TechLineage

Cogniyug

A Real time BIG Data Analytics Platform to derive Actionable Intelligence from Time Series Machine Data

Quick Start Guide

September 2013

Contents

Overview

The purpose of this document is to provide a quick introduction to 'Cogniyug', a real-time analytics platform for analyzing time series machines data. This document will help you to get started with Cogniyug in less than10 minutes by explaining some of its key features very briefly. For detailed information and elaborate explanation, we strongly recommend you to refer to the User Guide and the Administration Guide.

Download and Installation

Once you have downloaded the installer (INSTALLER_COGNIYUG_1.0.00.tar.gz) for evaluation version of Cogniyug, please transfer the same to a Linux server with following suggested minimum server configuration. [If you do not have access to the evaluation version of Cogniyug, you can request the same by writing to us on support@techlineage.com]

At the moment, Cogniyug is supported to run on Red Hat Enterprise Linux 6.x or Cent OS 6.x (x86_64) only. We recommend following server configuration to successfully install and run the evaluation version of Cogniyug on a single Linux server.

Operating System	RAM (Memory)	CPU	Disk Space	Network Configuration
Red Hat Linux 6.x Or Cent OS 6.x (x86_64)	12 GB or more	4 virtual cores or more	50 GB on the filesystem where Cogniyug is installed	Static IP address to the server on which Cogniyug is installed

The Installer will install and start all the components of Cogniyug on the Linux Server. To proceed with the installation, perform following steps as mentioned below:

1. Extract the Cogniyug installer file ‘INSTALLER_COGNIYUG_1.0.00.tar.gz’ in a suitable directory by running the following command.
   ```
   tar -xzf INSTALLER_COGNIYUG_1.0.00.tar.gz
   ```
2. This will create a directory with name 'installer'. Go to the 'installer' directory (cd installer)
3. Run the installation script
   ```
   ./setup.sh
   ```
4. This will start the installation procedure which is pretty straight forward. You have to
   a. Accept the Trail License Agreement
   b. Enter Full path of the directory to install Cogniyug (referred henceforth as $COGNIYUG_ROOT)
   c. Choose ALL the components to install on the same server. (option 3 when installer prompts you to install the components of Cogniyug)
   d. Enter an IP address for the web server
5. Installer will start all the required Cogniyug processes.
6. After the installation is complete go COGNIYUG_ROOT/COGNIYUG/Hooks directory. Copy the file demo.txt to your windows computer which will use soon to upload the data into Cogniyug.

Note:

- To restart all the processes of Cogniyug you can run init.sh script from directory $COGNIYUG_ROOT
- To stop all the processes of Cogniyug you can run stop.sh script from directory $COGNIYUG_ROOT
- If you want to delete all the imported data and restart Cogniyug all over again, you can use reset.sh followed by init.sh

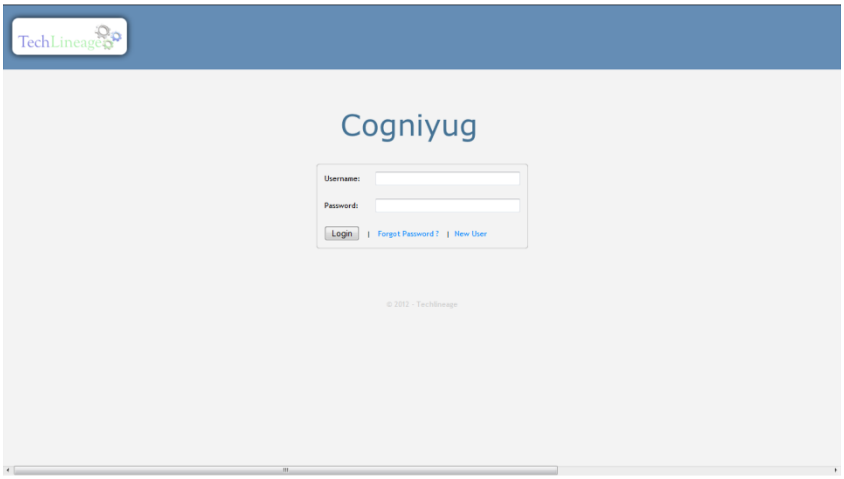
Login

Once the Cogniyug installation is complete and all its constituent processes have been started, you are ready to login to Cogniyug through its web interface. Open a browser (Mozilla Firebox or Google Chrome) and enter the following URL:

http://<ip-address>:8000

Where <ip-address> denotes the IP address of the Linux Server you provided for the web server (step 4-d above).

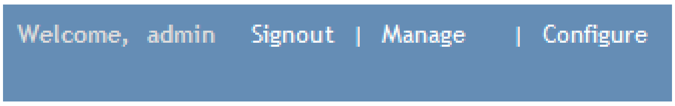
This should open the login page in the web browser as shown below:



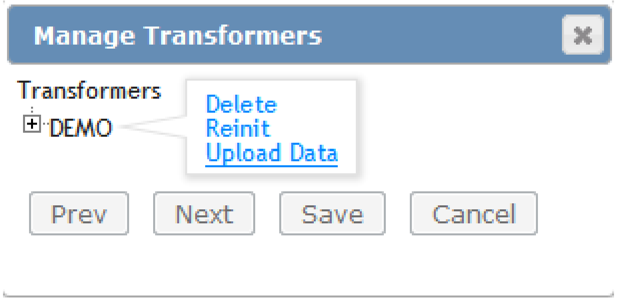
If you don't see the above window, you may have some configuration problem and the best thing would be to contact TechLineage support by writing to 'support@techlineage.com' (Please explain your problem as much as you can in your e-mail to support)

Basic Configuration

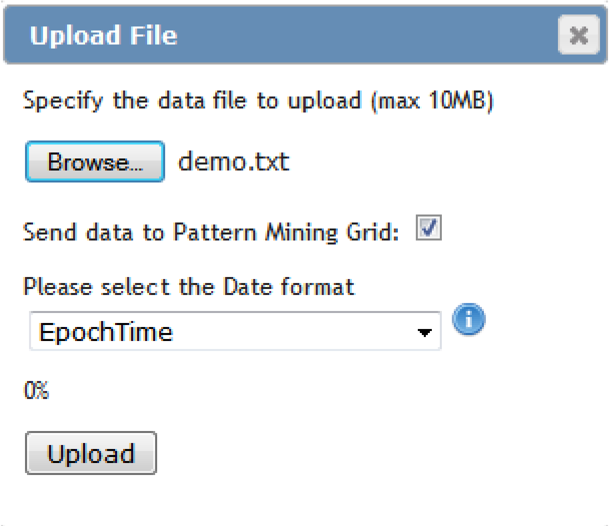
This is the time to import some data into Cogniyug and play around a bit with it. There are multiple ways to get the data into Cogniyug. This being the Quick Start guide, we will explain the simplest method here. After you login, click on 'Configure' in the right hand corner of the 'Home' page.



Click the 'Transformer' menu option – it will open the 'Manage Transformers' dialog box as shown below. (We have detailed explanation about the Transformer and other Cogniyug terminologies in the 'User Guide' and 'Administration Guide'.) You will see a pre-packaged Transformer named, 'DEMO'. Just click on this Transformer and Click 'Upload Data'



A new 'Upload File' dialogue will open as shown below



Specify the data file to upload (max 10MB)

demo.txt

Send data to Pattern Mining Grid: ☑

Please select the Date format

EpochTime

0%

Click on Browse button to browse the client side files (This will browse the files on the compute where your browser is running i.e. your windows desktop). Locate the demo.txt file on your local computer that we copied from Hooks directory in step 6 of "Download and Installation" section.

Select the checkbox against "Send data to Pattern Mining Grid".
From 'select the Date format' dropdown box, select EpochTime option that appears at the bottom of the list.

Click 'Upload' and wait for some time. The demo data will be imported into Cogniyug for our analysis.

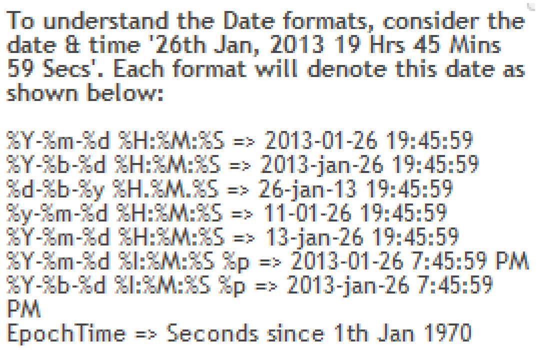
We uploaded the file 'demo.txt' in this case. This file conforms to Cogniyug Data format explained in detailed in the User Guide. Since Cogniyug Data format understands only EPOCH timestamps, we selected 'EpochTime' as the Date format above. If you examine demo.txt file, you will quickly realize that it has EPOCH timestamps so that it conforms to the Cogniyug data format.

However, for simplicity the 'Upload File' option also supports a bunch of other date formats. Click on the small 'info' icon ⓘ adjacent to the Date format field shown above to understand the supported 'Date Formats' while uploading a file using 'Upload File' option. Following table explains the meaning of the symbols used in the date format.

Symbol	Meaning of the symbol
%Y	Year with century as a decimal number (e.g. 2013)
%m	Month as a decimal number [01,12]. (e.g. 12 stands for December)

%d	Day of the month as a decimal number [01,31].
%H	Hour (24-hour clock) as a decimal number [00,23]. (e.g. 14 indicates 02PM)
%M	Minute as a decimal number [00,59] (e.g. 33 indicates 33 minutes passed the hour of the day)
%S	Second as a decimal number [00,61]
%b	Locale's abbreviated month name (e.g. Jan, Feb, Dec etc)
%y	Year without century as a decimal number [00,99]. (e.g. 13 means 2013)
%I	Hour (12-hour clock) as a decimal number [01,12].(e.g. 10 means 10 AM/PM)
%p	Locale's equivalent of either AM or PM

Using these date formats, you can write your own dates in the following human readable formats and upload the file.



To understand the Date formats, consider the date & time '26th Jan, 2013 19 Hrs 45 Mins 59 Secs'. Each format will denote this date as shown below:

```
%Y-%m-%d %H:%M:%S => 2013-01-26 19:45:59
%Y-%b-%d %H:%M:%S => 2013-jan-26 19:45:59
%d-%b-%y %H.%M.%S => 26-jan-13 19:45:59
%y-%m-%d %H:%M:%S => 11-01-26 19:45:59
%Y-%m-%d %H:%M:%S => 13-jan-26 19:45:59
%Y-%m-%d %I:%M:%S %p => 2013-01-26 7:45:59 PM
%Y-%b-%d %I:%M:%S %p => 2013-jan-26 7:45:59
PM
EpochTime => Seconds since 1th Jan 1970
```

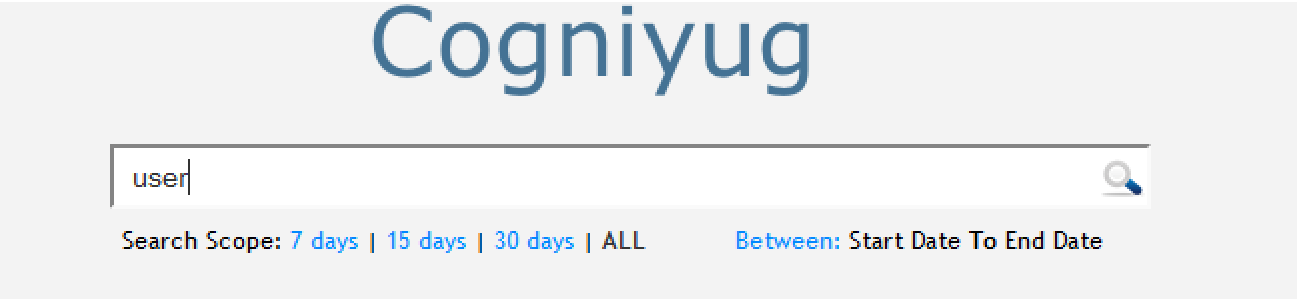
Remember that the date field uses hyphen (or dash '-') as the separator and timestamp field uses colon (':') as the separator. Try to create some small test files using above date formats in your favorite editor.

NOTE: - You cannot mix the above date formats in one single file. A file has to decide on a date format and stick to it in all the messages.

The Search

After you have configured your first Transformer successfully, the next step is to look for your data in Cogniyug and then perform various operations on the data.

Login to Cogniyug Web UI using admin/admin credentials and on the Home page, enter a single word 'user' in the search window as shown below and hit enter.

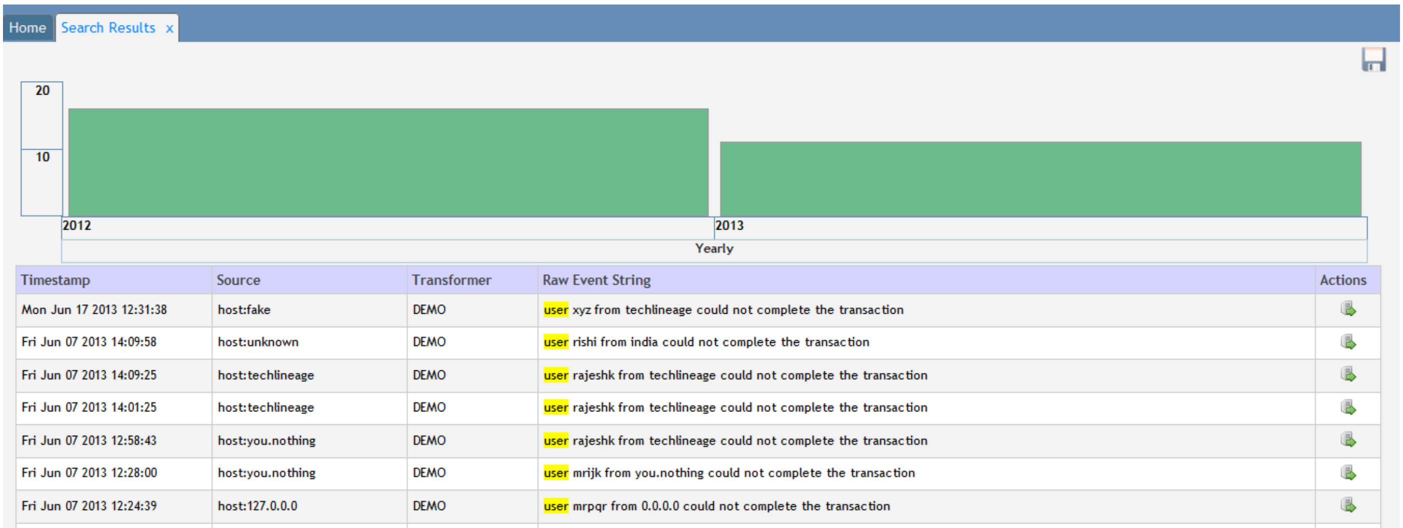


Cogniyug

user

Search Scope: 7 days | 15 days | 30 days | ALL   Between: Start Date To End Date

It will open up a new tab with 'search results' as shown below



Timestamp	Source	Transformer	Raw Event String	Actions
Mon Jun 17 2013 12:31:38	host:fake	DEMO	user xyz from techlineage could not complete the transaction	
Fri Jun 07 2013 14:09:58	host:unknown	DEMO	user rishi from india could not complete the transaction	
Fri Jun 07 2013 14:09:25	host:techlineage	DEMO	user rajeshk from techlineage could not complete the transaction	
Fri Jun 07 2013 14:01:25	host:techlineage	DEMO	user rajeshk from techlineage could not complete the transaction	
Fri Jun 07 2013 12:58:43	host:you.nothing	DEMO	user rajeshk from techlineage could not complete the transaction	
Fri Jun 07 2013 12:28:00	host:you.nothing	DEMO	user mrijk from you.nothing could not complete the transaction	
Fri Jun 07 2013 12:24:39	host:127.0.0.0	DEMO	user mrpqr from 0.0.0.0 could not complete the transaction	

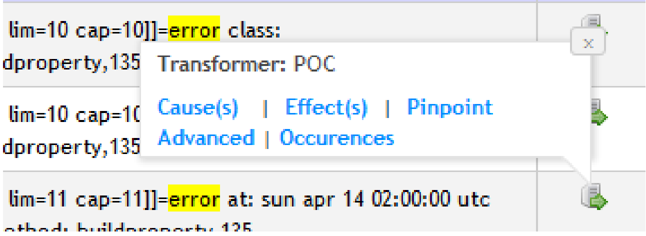
The 'Search Results' page is mainly divided into two halves, the top portion or the first half is the 'time-density' graph and the bottom portion or the second half shows the actual search results in the paginated format.

You can single click or double Click on the time density graph and check the 'Results' pane in the bottom half of search results. A single click will basically show you the data from the respective time region and double click will take you deeper into the data.

Cogniyug supports strong grammar and expressions using which you may construct complex search queries. For example, you may search "user AND xyx" to see the result of 'user' with name 'xyz'. Try few searches yourself. Please refer to User Guide for examples and more explanation about the search grammar, how to save a search, how to limit the scope of the search etc.

Actions on search results

After performing the 'search' and locating the exact instance of the event/log message, you will be able to perform various actions on the selected event/log message. The right-most column of the Search Results window has Actions icon i.e. . Locate the event, say "user xyz from techlineage could not complete the transaction" and click on actions to see available actions as shown below:



lim=10 cap=10]]=error class:
dproperty,135

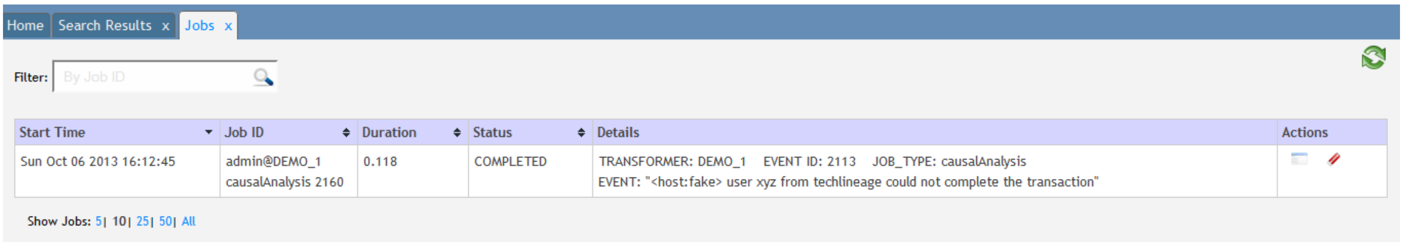
lim=10 cap=10
dproperty,135

lim=11 cap=11]]=error at: sun apr 14 02:00:00 utc
ethod: buildproperty 135

Transformer: POC

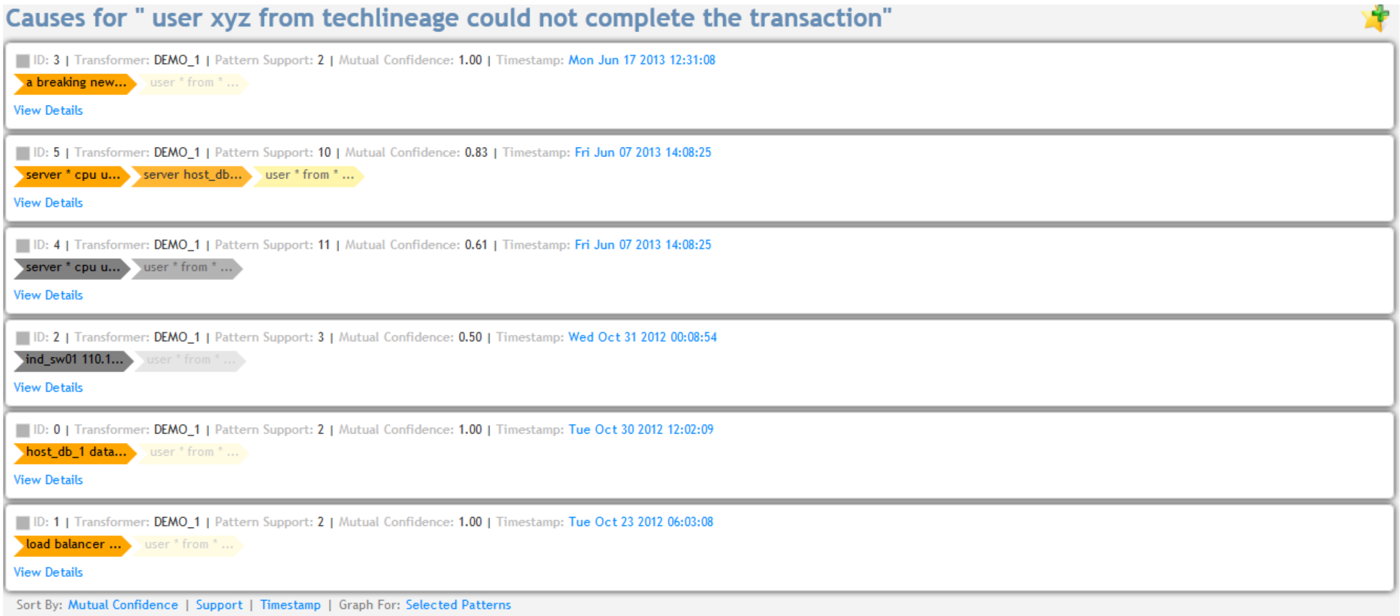
Causal Analysis

Click on 'Causes' and a dialog indicating that the request has been converted into a job will appear on the screen. Just acknowledge the same and go to Jobs panel by clicking 'Manage -> Jobs' at the top right hand corner of the browser (next to 'Logout' option). This will open up Jobs tab page as shown below. You will be able to see the job that you submitted for causal analysis.



Start Time	Job ID	Duration	Status	Details	Actions
Sun Oct 06 2013 16:12:45	admin@DEMO_1 causalAnalysis 2160	0.118	COMPLETED	TRANSFORMER: DEMO_1 EVENT ID: 2113 JOB_TYPE: causalAnalysis EVENT: "<host:fake> user xyz from techlineage could not complete the transaction"	

Click on 'Show Results' icon i.e. in the last column of the Job's tab. A new tab with Job results will open as shown below



Causes for " user xyz from techlineage could not complete the transaction"

ID: 3 | Transformer: DEMO_1 | Pattern Support: 2 | Mutual Confidence: 1.00 | Timestamp: Mon Jun 17 2013 12:31:08
a breaking new... user * from * ...
View Details

ID: 5 | Transformer: DEMO_1 | Pattern Support: 10 | Mutual Confidence: 0.83 | Timestamp: Fri Jun 07 2013 14:08:25
server * cpu u... server host_db... user * from * ...
View Details

ID: 4 | Transformer: DEMO_1 | Pattern Support: 11 | Mutual Confidence: 0.61 | Timestamp: Fri Jun 07 2013 14:08:25
server * cpu u... user * from * ...
View Details

ID: 2 | Transformer: DEMO_1 | Pattern Support: 3 | Mutual Confidence: 0.50 | Timestamp: Wed Oct 31 2012 00:08:54
ind_sw01 110.1... user * from * ...
View Details

ID: 0 | Transformer: DEMO_1 | Pattern Support: 2 | Mutual Confidence: 1.00 | Timestamp: Tue Oct 30 2012 12:02:09
host_db_1 data... user * from * ...
View Details

ID: 1 | Transformer: DEMO_1 | Pattern Support: 2 | Mutual Confidence: 1.00 | Timestamp: Tue Oct 23 2012 06:03:08
load balancer ... user * from * ...
View Details

Sort By: Mutual Confidence | Support | Timestamp | Graph For: Selected Patterns

This is an important page that shows all possible causes of the event *type* 'User xys from techlineage could not complete the transaction'. Each row of the results is a *pattern* with statistical measures such as

- Pattern Support indicating how many times the pattern has appeared
- Mutual Confidence indicating the confidence of the cause
- Timestamps showing the exact occurrence time of each pattern. If you click on the timestamps, you will see a list of the timestamps. The number of timestamps in the timestamp list will be exactly equal to the Pattern Support value.

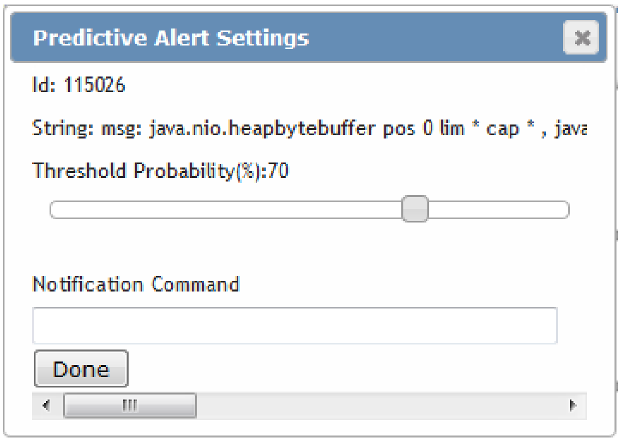
You may sort the results on any of the above three fields. You may also click on any 'View Details' of any pattern and check the details

(Note: In the above example, you may see that there some events with wild char characters e.g. 'user * from * could not complete the transaction'. Here Cogniyug is generalizing the analysis for the event's *type* rather than specific events. This is the default behavior of Cogniyug and we will explain more about it in the User Guide.)

Please refer to User Guide for deeper explanation on all the statistical measures reported by Cogniyug and their interpretation.

Predictions

After seeing the various causes, you may feel that is important to predict this event. You can simply click on the 'Predict Event' icon at the right hand corner of the Job results page to define the prediction in the following window



Id: 115026

String: msg: java.nio.heapbytebuffer pos 0 lim * cap * , java

Threshold Probability(%):70

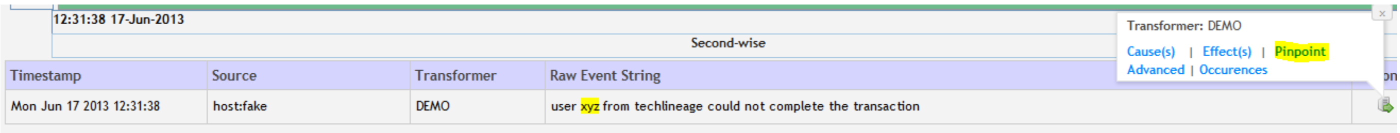
Notification Command

Press 'Done' and you have successfully configure the prediction for the event 'user * from * could not complete the transaction'. For deeper explanation on predictions, please refer to Use Guide.

Pinpoint

In the above example we did a *generic casual* analysis for all the events that were of type 'user * from * could not complete the transaction'. You may want to perform an accurate analysis for a specific instance of a specific event that has happened on a specific date. Go to "Home" tab and search the string, say 'user' again. Now in the search results locate the event 'user xyz from techlineage could not complete the transaction'. Let us try to understand why this particular event happened at a particular time i.e. on Mon Jun 17 2013 12:31:38.

Click 'Pinpoint' in the 'Actions' column in the 'Search Results' tab for the specific event.


12:31:38 17-Jun-2013

Second-wise

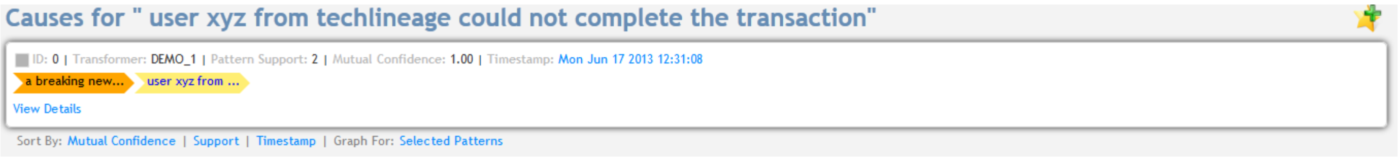
Transformer: DEMO

Cause(s) | Effect(s) | Pinpoint

Advanced | Occurences

Timestamp	Source	Transformer	Raw Event String	on
Mon Jun 17 2013 12:31:38	host:fake	DEMO	user xyz from techlineage could not complete the transaction	

A Job will be submitted and the results of the same can be viewed in Job's tab as explained in the previous example.


Causes for " user xyz from techlineage could not complete the transaction"

ID: 0 | Transformer: DEMO_1 | Pattern Support: 2 | Mutual Confidence: 1.00 | Timestamp: Mon Jun 17 2013 12:31:08

a breaking new... user xyz from ...

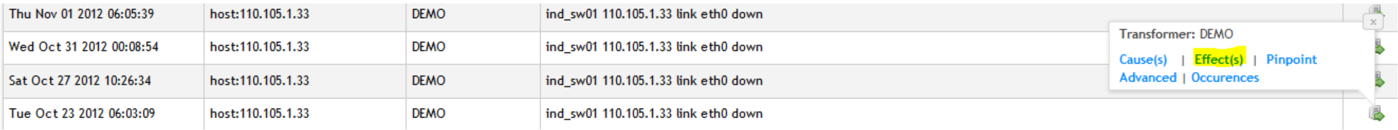
View Details

Sort By: Mutual Confidence | Support | Timestamp | Graph For: Selected Patterns

The result in this case will be pattern(s) explaining the specific reason(s) behind the occurrence of the 'specific instance' of the event on Mon Jun 17 2013 12:31:38

Effect Analysis

Search for an event, say "link eth0 down" by entering this string in the Search window. (Note: Enclose the string in double quotes as we are looking for an exact match).


Thu Nov 01 2012 06:05:39	host:110.105.1.33	DEMO	ind_sw01 110.105.1.33 link eth0 down
Wed Oct 31 2012 00:08:54	host:110.105.1.33	DEMO	ind_sw01 110.105.1.33 link eth0 down
Sat Oct 27 2012 10:26:34	host:110.105.1.33	DEMO	ind_sw01 110.105.1.33 link eth0 down
Tue Oct 23 2012 06:03:09	host:110.105.1.33	DEMO	ind_sw01 110.105.1.33 link eth0 down

Transformer: DEMO

Cause(s) | Effect(s) | Pinpoint

Advanced | Occurences

Click on 'Effects' as shown above. Now, view the results of the Job created for this Effect Analysis. The results will have all the statistical measures as that of the Causal Analysis Job. For details on interpreting the results of the Effect Analysis jobs, please refer to the User Guide.

Occurrences

This option in the 'Actions' column of the 'Search Results' returns the exact occurrences of the selected event. The time density graph and results pane will be redrawn to show the exact matches of the events.

Done!

You have got a glimpse of capabilities of Cogniyug and you are all set to take a deeper dive into Cogniyug by referring to the User Guide.

For any questions, please feel free to write back to us on 'support@techlineage.com'