

# **GENESYS**

This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Workbench User's Guide

AD Insights Console

## Contents

- 1 AD Insights Console
  - 1.1 Statistics Summary
  - 1.2 Historic Heat-maps Summary
  - 1.3 Data-Table

# AD Insights Console

The Workbench Insights Console is a dedicated console page that displays:

- a real-time statistics summary of Active Insights/anomalies Critical, Major, Minor
- a statistics summary Heat-map of historic Insights/anomalies Score and Count not real-time; click Refresh to update
- a real-time Data-table of Active and Closed Insights/Anomalies

#### Important

- Workbench Insights are not necessarily always actionable, they may be merely informational events that the user can review to determine if further investigation/ analysis is required
  - i.e. utilize the Workbench Dashboards and Visualizations to dig deeper and determine if the Workbench Insights are truly business impacting issues
- Insights are not automatically closed and are required to be manually closed. Only closed insights are purged from the system after exceeding the environments configured retention period.
- In case of a switchover, where an Additional Anomaly Detection node is elevated to Primary, a period of 1 hour is reserved to ensure all models are accurately updated across nodes to reflect current state. During this period, new Workbench Insights will not be available.

Workbench Dashboards Al	arms <sup>8</sup> Changes	Channel Monitoring 🗸	Insights 100 Discover Vi	sualize Configuration		Status 📕 🗸	$2$ fizz $\checkmark$	?``
Insights						Active Insights	:(100) 📕 26 📕 30	44
Max. Anomaly Score			Refresh C	Insights Count			Refresh	G
Feb	Mar Apr	May .	Jun Jul	Feb	Mar A	pr May .	Jun Jul	
Mon				Mon				
Wed				Wed				
Fri <b>F</b> i	╋╋╋			Fri 🛛 🗖 🗖 🗖				
		None 1-25%	26-50% 51-75% 76-100%			None 1	-13 13-26 26-39	> 39
							× Show only Active In	isight
						Clear Active In	sight(s)	Γ×,
$\Box$ Generated $\neq \downarrow$ $\blacksquare$	Status 🗟	ç ≏≂ Severity ≯ ≏⇒	Insight Message 🦆 📿		Host 🧚 📿	Application → C	Data-Center	
Tue 06 Jul 2021 22:37:40	Active	Minor	Spike detected during last compared to the last 23 ho	60 seconds. 29% increase urs.	test_hostname	host	DC1	×
Tue 06 Jul 2021 12:19:40	Active	Major	Spike detected during last compared to the last 21 ho	60 seconds. 65% increase urs.	test_hostname	host	DC1	×
Mon 05 Jul 2021 02:53:41	Active	<ul> <li>Minor</li> </ul>	Spike detected during last compared to the last 23 ho	60 seconds. 29% increase urs.	test_hostname	host	DC1	×
Sun 04 Jul 2021 16:35:41	Active	<ul> <li>Major</li> </ul>	Spike detected during last compared to the last 21 ho	60 seconds. 65% increase urs.	test_hostname	host	DC1	×
Sun 04 Jul 2021 10:53:40	Active	Minor	Spike detected during last compared to the last 19 ho	60 seconds. 99% increase urs.	test_hostname	host	DC1	×
Fri 02 Jul 2021 15:09:41	Active	Minor	Spike detected during last	60 seconds. 99% increase	test_hostname	host	DC1	×
Total Insights: 103							∧ GoTo-	Тор

# Statistics Summary

The statistics summary of Active Insights, displays Active total Critical (=), Major(=), and Minor(=)



## Historic Heat-maps Summary

The statistics summary of historic Insights displays the last 6 months of summary data in the following graphical representation:



#### Max. Anomaly Score

The **Max. Anomaly Score** heat-map panel displays the *maximum* anomaly score detected by AD for each day.

Each square shows the specific source with the highest anomaly score that day: date, anomaly score value, data center name, host name and metric name. In this graph, the ranges are set as follows:

- 1% 25%: Normal Behavior
- 25% 50%: Minor Insights
- 51% 75%: Major Insights
- 76% 100%: Critical Insights

#### Insights Count

The **Insights Count** heat-map panel displays the number of anomalies detected with an anomaly score greater than 25% for each day.

Each square shows the date and the number of Insights detected that day; the ranges are calculated based on the maximum value detected during the last 6 months.

#### Important

- The AD Heat-maps display data based on the Workbench data Retention Period parameter
- The Workbench Retention Period is 30 days by default; therefore, by default the AD Heat-maps will show the last 30 days of AD Insights
- If/when the Workbench Retention Period is changed, the AD Heat-map display will be reflected accordingly; up to a maximum of the last 6 months of AD Insights
- Details of the Workbench Retention Period setting can be found here

## Data-Table

The real-time Insights Console data-table displays Workbench Insights - Machine Learning Anomalies raised with an anomaly score greater than 25%.

					Clear Active Ins	now only Active Instantion	sights
□ Generated 🍾 ↓ 🛗	Status ≯⊱ ≌⇒	Severity ≯⊱ ≌⇒	Insight Message 🤸 📿	Host ≯⊱ 📿	Application 🧚 📿	Data-Center	
Mon 28 Jun 2021 12:12:39	Active	<ul> <li>Minor</li> </ul>	Spike detected during last 60 seconds. 6.0% increase compared to the last 2.0 hours.	CC-CHE-CTIDB1	host	APAC	×
Mon 28 Jun 2021 07:38:33	Active	<ul> <li>Major</li> </ul>	Spike detected during last 51 seconds. 14.0% increase compared to the last 0.0 hours.	cc-dev-chn-w-2	host	IND	×
Mon 28 Jun 2021 07:31:41	Active	<ul> <li>Minor</li> </ul>	Spike detected during last 60 seconds. 72.0% increase compared to the last 18.0 hours.	cc-dev-chn-w-2	host	IND	×
Mon 28 Jun 2021 03:45:21	Active	<ul> <li>Major</li> </ul>	Drop detected during last 60 seconds. 7.0% decrease compared to the last 24.0 hours.	cc-tools-chn-dev-1	host	IND	×
Mon 28 Jun 2021 02:30:28	Active	Critical	Spike detected during last 60 seconds. 16.0% increase compared to the last 24.0 hours.	cc-tools-chn-dev-1	host	IND	×
		- 0.000	Spike detected during last 60 seconds. 1.0% increase				

#### Data-Table Default Columns

- Generated The date and time of an insight anomaly generation. (Note: Timestamps are stored in UTC and translated to local time based on the Users Browser Time-Zone)
- Status Indicates insight status is Active or Closed.
- Severity Denotes the severity of the anomaly . It can be Critical , Major, and Minor.
- Insight Message The message about the anomaly event in text format.
- · Host The name of the Host/Server associated to the anomaly event.
- Application The name of the application associated to the anomaly event.
- Data-Center The name of the Data-Center associated to the anomaly event.

#### Data-Table Additional Columns

Note: Additional column able to select using show/hide column option.

- ID The internal ID of the anomaly event.
- Cleared The date and time at when the anomaly event was cleared.
- **IP** The name of the IP associated to the anomaly event.
- Metric Name it's the specific metric monitored by a host or application. Can be CPU, Memory, Disk, Network .
- Anomaly Score core value assigned by AD, which determines how unusual the detected behavior in the metric is compared to its history

#### Insights Table Options

Show Only Active Insights: a toggle filter to show only the active Insights

- Clear Active Insight: a DataTable row icon to Close/Clear a single Insight
- Clear Active Insight(s): a button to Close/Clear multiple/selected (max 200 at a time) active Insights
- Show/Hide Column: an option to Show/Hide specific DataTable columns
- Export As XLS/PDF: export selected DataTable rows as PDF or Excel document
- Normal/Full-Screen To toggle between the normal and full screen mode for data table
- GoTo-Top: an option link to navigate to top of the Insights table

#### Important

• Post a Workbench Data-Center sync, only Active insights will be synced.

#### Insights Detail View

By clicking a particular Insight row in the Data-Table an Insight detail dialog will be presented with Visualizer, Correlations, and Detail tabs.

	Workbench Dashboards	Alarms 999+ 0	Changes Ch	nannel Monitoring 💛 Insights  Disco	ver )	lisualize Configuration	Status 🥎 🗸		? ~
I	nsights					Visualizer Correlations Details			×
	Generated ≯↓ ⊞	Status ≯ ≌	Severity ≯⊱	Insight Message 🍾 📿	Hos	Open Alert Anomaly Context CPU - Drop detected 49% (based last	13 hours)	Alert Type AD Prediction Severity	n
	Thu 03 Jun 2021 17:02:35	Active	Minor	P DEMO Insight: Drop detected during last 20 minutes. 49% decrease compared to the last 13 hours.	gv es	Anomaly Score		Minor	•
	Thu 03 Jun 2021 06:42:18	Active	<ul> <li>Critical</li> </ul>	P DEMO Insight: Drop detected during last 51 minutes. 93% decrease compared to the last 4 hours.	fw sy	30	70	80 90	100
	Tue 01 Jun 2021 16:40:40	Active	<ul> <li>Minor</li> </ul>	DEMO Insight: Spike detected during last 55 minutes. 48% increase compared to the last 12 hours.	uk ch ab	B 25- 20 Ministry Type:	ip06.frm.cct.genesysla .oadAverage 3pike Up	ab.com	1
	Mon 31 May 2021 11:03:09	Active	<ul> <li>Major</li> </ul>	P DEMO Insight: Spike detected during last 33 minutes. 67% increase compared to the last 20 hours.	uk ch ab	A Dereidy, in high: a dereidy, in high: a normaly Second Metric Value: State:	0% increase based la 15.45 17.42 2020-02-07 21:40:17 2020-02-07 20:55:17	st day	
	Mon 31 May 2021 07:05:58	Active	<ul> <li>Major</li> </ul>	P DEMO Insight: Drop detected during last 52 minutes. 52% decrease compared to the last 20 hours.	uk ch ab	10 12:00 15:00 18:00 21:00 00:00 Time (House)	5 )aily 03:00 (	06:00 09:00	
	Sun 30 May 2021 22:35:12	Active	Minor	P DEMO Insight: Drop detected during last 12 minutes. 33% decrease compared to the last 12 hours.	uk ch b.c	Time (roury)			
	Cun 30 May 2021 02-50-36	Activo	<ul> <li>Maior</li> </ul>	P DEMO Insight: Spike detected during last 11 minutes 50% increase	br				

#### Visualizer

Display Insights context in graphical view. Main Sections:

- Insight Source: Hostname metric name
- Insight Context: {anomaly\_type} {anomaly\_score} {duration\_time} {metric\_value}
  - In case where the Insights have many Anomaly Points; the Anomaly Score is the maximum score for

each Anomaly Point.

- Insight duration is defined as the time between the first and last anomaly point in the same hour; when this time is smaller than 15 minutes it will be displayed in seconds.
- Alert Type: AD Insight or AD Prediction
- Severity: Minor, Major or Critical
- Anomaly Graph: detailed zoom on anomalies detected.
  - Metric Value with information from one hour before and one hour after.
  - Normal regions to show commons ranges and variability.
  - Anomaly points (circles):anomaly type, severity, anomaly score, metric value, date and time.
  - Anomaly Score Legend

#### Visualizer Correlations Details



AD is able to detect four types of anomalies:

• Spike: is considered as an acute increase in the metric value followed by an immediate return to the underlying level.



• Drop: is considered as an acute decrease in the metric value followed by an immediate return to the underlying level.



• Jitter: is a set of drops and spikes with a duration greater than 15 minutes.



- Trend Prediction: Insights generated based on hourly trend predictions.
  - A new insight is generated when high values are (> 95%) predicted in the next hours [0 72 hours]
  - Score give an indication of the metric rate of change.
  - Because these insights are based on predictions, these don't have time correlations with other insights.
  - Alert Type: AD Prediction
  - A P icon is used in Insights Table to easily identify.



#### Correlations

Help to analyze time correlation details between insights:

- Different insights are correlated in a time frame of 30 minutes (gray region).
- A maximum of 5 correlated metrics are visualized.
- Each graphic as a title has the source: host name and metric name.
- For each metric are visualized the anomaly points as red circles.
- All graphics extends between one hour before the correlation region and one hour after.



#### 2. metricbeat\_10.20.192.122\_25 ens192 network\_in\_kBps



#### 3. metricbeat\_10.20.192.122\_46 cpu\_total



#### Details

Display table row information in vertical order:

- ID
- Generated date: Fri 24 Sep 2021 16:17:54
- Cleared date (empty for active insights)
- Status
- Severity
- Insight Message

AD Insights Console

- Host
- Application
- Data-Center
- IP
- Metric Name
- Anomaly Score

Visualizer	Correlations	Details
ID		59b3d798-4872-4a60-9abe-a2a56290260e
Generated		Sat 18 Sep 2021 04:12:58
Cleared		
Status		Active
Severity		Minor
Insight Mes	sage	Jitter detected in metricbeat_10.20.192.122_6 -
		cpu_total during 33 minutes; 37% score on metric
		value: 0.0
Host		
Application		host
Data-Center	r	DC_124
IP		
Metric Name	е	cpu_total
Anomaly Sc	ore	37.2

#### **AD Insight Alarms**

AD Alarms are part of Workbench Alarms in WD UI. AD automatically control the status for each alarm generated: continuously each alarm is monitored to be closed. These alarms have an hierarchical behavior: when an alarm is generated, automatically all below that are closed. AD can generate four types of alarms:

1. AD is not able to connect with Workbench Logstash.

- Severity: Critical
- Structure: {ad\_appname} is not able to connect with Logstash {logstash\_host}
- Suggested Actions: validate if Logstash configuration in both, AD and Logstash are properly. Check if Logstash Node is down or is restarting.

2. AD is connected to Workbench Logstash but is not receiving metric data.

- Severity: Critical
- Structure: {ad\_appname} is not receiving metric data from Logstash
- Suggested Actions: validate if Logstash is receiving data from Metricbeats or all Metricbeats are down.
- 3. AD is not receiving data from a particular workbench host
  - Severity: Major
  - Structure: {ad\_appname} is not receiving metric data from host {hostname}
  - Suggested Actions: validate if that specific host is down.
- 4. There is an additional type of Alarm generated when an AD node is down.
  - Severity: Critical
  - Structure: AD Node {ad\_node\_name} is down
  - Suggested Actions: validate if that specific host is down.

PE	Workben	ch Active Alarms			WB	Details	×
	Total	Critical	Major	<ul> <li>Mino</li> </ul>	Nr	ID	e8ce5e57-9eef-43c5-8ac3- b1db6bf70185
	0	0	0	0		Generated	Sat 18 Sep 2021 04:47:45
						Cleared	Sat 18 Sep 2021 04:53:01
ingage A	Alarms					Status	Closed
						Severity	<ul> <li>Major</li> </ul>
Cauc	uitu à œ	Alarm Massage	10		Hart & O	Alarm Message	WB_AD_ccdev-st-adtst5 is not receiving metric data from host metricbeat_10.20.192.125_25
Jeve	muy ∻ ≞⊳	Alarm Message	* ((		HOSE & CE	Host	metricbeat_10.20.192.125_25
• 1	Major	WB WB_AD_0 receiving metricbe	ccdev-st-adtst metric data fro at_10.20.192.1	5 is not om host 25_25	metricbeat_ 25_25	Application Sent to RAM	
• 1	Major	WB_AD_ receiving metricbe	ccdev-st-adtst g metric data fro at_10.20.192.1	5 is not om host 25_28	metricbeat_ 25_28	Service Expiration	172800
• 1	Major	WB_WB_AD_receiving metricbe	ccdev-st-adtst! g metric data fro at_10.20.192.1	5 is not om host 25_44	metricbeat_ 25_44	Data-Center	