

Cribl Practices

Overview

Welcome to the Cribl Practices section! This segment is designed to serve as a comprehensive guide for newcomers and beginners to Cribl LogStream, empowering them to efficiently manage and edit pipelines while familiarizing themselves with the platform's features. Whether you're a seasoned professional or just starting your journey with Cribl, this section aims to provide you with the necessary skills to transition seamlessly into the Cribl team workforce for new projects.

Within this section, you'll find a series of hands-on labs and exercises carefully curated to facilitate your learning experience. These labs offer a practical approach to understanding Cribl LogStream, allowing you to dive into real-world scenarios and explore various functionalities firsthand.

By engaging with these labs, you'll gain proficiency in managing and editing pipelines, mastering key features, and honing your troubleshooting skills. Whether it's parsing, routing, transforming, or enriching data, each practice is designed to equip you with the essential knowledge and techniques needed to excel in Cribl LogStream.

Whether you're looking to enhance your existing skills or embark on a new journey with Cribl, this section provides a valuable resource to accelerate your learning and development. So, dive in, explore, and empower yourself to unleash the full potential of Cribl LogStream!

Here's a guide on how to play with the labs:

1) Sign up for a Cribl.Cloud Account: If you haven't already done so, navigate to <https://manage.cribl.cloud/> and sign up for a new account. Follow the registration process to create your account.



Welcome

Login to Cribl.Cloud

Email address*

jialiang_chan

Continue

Don't have an account? [Sign up](#)

OR



Continue with Google



Create Your Account

Signup for Cribl.Cloud

Email address*

Continue

Already have an account? [Log in](#)

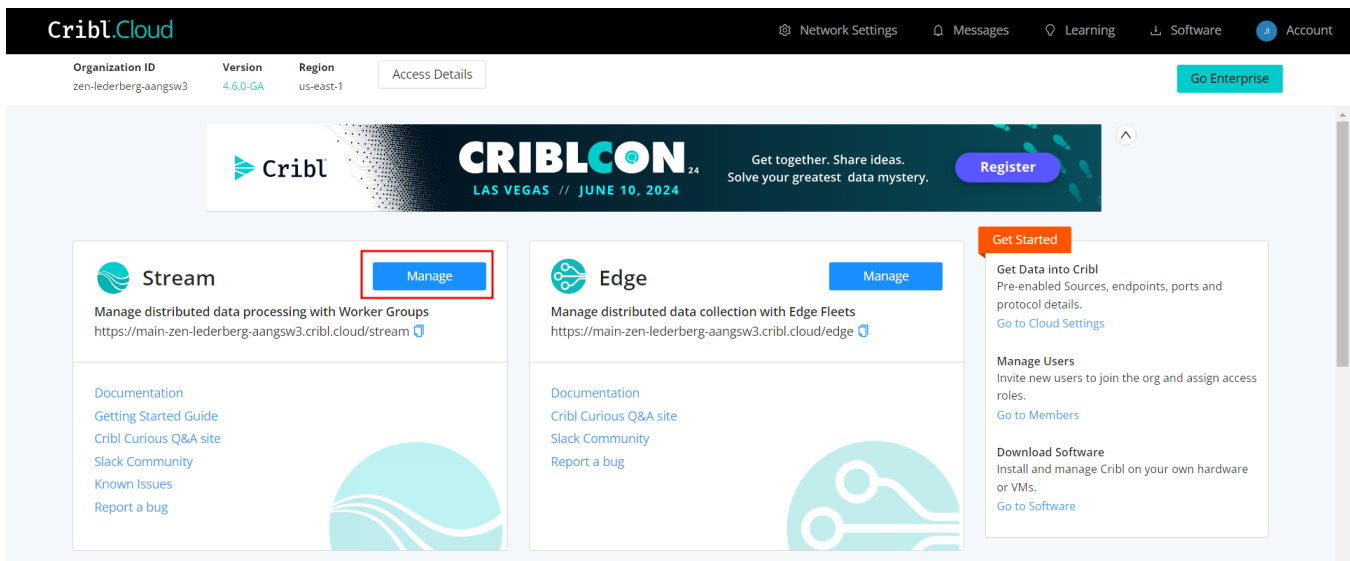
OR



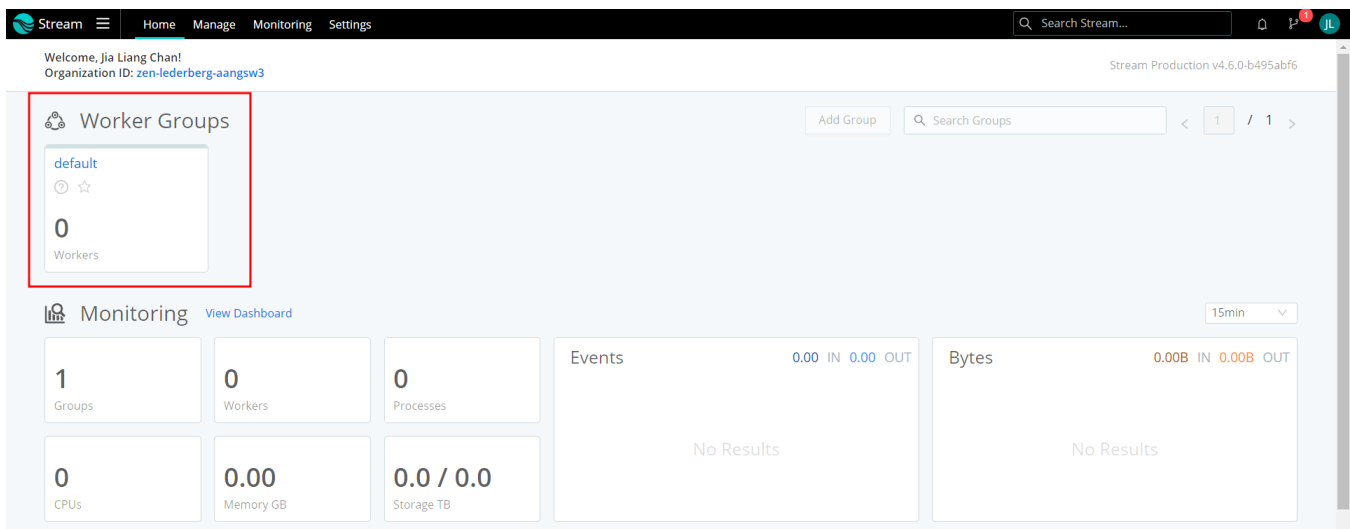
Continue with Google

2) Access Cribl.Cloud UI: Once you've successfully registered and logged in, you'll be directed to the Cribl.Cloud user interface. Here, you'll find various options and functionalities to manage your streams.

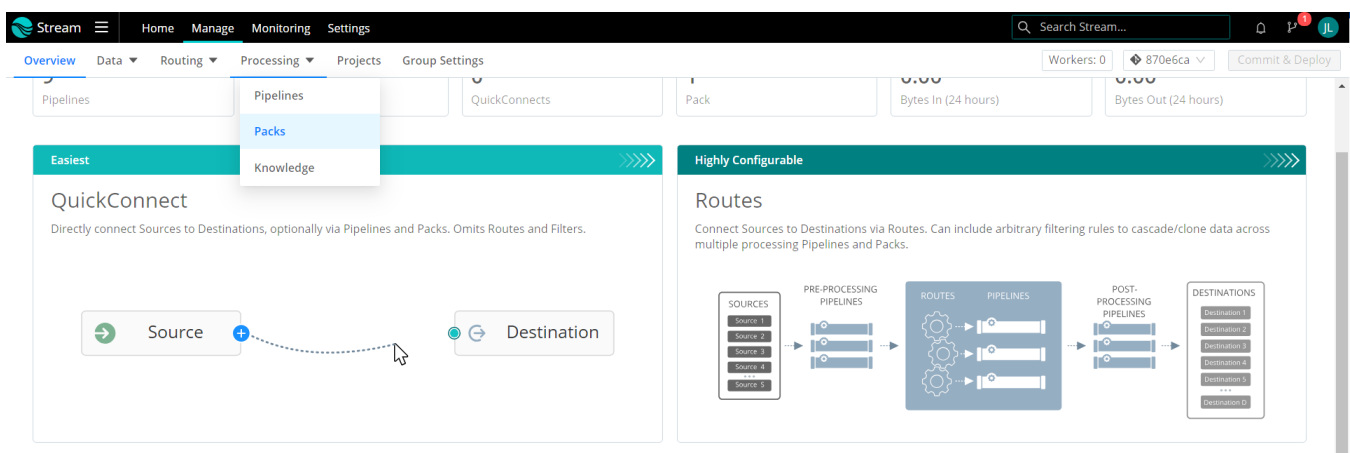
3) Navigate to "Manage Stream": In the Cribl.Cloud UI, locate and click on the "Manage Stream" tab or option. This will take you to the section where you can create, manage, and configure your streams.



4) Access the default Worker Group: In the Cribl.Cloud UI, locate and click on the "default" tab under Worker Groups section.



5) Navigate to Packs: In the Cribl.Cloud UI, locate and click on the "Processing > Packs" tab under Manage tab on navigation bar.



6) **Open Lab Exercises in (.crlb) file extension and Start the Fun:** In the Cribl.Cloud UI, locate and click on the "Add Pack > Import from File" to select the lab exercise that you wish to start for

Stream

HomeManageMonitoringSettings

Search Stream...

Workers: 0870e6caCommit & Deploy

OverviewDataRoutingProcessingProjectsGroup Settings

Packs

Filter Packs

| Display name | ID | Description | Source | Attached to | Spec | Version | Author |
|--|------------|-------------------------|---------------------------|-------------|------|---------|-------------|
| <input type="checkbox"/> Hello, Packs! | HelloPacks | A sample pack with a... | file/opt/cribl_data/fa... | 0 resources | | 1.0.0 | Cribl, Inc. |

Add Pack

Add from Dispensary

Create Pack

Import from File

Import from URL

Import from Git

Open

Downloads > 1_CCSC > JiaLiang_Chan_CCSCAdvancedPacks_Cribl_20240201

Search JiaLiang_Chan_CCSCA...

Organize

New folder

| Name | Date modified | Type | Size |
|--|--------------------|------------|-------|
| Advanced_Aggregations.crlb | 31/1/2024 10:04 pm | Cribl File | 4 KB |
| Advanced_SiteScope.crlb | 1/2/2024 2:08 am | Cribl File | 5 KB |
| Beginner_Bro.crlb | 30/1/2024 3:06 pm | Cribl File | 3 KB |
| Beginner_Extract_Host.crlb | 30/1/2024 3:37 pm | Cribl File | 2 KB |
| Beginner_Lookup_Host.crlb | 30/1/2024 4:07 pm | Cribl File | 3 KB |
| Beginner_Mask_Multiple_Fields.crlb | 30/1/2024 8:22 pm | Cribl File | 6 KB |
| Beginner_Mask_PII.crlb | 30/1/2024 9:42 pm | Cribl File | 5 KB |
| Beginner_Sample_Events.crlb | 30/1/2024 11:47 pm | Cribl File | 5 KB |
| Expert_Mercury.crlb | 1/2/2024 4:27 am | Cribl File | 10 KB |
| Intermediate_Check_Point_Enrichment.crlb | 31/1/2024 12:29 am | Cribl File | 4 KB |
| Intermediate_Check_Point_Serialize.crlb | 31/1/2024 2:03 am | Cribl File | 4 KB |
| Intermediate_Decode.crlb | 31/1/2024 2:19 am | Cribl File | 3 KB |
| Intermediate_Fixing_Time.crlb | 31/1/2024 3:04 am | Cribl File | 3 KB |
| Intermediate_Regex_Extract_Lookup_mat... | 31/1/2024 4:29 am | Cribl File | 9 KB |

File name

Custom Files (*.tagc*.crlb)

OpenCancel

Reminder:

Navigate to "Processing > Pack Settings > README". Each pack is self-contained and includes a ReadMe that describes a specific SCIPAB (Situation, Complication, Implication, Position, Action, Benefit). All that should be needed to complete these Packs is a Cribl instance running anywhere (Cribl.Cloud). No live data or datagen needs to be configured. Once completed, you will export them to keep a copies to yourselves.

Inactive periods in Cribl.Cloud may lead to the closure of instances, potentially resulting in the loss of all saved work. Therefore, it is advised to export all your work locally as a backup or reference for future use.

Stream

HomeManageMonitoringSettings

Search Stream...

Workers: 0870e6caCommit & Deploy

OverviewDataRoutingProcessingProjectsGroup Settings

PackBeginner_Mask_PIIRoutesPipelinesKnowledgePack Settings

Pack Settings / README

README

Settings

README.md

Beginner Lab - Mask PII ANSWER KEY

- Level = Beginner
- Points = 1

SCIPAB

Situation: Some data logged into events should not be visible

Complication: PII data is particularly sensitive and *must* be masked

Implication: Failure to mask PII data could result in security audit failures

Position: Cribl LogStream's Mask function can be used obfuscate or mask the unwanted data

Action: Create a pipeline to mask potential social security numbers and credit card account numbers

Benefit: PII has been removed from the data stream, in-flight, before it reaches our log store

Requirements

View

Edit

Navigate to "Processing > Pipelines", and start your journey with playing around with the function ("Add Function") and achieving the goals stated in README.

In "Sample Data" tab, there are the sample logs which has been generated for you to apply functions built in your pipeline onto the events, and eventually you can observe the changes and behavior in "Simple Preview" tab

Stream Home Manage Monitoring Settings

Overview Data Routing Processing Projects Group Settings

Workers: 0 870e6ca Commit & Deploy

Pack Beginner_Mask_PII Routes Pipelines Knowledge Pack Settings

Mask_PII 0 In 0 Out 0 Err Attached to 1 Route

Add Function

Status Sample Data Simple Preview

Sample data file mask_pii.log Pipeline Mask_PII

IN OUT

Select Fields (7 of 7)

Event

1 2021-11-04 07:06:18.822 +08:00

raw: 2020-04-23 13:55:58,872,Event [Event=UpdateBillingProvQuote, timestamp=1587658161, JMSCorrelationID=NA, JMSMessageID=ID:ESP-PD.174304828C850:5452E574, orderType=RatePlanFeatureChange, quotePriority=NORMAL, conversationID=ESB-3C182E2F0413700E:AE1A98CE:A3E80A9546227:08B65, credits=NA, JMSReplyTo=pub.esb.genericasync.response, timeToLive=-1, serviceName=UpdateBillingProvisioning, esn=9FFC24E7048114, accountNumber=9000001675, social=91b11792d5b5c86d415e7b1d463a, MethodName=InternalEvent, AdapterName=UpdateBillingProvQuote, messageId=NA, orderNumber=810000000000576, quoteNumber=65212270, ReplyTo=NA, username=maskleintjemoi, EventConversationID=NA, mdn=6072375921, accountType=PostPaid, marketCity="NEW ORLEANS", marketState=LA, marketZip=70189, billingCycle=6, autoBillingPayment=1, phoneCode=552, phoneType=Feature, phoneName="Samsung Solstice 2", planCode=ULPOST70, planType=PostPaid, planPrice=69.99, planName="Unlimited", planDescription="Nationwide Unlimited Minutes, Unlimited Text, Unlimited Data", cardNumber=5f64041b1626426de8a4ee17bfa91179, networkProviderName=Spunktel] Show less

#_time: 1635980778.822

cribl_breaker: ndjson

host: 127.0.0.1

index: cribl

source: /opt/tibco/tra/apps/ESB/logs/business_event.log

sourcetype: business_event

2 2021-11-04 07:06:18.822 +08:00

raw: 2020-04-23 13:55:59,948,Event [Event=UpdateBillingProvQuote, timestamp=1587658158, JMSCorrelationID=NA, JMSMessageID=ID:ESP-PD.5A5996A1F9470:D378E546, orderType=NewActivation, quotePriority=NORMAL, ...] Show more

#_time: 1635980778.822

cribl_breaker: ndjson

host: 127.0.0.1

index: cribl

source: /opt/tibco/tra/apps/ESB/logs/business_event.log

sourcetype: business_event

3 2021-11-04 07:06:18.822 +08:00

raw: 2020-04-23 13:56:03,066,Event [Event=UpdateBillingProvQuote, timestamp=1587658163, JMSCorrelationID=NA, JMSMessageID=ID:ESP-PD.7664E8898F45A:30753AA1, orderType=NewActivation, quotePriority=NORMAL, ...] Show more

#_time: 1635980778.822

cribl_breaker: ndjson

host: 127.0.0.1

index: cribl

source: /opt/tibco/tra/apps/ESB/logs/business_event.log

sourcetype: business_event

Sample result from the "Simple Preview" tab, after implementing functions in your pipeline:

Stream Home Manage Monitoring Settings

Overview Data Routing Processing Projects Group Settings

Workers: 0 870e6ca Commit & Deploy

Pack Beginner_Mask_PII_Done Routes Pipelines Knowledge Pack Settings

Mask_PII 0 In 0 Out 0 Err Attached to 1 Route

Add Function

Status Sample Data Simple Preview

Sample data file mask_pii.log Pipeline Mask_PII

IN OUT

Select Fields (8 of 8)

Event

1 2021-11-04 07:06:18.822 +08:00

raw: 2020-04-23 13:55:58,872,Event [Event=UpdateBillingProvQuote, timestamp=1587658161, JMSCorrelationID=NA, JMSMessageID=ID:ESP-PD.174304828C850:5452E574, orderType=RatePlanFeatureChange, quotePriority=NORMAL, conversationID=ESB-3C182E2F0413700E:AE1A98CE:A3E80A9546227:08B65, credits=NA, JMSReplyTo=pub.esb.genericasync.response, timeToLive=-1, serviceName=UpdateBillingProvisioning, esn=9FFC24E7048114, accountNumber=9000001675, social=91b11792d5b5c86d415e7b1d463a, MethodName=InternalEvent, AdapterName=UpdateBillingProvQuote, messageId=NA, orderNumber=810000000000576, quoteNumber=65212270, ReplyTo=NA, username=maskleintjemoi, EventConversationID=NA, mdn=6072375921, accountType=PostPaid, marketCity="NEW ORLEANS", marketState=LA, marketZip=70189, billingCycle=6, autoBillingPayment=1, phoneCode=552, phoneType=Feature, phoneName="Samsung Solstice 2", planCode=ULPOST70, planType=PostPaid, planPrice=69.99, planName="Unlimited", planDescription="Nationwide Unlimited Minutes, Unlimited Text, Unlimited Data", cardNumber=5f64041b1626426de8a4ee17bfa91179, networkProviderName=Spunktel] Show less

#_time: 1635980778.822

cribl_breaker: ndjson

cribl_pipeline: Mask_PII

host: 127.0.0.1

index: cribl

source: /opt/tibco/tra/apps/ESB/logs/business_event.log

sourcetype: business_event

2 2021-11-04 07:06:18.822 +08:00

raw: 2020-04-23 13:55:59,948,Event [Event=UpdateBillingProvQuote, timestamp=1587658158, JMSCorrelationID=NA, JMSMessageID=ID:ESP-PD.5A5996A1F9470:D378E546, orderType=NewActivation, quotePriority=NORMAL, ...] Show more

#_time: 1635980778.822

cribl_breaker: ndjson

cribl_pipeline: Mask_PII

host: 127.0.0.1

index: cribl

source: /opt/tibco/tra/apps/ESB/logs/business_event.log

sourcetype: business_event

Before that, social and cardNumber (highlighted in yellow) is in plaintext, and we could observe they turned into hash after going through the Mask_PII pipeline we built.

Status

Sample Data

Simple Preview ?

Sample data file

mask_pii.log

Pipeline

Mask_PII

Run

IN

OUT

Select Fields (7 of 7)

| # | Event |
|---|---|
| 1 | <pre> raw: 2020-04-23 13:55:58,872,Event [Event=UpdateBillingProvQuote, timestamp=1587650161, JMSCo lationID=NA, JMSMessageID=ID:ESP-PD.174304828C850:5452E574, orderType=RatePlanFeatureChang e, quotePriority=NORMAL, conversationId=ESB-3C182E2F0413700E:AE1A98CE:A3E0A9546227:0B65, cr edits=NA, JMSReplyTo=pub.esb.genericasync.response, timeToLive=-1, serviceName=UpdateBillin gProvisioning, esn=9FFC24E704B114, accountNumber=900001675, social=222262211, MethodName=In ternalEvent, AdapterName=UpdateBillingProvQuote, meid=NA, orderNumber=810000000000576, quo teNumber=65212270, ReplyTo=NA, userName=misskleintjemoi, EventConversationID=NA, mdn=607237 5921, accountType=PostPaid, marketCity="NEW ORLEANS", marketState=LA, marketZip=70189, bill ingCycle=6, autoBillPayment=T, phoneCode=SS2, phoneType=Feature, phoneName="Samsung Solstic e 2", planCode=ULPOST70, planType=PostPaid, planPrice=69.99, planName="Unlimited", planDesc ription="Nationwide Unlimited Minutes, Unlimited Text, Unlimited Data", cardNumber=35288276 16057876, networkProviderName=Splunktel] Show less _time: 1635980778.822 cribl_breaker: ndjson host: 127.0.0.1 index: cribl source: /opt/tibco/tra/apps/ESB/logs/business_event.log sourcetype: business_event </pre> |

Last but not least, the four important pillars will guide you throughout the journey to maximize your outcome.

- **Experiment and Learn:** With the instructions in hand, begin working through the lab exercises. Utilize the features and functionalities of Cribl LogStream to complete the tasks assigned in the lab. Don't hesitate to experiment and explore different options to deepen your understanding.
- **Seek Assistance if Needed:** If you encounter any challenges or have questions while working through the labs, don't hesitate to reach out for assistance. You can refer to the documentation, community forums, or contact support for help and guidance.
- **Review and Reflect:** Once you've completed the lab exercises, take some time to review your work and reflect on your learning. Consider what you've accomplished, any insights gained, and areas for further exploration or improvement.
- **Repeat and Explore More:** To further enhance your skills and knowledge, feel free to explore additional labs and exercises available in the Cribl Cloud environment. Repeat the process outlined above to continue learning and expanding your proficiency with Cribl LogStream.