



## **ITRS Insights v1.4**

### **visualising Results User Guide v1.0**

Copyright 2016. ITRS Group Ltd. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of ITRS Group Ltd.

ITRS Group Ltd

6th Floor, The Bonhill Building, 15 Bonhill Street,

London, EC2A 4DN, UK

t: +44 (0)20 7638 6700

f: +44 (0)20 7256 5760

# CONTENTS

## CHAPTER 1

ITRS Insights Visualising Results User Guide .....	5
The Visualization Interface .....	7
Define Results and Duration Visualization Parameters .....	8
Chart Types .....	12
Dashboards .....	18

## GLOSSARY

**This page intentionally left blank.**

# CHAPTER 1

## ITRS INSIGHTS VISUALISING RESULTS USER GUIDE

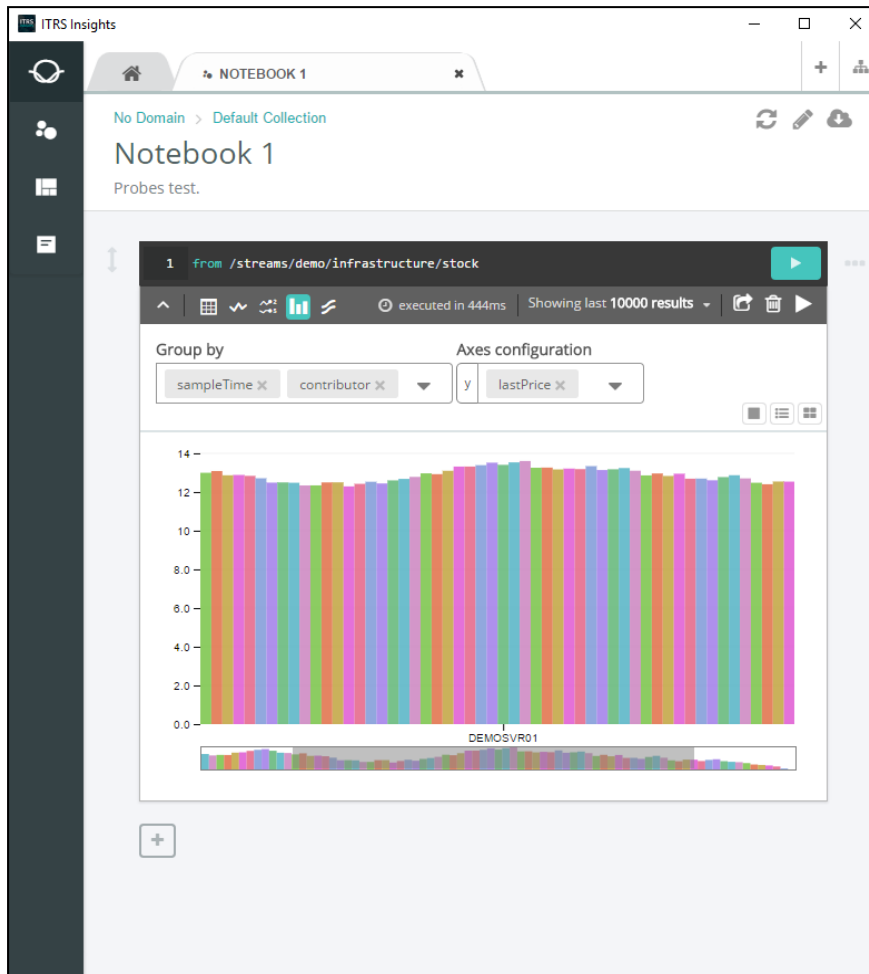
ITRS Insights provides a number of different ways to visualise your data and the outcome of your **queries**.

Once you have run the query, you can choose from a range of chart types to display the results, and you can apply a filter on how many results are displayed if you want to pare down your charts to something visually more manageable. Insights saves your visualization and chart preferences for each query, resetting them only if your query is changed in such a way that your visualization choices are no longer possible.

Finally, you can send any of your visualizations to one or more **Dashboards** to develop an aggregated visual display of your key query results in real time.

The visualisation options displayed to you are dependent on the content of the query that you run. For example, you will not be able to see the Anomaly Detection chart option unless your query includes a valid `select anomaly` clause.

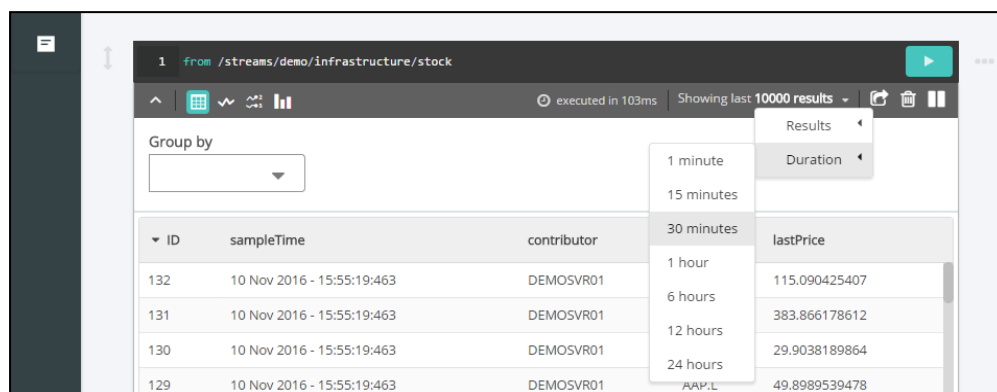
## THE VISUALIZATION INTERFACE



### The Visualization Interface

1. **Active tab** - identifies the Domain, Dashboard, Notebook or Collection that is being displayed
2. **Re-ordering bar** - drag and drop to reorder your query or free text search (when multiple queries or searches exist)

## DEFINE RESULTS AND DURATION VISUALIZATION PARAMETERS



Some queries will return vast amounts of data, and that may make your charts difficult to understand and interpret. To help you declutter your visualizations, Insights allows you to define an additional parameter to filter your results by - either Duration or number of Results.

For real-time searches, you can define either a duration over which to display results (anything from the last 1 minute to the last 24 hours), or a limit on the number of results that are displayed (from as few as the most recent 10 to as many as the most recent 10,000).

For historical queries, you can specify a limit on the number of Results it displays, but not a Duration.

Regardless of the Results and Duration parameters you specify, and regardless of whether the query is real-time or historical, the hard limit for the maximum number of results is 10,000 rows of data.

The drop-down menus for the Results and Duration settings are located on the visualization interface. They contain pre-configured settings that, once selected, are instantly applied.

Results (10, 100, 500, 5,000, 10,000(default)) limits the number of rows of results displayed



---

Duration (no limit (default), 1 minute, 15 minutes, 30 minutes, 1 hour, 6 hours, 12 hours, 24 hours) only available in real-time queries, this limits the number of results displayed to the number selected, based on when it was received in Insights.

Duration and Results parameters that you define are carried through to any dashboards or notebooks that you use to store the chart or query.

### How To Define a Results or Duration Limit for a set of Query Results

1. Run **ITRS Insights**
2. Create and run a **query**
3. Click the **Showing last xxx results** drop-down arrow
4. Select one of the **pre-set entries** for **either** Duration **or** Results (only one can be applied). The new parameter will be applied to the results in the window below

ITRS Insights

NOTEBOOK 1

No Domain > Default Collection

## Notebook 1

Probes test.

1 `from /streams/demo/infrastructure/stock`

2

executed in 103ms | Showing last

Group by

4

ID	sampleTime	contributor	
132	10 Nov 2016 - 15:55:19:463	DEMOSVR01	1 minute
131	10 Nov 2016 - 15:55:19:463	DEMOSVR01	15 minutes
130	10 Nov 2016 - 15:55:19:463	DEMOSVR01	30 minutes
129	10 Nov 2016 - 15:55:19:463	DEMOSVR01	1 hour
128	10 Nov 2016 - 15:55:19:463	DEMOSVR01	6 hours
127	10 Nov 2016 - 15:55:19:463	DEMOSVR01	12 hours
126	10 Nov 2016 - 15:55:18:463	DEMOSVR01	24 hours
125	10 Nov 2016 - 15:55:18:463	DEMOSVR01	AAP.L
124	10 Nov 2016 - 15:55:18:463	DEMOSVR01	IBM.L
123	10 Nov 2016 - 15:55:18:463	DEMOSVR01	VOD.L

Showing 1 to 10 of 132 entries

+

---

If you've set a duration limit on your real-time query results, you can reset the Duration to default (no limit) by selecting 10,000 from the Results drop-down.

## CHART TYPES

### KPI

The Key Performance Indicator chart is designed to be placed on a dashboard or other UI control to provide rapid interpretation of a query result.

You can view the data as a *number*, *column* or *sparkline*, or select the *status* setting to display a color-coded arrow indicator that allows super-fast understanding of whether the KPI trend is good or bad.

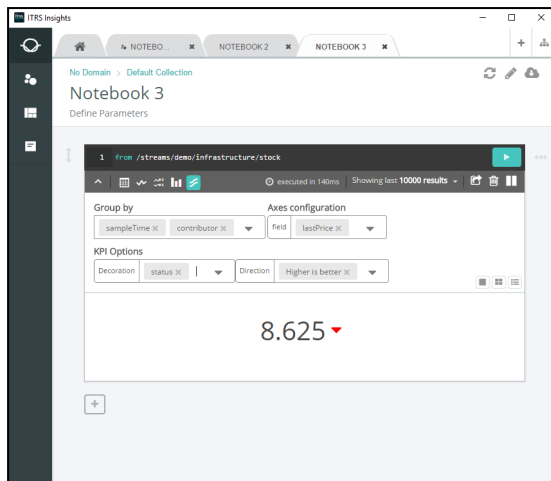
You can configure the following fields in order to customize your visualization:

**Group By** - group results by one of the variables shown in the drop-down menu

**Axes Configuration** - assign a variable to the x and y axes using the drop-down menu

**KPI Options** - set the *Decoration* of the visualization (*number* (default), *status*, *column* or *sparkline*). You can also set the meaning of the trending data (*Higher is better* (default) or *Lower is better*.) When *Decoration* is set to *Status*, the *Direction* setting will determine when a green arrow or red arrow will be displayed next to the values being returned by the query.

When you select *sparkline* or *column* as your *Decoration*, only the ten most recent results are displayed.



## Table



The most simple, and default, manner of displaying query results is a table. Tables can be sorted by selecting the appropriate column.

You can configure the following fields in order to customize your visualization:

**Group By** - group results by one of the variables shown in the drop-down menu

The screenshot shows the ITRIS Insights application interface with the 'Table' view selected. The table displays query results for the field 'lastPrice'. The table has columns for 'ID', 'sampleTime', 'contributor', 'ticker', and 'lastPrice'. The data is grouped by 'sampleTime' and 'contributor'. The table shows 10 rows of data, with the first row having an ID of 8322 and a lastPrice of 7.6479493955. The table is sorted by 'lastPrice' in descending order. The 'Showing last: 10000 results' message is visible at the top right of the table.

ID	sampleTime	contributor	ticker	lastPrice
8322	21 Nov 2016 - 16:31:12:341	DEMOSVR01	RECL	7.6479493955
8316	21 Nov 2016 - 16:31:11:341	DEMOSVR01	RECL	7.7171723648
8310	21 Nov 2016 - 16:31:10:341	DEMOSVR01	RECL	7.71811728942
8304	21 Nov 2016 - 16:31:09:341	DEMOSVR01	RECL	7.70477407056
8298	21 Nov 2016 - 16:31:08:341	DEMOSVR01	RECL	7.77781203413
8292	21 Nov 2016 - 16:31:07:341	DEMOSVR01	RECL	7.76341863238
8286	21 Nov 2016 - 16:31:06:341	DEMOSVR01	RECL	7.80028952957
8280	21 Nov 2016 - 16:31:05:341	DEMOSVR01	RECL	7.76235822183
8274	21 Nov 2016 - 16:31:04:341	DEMOSVR01	RECL	7.82478263092
8268	21 Nov 2016 - 16:31:03:341	DEMOSVR01	RECL	7.89005010371

## Line Chart



A line chart or line graph is a type of chart which displays information as a series of

data points called 'markers' connected by straight line segments. The measurement points are ordered (typically by their x-axis value) and joined with straight line segments.

A line chart is often used to visualise a trend in data over intervals of time – a time series – thus the line is often drawn chronologically.

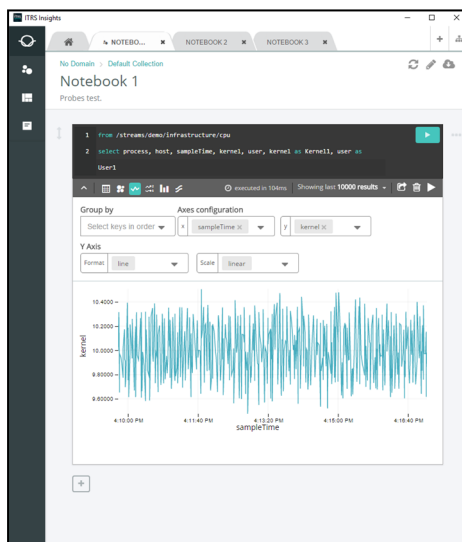
You can configure the following fields in order to customize your visualization:

**Group By** - group results by one of the variables shown in the drop-down menu

**Axes Configuration** - assign a variable to the x and y axes using the drop-down menu

**Y Axis Scale** - choose your scale from the drop-down menu. Choices include linear and logarithmic.

**Y Axis Format** - choose your format from the drop-down menu. Choices include line, area and stacked area



## Bubble Chart



A bubble chart is a type of chart that displays three dimensions of data. Each entity with its triplet ( $v_1$ ,  $v_2$ ,  $v_3$ ) of associated data is plotted as a disk that expresses two of

the vi values through the disk's xy location and the third through its size.

You can configure the following fields in order to customize your visualization:

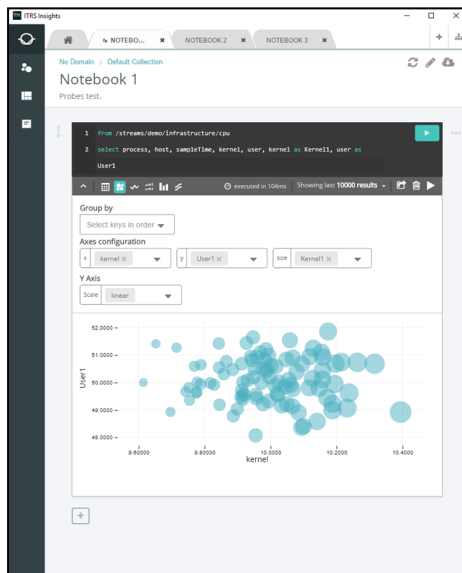
**Group By** - group results by one of the variables shown in the drop-down menu

**Axes Configuration** - assign a variable to the x and y axes using the drop-down menu

**Y Axis Scale** - choose your scale from the drop-down menu. Choices include linear and logarithmic.

For example with the query:

```
from /streams/demo/infrastructure/cpu
select process, host, sampleTime, kernel, user, kernel
as kernel1, user as user1, kernel as kernel2, user as
user2, kernel as kernel3, user as user3
```



## Bubble Map

A bubble map displays geographic location and size data points of a query as bubbles.

It allows you to see the geographical dispersion of data points. Bubble maps should be used when showing density of information or events with a geographical context.

You can configure the following fields in order to customize your visualization:

**Group By** - group results by one of the variables shown in the drop-down menu

**Axes Configuration** - assign a variable to the x and y axes using the drop-down menu

**Y Axis Scale** - choose your scale from the drop-down menu. Choices include linear and logarithmic.

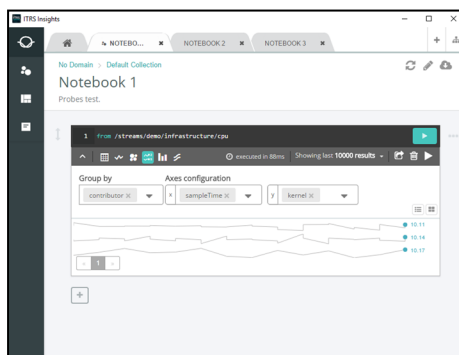
## Spark lines

A sparkline is a very small line chart, typically drawn without axes or coordinates and presents the general shape of the variation (typically over time) in some measurement.

You can configure the following fields in order to customize your visualization:

**Group By** - group results by one of the variables shown in the drop-down menu

**Axes Configuration** - assign a variable to the x and y axes using the drop-down menu

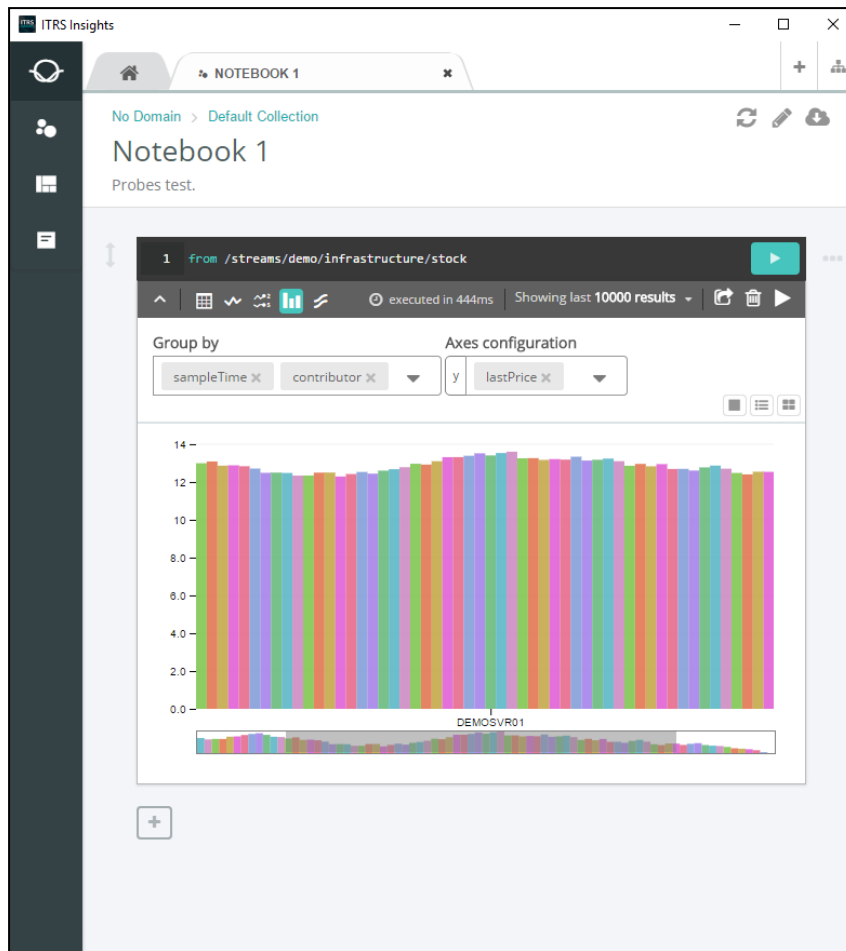


## Column Chart

Selecting the column chart an axis selection that makes sense is automatically



chosen.



```
from historical /streams/demo/fix/exchange where MsgType=="New  
Order Single" group by Symbol select Symbol, sum(OrderQty) as  
Volume
```

Depending on the contents of your query return you can change the axis configurations and also group by certain values.

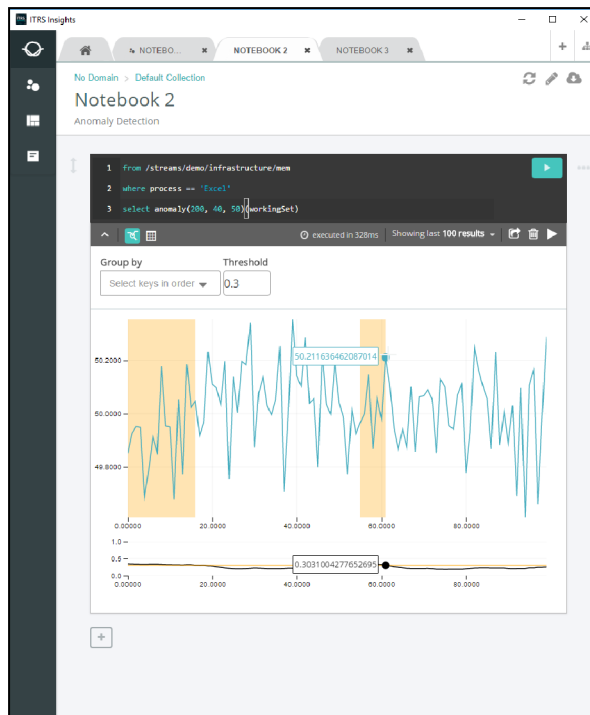
### Anomaly Detection 📊

This chart option will appear when using **Anomaly** and highlights where anomalies are found. So for instance if we take an ECG stream then we can run a query to emit and chart the following.

With the anomaly displayed underneath and any area where this is breached highlighted on the main chart.

```
from /streams/demo/infrastructure/ecg
```

```
group by contributor
select contributor, anomaly(200, 40, 20) (value) as result
emit every value
```



## DASHBOARDS

You can also use a **Dashboard** to share the visualization of query results without the viewer needing to have direct access to the query and/or data.

# GLOSSARY

## C

---

### Collector

New term for a lightweight monitoring agent, which is deployed on every managed Node. See Netprobe.

### Contributor

An external source that provides one or more data streams to Valo. Contributors can be grouped together by common attributes to create Domains.

## D

---

### Dashboard

Dashboards provide an aggregated view of Data Visualizations

### Domain

Two or more Contributors grouped together by a common attribute. Domains help to organise and group different data sources in intuitive ways.

## G

---

### Gateway

A network node that provides access to another network that uses different protocols and enables transmitted data to use its routing paths.

## I

---

### Insights

A streaming big data analytics platform that simplifies the complexity involved in analysing vast amounts of data at speed. Insights combines big data storage with a real time computation engine and in-built machine learning and algorithms.

### ITRS Geneos

A real-time monitoring tool for managing increasingly complex and interconnected IT estates. Built for financial services and trading organisations, it

collects a multitude of data relating to the performance of the servers, infrastructure, connectivity and applications, analyses it to detect anything untoward, and presents it in relevant, intuitive visualisations to help diagnose and fix issues quickly.

## N

---

### Netprobe

Lightweight monitoring agent, which is deployed on every managed Node

### Notebook

A place in which to store a query or search, or a pipeline of queries or searches.

## S

---

### Schema

Document of understanding that defines what data a stream contains - its structure and shape - and in what format.

### SSR

The semi-structured repository (SSR) is based on Lucene which provides very powerful text search capabilities. Even though Lucene is geared towards indexing text, it also has very good index support for numerical data. However, if the data contains purely numerical fields the TSR might be a better fit as a repository for this kind of data.

### Stream

A stream is made up of data (messages or events) coming from one or more external contributors. Each stream has a schema that defines what information, in what format is expected. Streams are append only.

## T

---

### Tenant

The highest level of data grouping. Within a company, it may be different departments such as Sales or Engineering. If a government is collecting data from its cities, the tenant could be the city name.

### Transformational Pipeline

Each query instruction takes an input and produces an output via some form of transformation.

### TSR

The Time Series Repository (TSR) is a custom built data repository designed to handle numerical time series oriented data streams. By time series we mean a series of data points each of which has an associated time stamp.

## V

---

### Valo

Real-time analytics on data streams