ALIBABA CLOUD

阿里云

日志服务

快速入门

文档版本：20201231

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.快速入门

本文介绍如何通过日志服务控制台采集ECS日志，并对日志进行查询和分析。

前提条件

- 已有可用的ECS。更多信息，请参见云服务器ECS快速入门。
- ECS服务器上已有待采集的日志。

  本示例中待采集的日志路径为*/var/log/nginx/access.log*，日志样例为 `127.0.0.1|#|-|#|13/Apr/2020:09:44:41 +0800|#|GET /1 HTTP/1.1|#|0.000|#|74|#|404|#|3650|#|-|#|curl/7.29.0` 。针对该日志样例，本示例选择分隔符模式进行采集。

操作视频

本视频指导您快速使用日志服务。

步骤1：创建Project和Logstore

1. 登录日志服务控制台。
2. 创建Project。
   i. 在**Project列表**区域，单击**创建Project**。
   ii. 在**创建Project**面板中，按照如下说明配置参数，其他参数均可保持默认配置。

参数	描述
Project名称	Project的名称，全局唯一。创建Project成功后，无法更改其名称。
所属地域	Project的数据中心。建议选择与ECS相同的地域，即可使用阿里云内网采集日志，加快采集速度。 创建Project后，无法修改其所属地域，且日志服务不支持跨地域迁移Project。

   iii. 单击**确定**。
3. 创建Logstore。创建Project完成后，系统会提示您创建一个Logstore。

   在**创建Logstore**面板中，按照如下说明配置参数，其他参数均可保持默认配置。

参数	描述
Logstore名称	Logstore的名称，在其所属Project内必须唯一。创建Logstore成功后，无法更改其名称。
Shard数目	日志服务使用Shard读写数据。 一个Shard提供的写入能力为5 MB/s、500次/s，读取能力为10 MB/s、100次/s。如果一个Shard就能满足您的业务需求，您可配置**Shard数目**为**1**。在只创建1个Logstore且只使用1个Shard的情况下，不会产生Shard费用。

参数	描述
自动分裂Shard	开启自动分裂功能后，如果您写入的数据量超过已有Shard服务能力，日志服务会自动根据数据量增加Shard数量。 如果您确保配置的Shard数量已满足业务需求，可关闭**自动分裂Shard**开关。

步骤2：采集日志

1. 在**接入数据**区域，选择**分隔符-文本日志**。
2. 选择目标Project和Logstore，单击**下一步**。
3. 安装Logtail。
   i. 在**ECS**页签中，选中目标ECS实例，单击**立即执行**。
   ii. 确认**执行状态**为**成功**后，单击**确认安装完毕**。
4. 创建IP地址类型的机器组，单击**下一步**。按照如下说明配置参数，其他参数均可保持默认配置。

参数	说明
名称	机器组的名称，在其所属Project内必须唯一。创建机器组成功后，无法更改其名称。
IP地址	ECS服务器IP地址。多个IP地址之间请用换行符分隔。 **注意** 请勿将Windows机器和Linux机器添加到同一机器组中。

5. 选中目标机器组，将该机器组从**源机器组**移动到**应用机器组**，单击**下一步**。

> **注意** 如果创建机器组后立刻应用，可能因为连接未生效，导致心跳为FAIL，您可单击**自动重试**。如果还未解决，请参见Logtail机器组无心跳进行排查。

6. 创建Logtail配置，单击**下一步**。按照如下说明配置参数，其他参数均可保持默认配置。

参数	描述
配置名称	Logtail配置的名称，在其所属Project内必须唯一。创建Logtail配置成功后，无法修改其名称。

参数	描述
日志路径	待采集的日志的目录和文件名。 日志文件名支持完整文件名和通配符两种模式，文件名规则请参见Wildcard matching。日志文件查找模式为多层目录匹配，即指定目录（包含所有层级的目录）下所有符合条件的文件都会被查找到。例如： ○ */apsara/nuwa/.../*.log*表示*/apsara/nuwa*目录（包含该目录的递归子目录）中后缀名为*.log*的文件。 ○ */var/logs/app_*/*.log*表示*/var/logs*目录下所有符合*app_ *模式的目录（包含该目录的递归子目录）中包含*.log*的文件。 **说明** ○ 默认情况下，一个文件只能被一个Logtail配置采集。 ○ 目录通配符只支持星号（*）和问号（?）。
日志样例	根据实际场景输入一条日志样例。例如： 127.0.0.1|#|-|#|13/Apr/2020:09:44:41 +0800|#|GET /1 HTTP/1.1|#|0.000|#|74|#|404|#|3650|#|-|#|curl/7.29.0
分隔符	根据您的日志格式配置分隔符。例如：`|#|`。 **说明** 指定引用符为**不可见字符**时，您需要查找不可见字符在ASCII码中对应的十六进制数，输入的格式为`0x*不可见字符在ASCII码中对应的十六进制数*`。例如：ASCII码中排行为1的不可见字符填写为**0x01**。
日志抽取内容	日志服务会根据您输入的日志样例及选择的分隔符提取日志内容，并将其定义为Value，您需要为Value指定对应的Key。

单击**下一步**即表示创建Logtail配置完成，日志服务开始采集日志。

说明
- Logtail配置生效时间最长需要3分钟，请耐心等待。
- 如果遇到Logtail采集报错，请参见诊断采集错误。

7. 预览数据，单击**下一步**。日志服务默认开启全文索引，用于查询和分析日志。更多信息，请参见开启并配置索引。

> 说明
>
> - 索引只对新写入的日志数据生效。
> - 如果您要查询和分析日志，那么全文索引和字段索引属性必须至少启用一种。同时启用时，以字段索引为准。

步骤3：查询和分析日志

1. 在**Project列表**区域，单击目标Project。
2. 在**日志存储 > 日志库**页签中，单击目标Logstore。
3. 输入查询和分析语句，选择时间范围，单击**查询/分析**。例如：执行如下查询和分析语句统计最近1天访问IP地址的来源情况，并通过表格展示查询和分析结果。
   - 查询和分析语句

     ```
     * | select count(1) as c, ip_to_province(remote_addr) as address group by address limit 100
     ```

   - 查询和分析结果

     如下图表示最近1天内有329个访问来自广东省，313个访问来自北京市。日志服务支持通过可视化图表展示查询和分析结果。更多信息，请参见统计图表。

     

更多操作

- 投递数据：您可以将采集到的数据投递到OSS、Maxcompute、AnalyticDB、TSDB等云产品中进行存储或计算分析。更多信息，请参见数据投递。
- 消费数据：您可以将采集到的数据进行消费。更多信息，请参见实时消费。
- 数据加工：您可以将采集到的数据进行加工，实现数据的规整、富化、分发、汇总等操作。更多信息，请参见数据加工。