

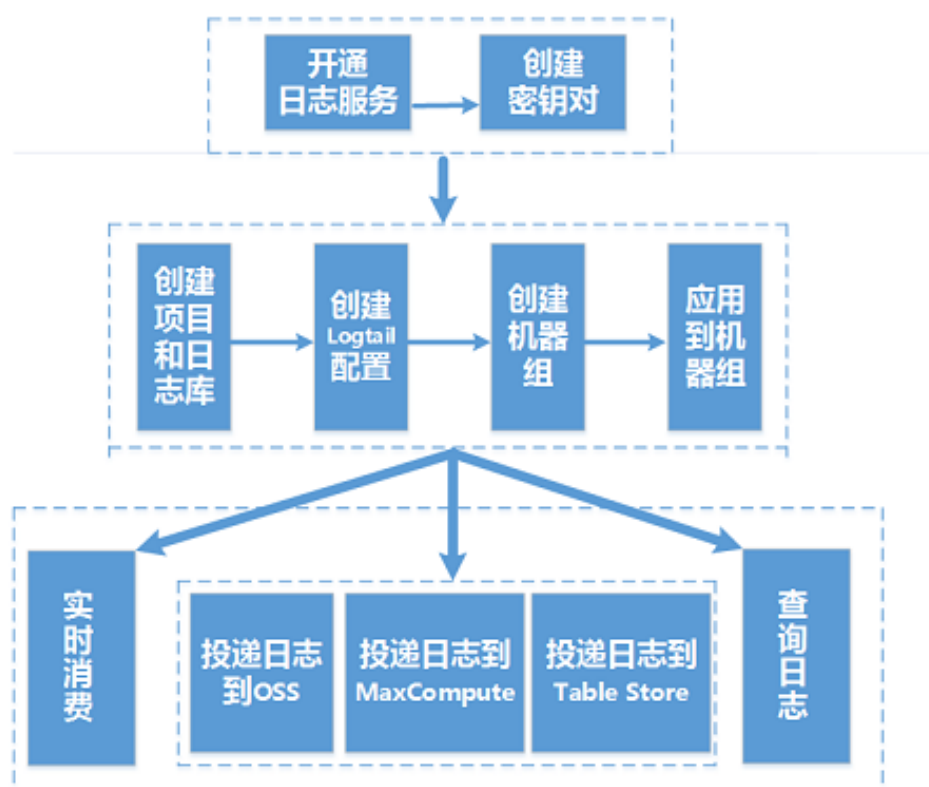
日志服务

快速入门

快速入门

日志服务（Log Service）是阿里云提供的、针对海量日志收集、存储、查询的平台化服务。您可以使用日志服务来集中收集服务集群中所有的日志，并支持实时消费，实时查询和投递到OSS、MaxCompute等其他云产品做进一步分析。

日志服务操作流程：



本文档在Windows环境下，为您演示配置Logtail采集阿里云ECS日志并投递日志到MaxCompute的基本流程。本案例涉及采集日志、实时查询、投递日志等日志服务基本功能，是日志服务的入门级操作指南。

准备开始

1 创建阿里云账号

具体方法请参考 [阿里云账号注册流程](#)。

2 开通日志服务

使用注册成功的阿里云账号登录 [日志服务产品页](#)，单击 **立即开通**。



日志服务

日志服务 (Log Service, 简称Log) 是针对日志类数据一站式服务, 在阿里巴巴集团经历大量大数据场景锤炼而成。用户无需开发就能快速完成数据采集、消费、投递以及查询分析等功能, 帮助提升运维、运营效率, 建立DT时代海量日志处理能力。更多内容请参考[服务简介](#)和[典型场景](#)。

立即开通

产品价格

降价预告 (2017年1月初): 新增免费额度、索引降价

3 创建密钥对

Access Key是Logtail收集日志数据的必要条件。开始使用日志服务之前, 您需要创建密钥对。

在 日志服务管理控制台, 将鼠标移至页面右上角您的用户名上方, 在显示的菜单中单击 **accesskeys**。在弹出的确认对话框中单击 **继续使用AccessKey** 以进入 **AccessKey管理页面**。创建密钥对 (Access Key), 确认状态已设置为 “启用”。

Access Key管理 (1)

创建Access Key

Access Key ID和Access Key Secret是您在阿里云API的凭证, 具有该用户凭证的权限, 请妥善保管。

Access Key ID	Access Key Secret	状态	创建时间	操作
LT42		启用	2016-03-04 10:00:00	删除 刷新

创建项目和日志库

1 创建项目

当您第一次进入日志服务管理控制台, 系统会提示您创建一个项目 (Project)。您也可以通过单击右上角的 **创建Project** 进行操作。

创建Project需要指定 **Project名称** 与 **所属区域**, 请根据您的实际需求进行创建。其中 “杭州内部生产1” 和 “上海内部生产1” 为弹内日志服务, 其余皆为公共云区域。

创建Project

* Project名称: logservice-test

注释: 日志服务

不能输入字符<>""\, 最多512个字节

* 所属区域: 华东 1

确认

取消

2 创建日志库

在Project创建完成的同时，系统会提示您创建一个日志库（以下称为Logstore）。您也可以进入该Project，通过单击右上角的 **创建** 进行操作。创建Logstore需要指定如何使用这些日志。

创建LogStore ×

* LogStore名称:

logstore

LogStore属性

* 数据保存时间:

1

目前Loghub保存时间和索引已经统一，数据生命周期以Loghub设置为准（单位：天）

* shard数目:

2 ▼

* 计费:

单个Shard 0.04元/天（其它计费项）

确认

取消

收集日志

日志服务支持多种日志源和多种采集方式，详情请参见采集方式。您可以选择通过Logtail客户端收集日志或者API/SDK写入日志。本文档以创建Logtail配置收集日志为例，API方式请参考API，SDK方式请参考SDK。

在ECS上安装Logtail客户端。

下载安装包。

下载Logtail安装包到云服务器ECS。Windows安装包：http://logtail-release.oss-cn-hangzhou.aliyuncs.com/win/logtail_installer.zip

安装Logtail。

将安装包解压缩到当前目录，进入目录logtail_installer。以管理员身份运行cmd，并执行安装命令.\logtail_installer.exe install cn_hangzhou进行安装。

注意：根据网络环境和日志服务所处Region的不同，您需要根据具体网络部署执行对应的安装命令。本文档以华东1（杭州）的ECS经典网络为例，其他区域请参见详细说明。

更多信息请参考 [安装Logtail \(Windows \)](#) 和 [安装Logtail \(Linux \)](#)。

配置Logtail收集日志。

在日志服务管理控制台单击目标Project进入**Logstore列表**。单击目标Logstore一行中的**管理**，进入**Logtail配置列表**。

页面右上角单击**创建**。进入Logtail配置流程。

Logtail配置流程包含以下操作步骤：选择数据源、指定日志目录结构和收集模式、应用到机器组。

选择数据源。

单击选择数据源。本文以采集文本日志为例，采集syslog请参见[通过Logtail采集syslog](#)。



指定收集模式。

指定配置名称和日志路径。

请按照页面提示填写配置名称、日志路径和日志文件名称。文件名称可以填写完整名称，也支持通配符模式匹配。

指定日志收集模式。

日志服务目前支持极简模式、分隔符模式、JSON模式、完整正则模式和飞天日志方式解析日志。本文以分隔符模式为例，关于收集模式的详细说明请参考[收集步骤和其他信息](#)。

* 配置名称：

* 日志路径：

指定文件夹下所有符合文件名称的文件都会被监控到(包含所有层次的目录)，文件名称可以是完整名，也支持通配符模式匹配。Linux文件路径只支持/开头，例：/apsara/nuwa/.../app.Log，Windows文件路径只支持盘符开头，例如：C:\Program Files\Intel\...*.Log

模式：

[如何设置Delimiter类型配置](#)

日志样例：

```
10.200.98.220 200 41457921827/Jan/2016:20:50:13 +0800 POST
/PutData?
Category=YunOsAccountOpLog&AccessKeyId=U0UjpekFOOVJW45A&Date=Fri%2
C%2028%20Jun%202013%2006%3A53%3A30%20GMT&Topic=raw&Signature
=pD12XYLmGxkO%2Bmkd6x7hAgQ7b1c%3D HTTP/1.1 aliyun-sdk-java
```

请贴入需要解析的日志样例(支持多条) [常见样例>>](#)

* 分隔符：

填写日志样例。

指定日志收集模式为**分隔符模式**或**完整正则模式**时，需要您填写日志样例。日志服务支持在配置Logtail的同时，根据您选择的配置对日志样例尝试解析。如果解析失败，需要您修改分隔符配置或者正则表达式。请将需要解析的日志样例填写到对应位置。

指定分隔符。

您可以指定分隔符为制表符、竖线、空格，也可以自定义分隔符。请根据您的日志格式选择正确的分隔符，否则日志数据会解析失败。

指定日志抽取结果中的Key。

填写日志样例并选择分隔符后，日志服务会按照您选择的分隔符提取日志字段，并将其定义为Value，您需要分别为Value指定对应的Key。

* 分隔符: 制表符

日志内容抽取结果:

Key	Value
ip	10.200.98.220
status	200
thread	414579218
time	27/Jan/2016:20:50:13 +0800
url	POST /PutData?Category=YunOsAccountOpLog&AccessKey!
user-agent	aliyun-sdk-java

使用系统时间: ☒

高级选项: 展开

应用到机器组。

如果您之前没有创建过机器组，请先根据页面提示创建机器组，然后将Logtail配置应用到机器组。

如果需要创建Armory关联机器组请参考页面提示，跳转到内部指定链接。

创建机器组

* 机器组名称:

机器组标识: IP地址

机器组Topic:

* IP地址:

1. 绑定Armory的机器分组需要跳转到指定页面进行创建 (帮助)

2. 日志服务内部集群安装Logtail请参考文档 (帮助)

armory 机器分组创建链接

确认 取消

完成以上步骤后，日志服务即刻开始收集阿里云ECS上的日志，您可以通过控制台和API/SDK对已收集的日志进行实时消费。

注意：

- Logtail配置推送生效时间最长需要3分钟，请耐心等待。
- 如果需要收集IIS的访问日志，请参考 [IIS 日志收集最佳实践](#) 配置IIS。
- Logtail收集错误可以参见[收集错误查询](#)。

消费日志

日志服务为您提供多种日志消费方式，例如日志预览、实时查询、投递到其他云产品，详细介绍请参见消费日志。

1 预览日志

日志数据收集到日志服务后，在控制台上可以通过单击特定Logstore的日志消费方式进入预览界面。通过指定ShardId和时间可以预览起始的10个数据包。

例如，预览ShardId为0，时间范围最近15分钟的起始10个数据包。



2 查询日志

通过控制台查询日志。

日志数据收集到日志服务后，在控制台上可以通过单击特定Logstore的日志索引消费方式进入查询界面。通过指定日志主题Topic（目前只有通过API写入的日志才可能有Topic）、关键字、时间进行查询操作。直方图中，绿色表示在此时间范围内数据精确，黄色表示在此时间范围内数据不精确。可以通过单击或者拖拽黄色直方图部分进行再次查询。不精确的日志数据不会在**匹配日志**中返回。

例如，查询最近15分钟内的所有日志，可以设置查询条件为空，时间范围为最近15 分钟。



使用API/SDK查询日志。

类似于写入日志，API也提供了相应的查询日志接口 `GetLogs` 和 `GetHistograms`。关于API的完整参考请见API 参考。

除了API，日志服务还提供了多种语言（Java、.NET、PHP 和 Python）的SDK 方便用户查询日志。关于SDK的完整参考请见日志服务 SDK。

3 投递日志

日志服务不仅支持对多种来源、格式的数据进行批量收集和管理维护，还支持将日志数据投递到OSS、MaxCompute等云产品进行计算分析。本文档以投递日志数据到MaxCompute为例，为您介绍日志服务的日志投递功能。如您需要投递日志到OSS，请参考投递日志到OSS。

准备工作

为把日志服务内的日志投递到MaxCompute，您需要首先准备好相应的MaxCompute环境。步骤如下：

1. 开通 MaxCompute服务。您需要在阿里云管理控制台上启用MaxCompute服务。
2. 创建存储投递日志的MaxCompute表。请参考 投递日志到 ODPS了解表的结构和相关注意事项。

开启投递任务

日志服务提供把日志数据离线投递到MaxCompute的功能，您需要在管理日志数据消费模式界面指定日志数据投递的MaxCompute Project、Table名称和表对应列映射关系等属性，并确认授权日志服务写MaxCompute权限。

开启投递。

在日志服务管理控制台单击左侧的**LogShipper-投递导出 > MaxCompute（原ODPS）**，进入投递管理页面。选择目标Logstore名称并单击**开始投递**开启投递任务。

配置投递规则。

开启投递后跳转至**LogHub —— 数据投递**页面，在该页面需要配置投递大数据计算服务MaxCompute（原 ODPS）的相关内容。

| [LogHub —— 数据投递](#) [填写前请先查看帮助文档>>](#)

| 选择要投递的区域：**华东2**

LogHub Project wd-testlog
名称：

LogHub a123
LogStore 名称：

* 投递名称：

logtset

* 项目名：

wd01

* 日志表名：

tmail

* 字段关联：

source	↔	log_source	string
time	↔	log_time	bigint
topic	↔	log_topic	string
time	↔	time	string
ip	↔	ip	string
thread	↔	thread	string
_extract_others	↔	log_extract_otf	string

* 分区字段：

_partition_time	↔	log_partition_t
status	↔	status

* 时间分区格式：

20170606

* 导入时间间隔：

1800s

确定

取消

备注：source、time、topic、extract_others和partition_time是日志服务的系统保留字段,建议使用。对于映射配置的限制详情请参见[投递日志到MaxCompute](#)。

查看投递状态

在管理控制台 [MaxCompute投递任务管理](#) 中可以查看任务投递状态，当日志导入成功后，你可以通过 [MaxCompute管理控制台](#) 查看导入的日志数据。另外，如何在MaxCompute里解析、使用导入的MaxCompute表请参见[投递日志到 MaxCompute](#)。