	过滤器名称帮助您区分同一日志主题下的不同过滤器，过滤器名称可以由 1~64 位的大小写字母和数字组成，并且同一日志主题下的过滤器名称不能重复。
过滤关键词	过滤器将会按照您输入的过滤关键词在该日志主题下执行过滤和累加关键词的动作。 仅支持过滤单个字词，例如 Error、Warning 或者 Fail to root 等，不支持过滤组合后的字词，日志服务的过滤方式是精确匹配，且区分大小写，数字及特殊符号需用双引号包含起

名称	说明
	来。
日志样例	日志样例用于测试配置的“过滤关键词”是否能精准的匹配到相关日志，默认支持测试最近 10 条日志，如果无法匹配到相关日志，可以在日志列表中寻找符合条件的日志粘贴到测试框中验证过滤关键词是否生效，也可以调整过滤关键词。
指标名称	指标名称是指“过滤关键词”对应的指标名称，类似 key-value 中的 key 值，以便日志服务帮助您做指标统计，并且将指标统计值发布到云监控服务中便于您监控次关键词出现的频率、次数及设置阈值并且接收告警。指标名称可以由 1~64 位的大小写字母和数字组成，请注意同一日志主题下的指标名称不能重复，否则可能会造成数据不准的情况出现。

6.2 禁用过滤器

操作场景

对于已经配置过滤器的日志流可能出现日志格式或日志内容变化导致当前过滤关键词失效，该章节用于指导用户禁用已经失效或者不需要再进行监控及告警的过滤器。

前提条件

- 已获取控制台的登录账号与密码。
- 已创建日志组。
- 已创建日志流。
- 已完成日志采集。
- 已完成自定义指标过滤器的配置。

操作步骤

1. 进入控制台首页，在左上角单击 ，选择区域和项目。
2. 选择“服务列表 > 管理与部署 > 云日志服务”。
   进入云日志服务界面，默认进入日志管理页面。
3. 在日志组列表中选择需要禁用的过滤器所在的日志组名称。
   进入该日志组下的日志流列表页面。
4. 在日志流列表，找到目标日志流所在行。
5. 在自定义指标过滤列，单击自定义指标过滤下的数字或横线，进入该日志流下的过滤器列表，如下图：
6. 对于需要禁用的过滤器，单击其所在行的禁用按钮。

说明

过滤器禁用后，您将无法在云监控服务中再针对这项指教进行监控，之前配置的告警规则可能会因为数据不足而触发告警。

6.3 删除过滤器

操作场景

由于一个日志流下只能配置 5 个关键指标过滤器，所以如果您增加过滤器配置请您先删除不需要使用的过滤器后再试，本任务指导用户在日志列表中删除不需要使用的过滤器。

前提条件

- 已获取控制台的登录账号与密码。
- 已创建日志组。
- 已创建日志流。
- 已完成日志采集。
- 已完成自定义指标过滤器的配置。

操作步骤

1. 进入控制台首页，在左上角单击 ，选择区域和项目。
2. 选择“服务列表 > 管理与部署 > 云日志服务”。
   进入云日志服务界面，默认进入日志管理页面。
3. 在日志组列表中选择需要删除的过滤器所在的日志组名称。
   进入该日志组下的日志流列表页面。
4. 在日志流列表，找到目标日志流所在行。
5. 在自定义指标过滤列，单击自定义指标过滤下的数字或横线，进入该日志流下的过滤器列表，如下图：
6. 对于需要删除的过滤器点击其所在行的删除按钮。

说明

删除过滤器后，您将无法在云监控服务中再针对这项指标进行监控，之前配置的告警规则可能会因为数据不足而触发告警。

7 日志转储

7.1 概述

主机和云服务的日志数据上报至云日志服务后，默认存储时间为 7 天，可以在 1-30 天之间进行设置。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至其他云服务中进行等长期保存。

OBS 仅提供日志存储功能；DIS 除了提供日志存储能力外，还提供丰富的大数据分析能力，DIS 可以将大量日志文件传输到云端做备份，进行离线分析、存储查询及机器学习，还能用于数据丢失或异常后的恢复和故障分析。同时大量小文本文件可合并转储为大文件，提高数据处理性能。DMS 转储以通过分布式消费服务 API 实时消费处理日志，请根据您的业务场景选择 OBS、DIS、DMS 进行日志转储。

说明

本地的日志文件定时清空，不会影响转储的日志。

当前 LTS 支持转储至以下云服务：

- 7.2 转储至 OBS

7.2 转储至 OBS

对象存储服务 OBS 提供日志存储功能；您可以将日志转储至 OBS，并在 OBS 控制台下载日志文件。

前提条件

- 已创建日志组和日志流。
- 已完成 ICAgent 安装。

- 已配置日志采集规则。

操作步骤

1. 在云日志服务管理控制台，左侧导航栏中，单击“日志转储”。
2. 在“日志转储”页面右上角，单击“配置转储”。
3. 在“配置转储”页面，设置转储日志相关参数。

说明

转储任务创建成功后，已绑定的日志组和转储方式不支持修改，其他参数支持修改。

表7-1 配置转储参数说明

参数名称	说明	样例
日志组名称	选择已创建的日志组。	-
日志流名称	选择已创建的日志流。	-
转储方式	选择转储的云服务。	OBS
OBS 桶	选择已创建的 OBS 桶。如果没有可选择的 OBS 桶，单击“查看 OBS”，进入对象存储服务管理控制台，创建 OBS 桶。	-
自定义转储路径	• 开启：将日志转储至自定义路径中，用于区分不同日志流之间的转储日志文件。 格式为：/LogTanks/RegionName/*自定义转储路径*。格式需要符合如下规范： – “/LogTanks/RegionName”为系统默认路径，不可以修改。 – 自定义转储路径名称不允许为空，长度限制为 1~64 个字符。 – 名称只能由英文大小写字母、数字、中划线“_”、下划线“-”、小数点“.”和“/”组成。 示例：输入 LTS-test，则日志转储路径为：LogTanks_RegionName_LTS-test_*2019_01_01_日志文件名称*。 • 不开启：将日志转储至系统默认路径中。系统默认路径为：LogTanks_RegionName_*2019_01_01_日志组_日志流_日志文件名称*。	LTS-test
日志文件前缀	转储至 OBS 桶中的日志文件前缀。 日志文件前缀需符合如下规范： • 名称长度限制为 0~64 个字符。 • 名称只能由英文大小写字母、数字、中划线	LTS-log

参数名称	说明	样例
	“_”、下划线“-”和小数点“.”组成。 示例：输入 LTS-log，则日志文件名称为：LTS-log_日志文件名称。	

转储格式	用于配置日志的转储格式，可选择“原始日志格式”和“JSON 格式”。
	• 原始日志格式示例：
	云日志服务控制台展示的日志内容的格式为原始日志格式。
	`Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)`
	• JOSN 格式示例：
	`{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}`
		JSON

是否开启转储	选择开启转储。	开启
转储周期	日志自动转储至 OBS 桶的时间间隔，支持 2 分钟、5 分钟、30 分钟等。	3 小时

4. 单击“确定”，完成配置。当转储任务状态为“正常”时，表示转储任务创建成功。
5. 单击“转储对象”列的 OBS 桶名称，可以跳转至 OBS 控制台，查看转储的日志文件。转储到 OBS 后的日志，支持从 OBS 下载到本地进行查看。

8 常见问题

8.1 如何获取 AK/SK？

AK/SK（Access Key ID/Secret Access Key）即访问密钥，表示一组密钥对。

- AK：访问密钥 ID，是与私有访问密钥关联的唯一标识符。访问密钥 ID 和私有访问密钥一起使用，对请求进行加密签名。
- SK：与访问密钥 ID 结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

说明

每个用户最多可创建 2 个 AK/SK，且一旦生成永久有效。

操作步骤

1. 登录控制台，将鼠标移动到右上方的用户名称，并在下拉列表中选择“我的凭证”。
2. 在“我的凭证”页面中选择“管理访问密钥”页签。

3. 在列表上方单击“新增访问密钥”，输入登录密码，并通过邮箱或者手机进行验证。
4. 单击“确定”，生成并下载 AK/SK。

说明

为防止 AK/SK 泄露，建议您将其保存到安全的位置。

8.2 使用 agent 过程中，CPU 占用较高怎么处理？

如果在使用 agent 过程中遇到 CPU 占用较高的情况，请确认您配置的日志采集路径下是否有大量的日志文件，建议您配置合理的日志滚动和清理策略，以减少 agent 在收集日志过程中带来的系统资源占用。

8.3 云日志服务可以采集哪类日志？支持采集哪些文件类型？

云日志服务可以采集哪类日志

1. 主机日志，通过 ICAgent 采集器进行采集。
2. 云服务日志，如 ELB/VPC，需要到对应的云服务上启用日志上报。
3. 通过 API 上报日志。

云日志服务支持采集哪些文件类型（文件扩展名）

采集路径如果配置的是目录，示例：/var/logs/，则只采集目录下后缀为“.log”、“.trace”和“.out”的文件；如果配置的是文件名，则直接采集对应文件，只支持文本类型的文件，日志的时间（东八区 UTC/GMT+08:00）必须是最近 7 天以内的。

8.4 在 AOM（应用运维管理）中关闭日志采集开关，会影响 LTS（云日志服务）收集日志吗？

会。云日志服务与应用运维服务的日志采集开关为同步状态，即如果您在应用运维管理服务关闭了“超额继续采集日志”开关，则云日志服务的开关也同样关闭，关闭后将停止采集日志。

8.5 实时查看最新日志，每一次加载数据时延是多久？

正常情况下，每隔 3 秒加载一次。

8.6 日志文件较多，是否可以手动删除日志数据？

不可以。系统根据设置的日志存储时间（1~30 天）自动清理过期的日志数据。

8.7 日志可以在 LTS 存储多长时间？

主机和云服务的日志数据上报至云日志服务后，默认存储时间为 7 天，可以在 1-30 天之间进行设置。超出存储时间的日志数据将会被自动删除。对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

8.8 日志转储后会，LTS 会删除转储的内容么？

不会删除。日志转储是把日志“另存”一份至 OBS，转储后，单击“转储对象”列的 OBS 桶名称，可以跳转至 OBS 控制台，查看转储的日志文件。

8.9 日志转储页面，转储状态异常是什么原因？

- OBS 桶被删除，请您重新指定已创建的存储桶。
- OBS 桶策略异常，请您在对象存储服务中设置访问控制策略。

8.10 日志转储后如何下载？

当前日志下载需要用户将日志转储至 OBS，用户可以到 OBS 控制台下载日志文件。

查看方法：在 LTS 控制台“日志转储”页签下，单击“转储对象”列的 OBS 桶名称，可以跳转至 OBS 控制台，查看、下载转储的日志文件。

A 修订记录

版本日期	变更说明
2020-09-30	第一次正式发布。