Workbench User's Guide

Genesys Care/Support current

9/9/2022

Table of Contents

Workbench Deployment and User Guide

Welcome to the Genesys Care Workbench User's Guide version 9.3.000.00

Workbench is a consolidated suite of monitoring, testing and troubleshooting tools for your Genesys Engage On-Premise platform.

Workbench endeavours to simplify and accelerate the visibility, understanding and resolution of Genesys Engage On-Premise platform operational issues, empowering you with *insights into reality*.

This document provides you with the following information:

- Workbench Components and Architecture
- Workbench Planning, Deployment and Upgrade procedures
- The usage of Workbench features/functionality
- Workbench Configuration Options
- FAQ's, Limitations, Best Practises

Workbench Overview

Genesys Workbench (WB) 9 is a monitoring, testing, troubleshooting and remediation solution, with a suite of tools to assist with the operational monitoring, management and troubleshooting of Genesys platforms.

Workbench (WB) 9.0 was released February 2020, this WB 9.0 release was a reinvention that endeavours to provide a go-to monitoring, testing, troubleshooting and remediation product which simplifies and accelerates identification and resolution of issues, empowering Genesys customers and partners with valuable operational insights to better manage and support their Genesys Engage platform.

Workbench 9.1 adds an **optional** Metric data ingestion feature (from remote hosts/process - i.e. sip, urs, gvp etc) that enables observability of host and process CPU, Memory, Disk and Network metric data, providing rich insights and analysis capability into host and process metric utilization, performance and trends.

Workbench 9.2 adds an **optional** Anomaly Detection Workbench “Insights” feature that will autonomously and predictively raise anomalies based on outlier analysis of the ingested metric data (CPU, RAM, Disk, Network); details of the Workbench AD feature can be found here: Workbench Anomaly Detection (AD).

Workbench 9.3 adds an Notification Webhook feature that provides a simple and efficient method to send information (currently that information is limited to Active Alarms within Workbench; either Engage [i.e. Host Unavailable] Alarms received from Engage SCS or Workbench [i.e. Channel Monitoring - Call Flow - No Answer] generated) from Workbench, to a customer developed, or external, HTTP[S] endpoint; details of the feature can be found here: Notification Channels and Workbench Alerts.

Workbench 9.3 Key Features:

- A new **Workbench UI** enabling richer Dashboard and Visualization capabilities providing an at-a-glance view of Genesys platform health and status.
- View Genesys Engage "Alarms" via the **Workbench Alarms Console**, complimenting existing products such as Genesys Administrator Extensions (GAX).
- View Genesys Engage "Changes" via the **Workbench Changes Console**, enabling greater context and perspective of Genesys Engage Application Object changes.
- Leverage Workbench **Channel Monitoring** to create and schedule voice test calls to proactively identify potential interaction and routing issues before your customers are impacted; this feature can test Genesys voice call flows ensuring your service is functioning as designed and alerting you when issues are encountered.
    - Workbench Channel Monitoring integrates directly to the Genesys SIP Server and not the SIP Server Proxy
- Take advantage of the Workbench **Remote Alarm Monitoring Service**, when activated, the customers on-premise Workbench instance sends specific Alarms to Genesys Customer Care, this alarm interaction is intelligently routed to a Genesys analyst who will then proactively create a Support Case and will liaise with the customer accordingly to resolve the issue(s); the alarms can also be sent to the Genesys Mobile App if subscribed.

- View "Audits" via the **Workbench Configuration/Auditing Console**, enabling similar context to Changes with added detail such as Workbench Login/Logout events.
- **Ingest Metric data events**, via the Workbench Agent(s), for analysis, troubleshooting and operational insights
- Explore and observe metric data event insights via Workbench Dashboards and Visualizations
- Create your own custom metric data event Dashboards and Visualizations
- Analyze the 'raw' ingested metric data events via the Workbench Discover Console
- Search/filter for particular metrics, components, values etc
- Anomaly Detection **Workbench Insights** feature that will be autonomously and predictively raise anomalies based on the ingested Metric data
- Notification Webhook feature that provides a simple and efficient method to send active alarm events to a customer developed, or external, HTTP[S] endpoint

Important

- Note: currently Workbench 9.x is only compatible with Genesys Engage On-Premise
- Note: future Workbench 9.x roadmap features are subject to change, timescales TBD.

Important

- Workbench High-Availability (HA) is resiliency of event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)

Important

- Workbench Agent 8.5 is ONLY for LFMT
- Workbench Agent 9.x is ONLY for Workbench 9.x
- If/when Workbench and LFMT is deployed, both Workbench Agents 8.5 and 9.x would be needed on each remote host
  - The Workbench Agent 8.5 would be required for LFMT to collect log files from the remote hosts (i.e. sip, urs, gvp etc)
  - The Workbench Agent 9.x would be required for Workbench ingestion of data from the remote hosts (i.e. sip, urs, gvp etc)

New in this 9.3.000.00 Release

Workbench 9.3.000.00 provides:

- A Notification Webhook feature that provides a simple and efficient method to send information to a customer developed, or external, HTTP[S] endpoint
  - further details here: Notification Channels and Workbench Alerts.
- An upgrade of the Elastic back-end stack from 7.1 to 7.17

Previous Workbench Releases

Release	Release Date	Description
9.2.000.20	Jan 2022	• Workbench log4j vulnerability mitigations/fixes - using log4j 2.17.1
9.2.000.10	Dec 2021	• Workbench log4j vulnerability mitigations/fixes - using log4j 2.17.0
9.2.000.00	Nov 2021	• Workbench introduces an Anomaly Detection (AD) “Insights” feature that autonomously and predictively raises Machine Learning Anomalies, via the dedicated "Insights" Console, based on the dynamic Anomaly Detection model of the ingested metric data received from Hosts/ Processes of the Genesys Application servers (i.e. sip, urs, gvp etc).
9.1.100.00	May 2021	• ZooKeeper Authentication - protect the Workbench back-end configuration data stored in ZooKeeper via a username and password.

Release	Release Date	Description
		• Elasticsearch Authentication - protect the Workbench back-end ingested data (Alarms, Changes, CM, Auditing etc) stored in Elasticsearch via a username and password.
9.1.000.00	Dec 2020	• Workbench 9.1.000.00 adds a Metric data ingestion feature that enables observability of host and process CPU, Memory, Disk and Network metric data, providing rich insights and analysis capability into host and process metric utilization, performance and trends. • Workbench 9.1.000.00 also provides a stepping-stone to Workbench 9.2 (Q3 2021) where Anomaly Detection Workbench “Insights” will be autonomously and predictively raised based on abnormal outlier analysis of the ingested metric data modelled baseline.
9.0.100.00	May 2020	Linux support
9.0.000.00	Feb 2020	The reinvention of Workbench 8.5, with the core Alarm, Changes and Channel Monitoring features migrated.
8.5.100.113	Sept 2017	Workbench 8.5 has been replaced with Workbench 9.x - please upgrade to the latest release

Intended Audience

This document is intended primarily for Genesys platform System Administrators, Contact Centre Managers and Operations Personnel.

> **Important**
>
> - You should be familiar with Genesys Engage On-Premise components, architecture and functions.

Contact Genesys Customer Care

If you have an issue or a question regarding Workbench or Remote Alarm Monitoring, you can submit a Support Case to Genesys Customer Care.

1. Login to **My Support** and select **Open a Case** from the left-side menu.
2. For Product Category, select **Genesys Care Tools**
3. For Product, select **Workbench** or **Remote Alarm Monitoring** if related to the Workbench RAM Service
4. For Major Release, select **9.1**
5. Describe the issue on the next screen.
6. Submit your case and a Customer Care tools specialist will contact you.

Before contacting Genesys Customer Care, please refer to the Genesys Care Program Guide for complete contact information and procedures.

> **Important**
>
> Note that the Elastic (https://www.elastic.co/) stack leveraged by Workbench 9.x is not supported and maintained by Genesys, as such customers and partners **may** need to engage with the Elastic community regarding technical issues that are not within the scope of Workbench support.

Workbench Checklist

Use this section as a proactive checklist for successful Workbench planning, deployment and usage.

Item #	Description
1	Read this document thoroughly and plan your Workbench deployment carefully before starting the Workbench installation.
2	Given Genesys Workbench integrates to Genesys Engage components, ensure you have Genesys Engage knowledge, experience and training before installing Workbench.
3	Review the Architecture section to determine what Workbench architecture best suits your environment - i.e: • Do you have multiple Engage Data-Centers? • Do you want to ingest host and application process Metric data (i.e. CPU/RAM/DISK/ NETWORK) from your Engage Hosts into Workbench? • Do you want Workbench HA? • Do you want the minimal Workbench footprint?
4	Review the Workbench Components section to gain an insight into the function of the Workbench components and their respective integration points.
5	Review the Planning section to understand considerations and determine mandatory items/ actions required prior to installing Workbench - i.e. • Genesys recommends Engage Configuration Server (CS), Solution Control Server (SCS), Message Server (MS) and SIP Server versions of 8.5+. • Procure the Host/Server hardware running the Supported Workbench Operating Systems • Workbench components require Administrator (Windows) / Sudoer (not the *root* user) permissions for installation • Ensure the Network Ports utilized by Workbench are from a firewall perspective open and are not already used by other applications • For Linux Pre-Install Steps, ensure the ulimit,

Item #	Description
	/etc/security/limits.conf, /etc/sysctl.conf and vm.max_map_count settings are reviewed and the neccessary actions taken • Review the Linux Network and Security section
6	As part of Planning, carefully review and determine your Workbench Sizing requirements - i.e: • review, determine and record how many Engage Hosts will be running the Workbench Agent Remote? • review, determine and record for how many days you wish to store the ingested data within Workbench?
7	Review Workbench FAQ's for common questions.
8	Review Workbench Best Practises for common guidance.
9	Once the Planning section is complete, proceed to Download Workbench
10	Now review and complete the Workbench Pre-Installation Steps - i.e: • Workbench Installation Package Import using GAX - this creates the necessary Engage CME Workbench Application Templates and Admin Role • Provisioning the Workbench IO (Server) Application using GAX - i.e. "WB9IO" • Provisioning the Workbench Client Application using GAX - i.e. "WB9Client" • Provisioning the Workbench Client Role using GAX - i.e. "WB9Admin" • Follow the Console ChangedBy field for Genesys Engage Changes instructions to ensure the Workbench Changes Console **ChangedBy** field is accurate (not "N/A")
11	Begin the Workbench installation, starting with the Workbench Primary Node - i.e: • Workbench Primary Node Windows Installation • Workbench Primary Node Linux Installation
12	If Workbench HA is required, begin the Workbench Additional Node(s) installation - i.e:

Item #	Description
	• Workbench Additional Node Windows Installation • Workbench Additional Node Linux Installation
13	At this stage, you now have a Workbench single-node or Workbench Cluster deployment up and running at a given Data-Center - i.e. "APAC".
14	Repeat the above steps **9** and **10** for each Data-Center - i.e. for Data-Centers "EMEA" and "LATAM".
15	Hypothetically you now have **3** sepearate Workbench deployments running at Data-Centers "APAC", "EMEA" and "LATAM".
16	If required, you can synchronize these separate Workbench deployments into a **Workbench Distributed** architecture for holistic visibility - i.e: • Workbench Data-Center Synchronization • Overview, Benefits and Limitations • Data-Center Synchronization - Planning • Data-Center Synchronization - Configuration
17	Hypothetically, you now have a Workbench distributed architecture comprising of Workbench instances/Clusters running at Data-Centers "APAC", "EMEA" and "LATAM".
18	Review this section for details on Using Workbench
19	Review the Workbench Agent Remote section for details on ingesting Engage Host and Application Metric data into Workbench via the Workbench Agent Remote component
20	Review this section for details on the Workbench Remote Alarm Monitoring (RAM) feature • Workbench Remote Alarm Monitoring (RAM) enables the customers on-premise Workbench instance to transition/transmit a specific subset of Genesys Engage Critical and Major Alarms, externally, to Genesys Customer Care, who will then proactively create a Genesys Case and will liaise, if required, with the customer to proactively progress and resolve the issue(s); the RAM alarms can also sent to the customers mobile device via the Genesys Care Mobile App.
21	Review Workbench Troubleshooting for guidance on Workbench issues.
22	Review Workbench Options for help on Workbench

Item #	Description
	configuration options/settings.
23	Review these Workbench Upgrade sections when migrating to a new release of Workbench - i.e: Warning • **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSear data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.** • Pre-Upgrade Steps - Windows • Primary Node Upgrade - Windows • Additional Node(s) Upgrade - Windows • Rollback - Windows • Remove old version - Windows • Pre-Upgrade Steps - Linux • Primary Node Upgrade - Linux • Additional Node(s) Upgrade - Linux • Rollback - Linux • Remove old version - Linux

Planning and Deployment - New Install

This Planning and Deployment section contains general information for the planning, deployment/ installation and configuration of Workbench for new installations.

Workbench Architecture

Example Workbench and Workbench Anomaly Detection (AD) architectures are detailed below:

- Workbench "stand-alone/single node" architecture with single Engage Data-Center
- Workbench "Cluster" HA architecture with single Engage Data-Center
- Workbench "Cluster" HA architecture with multi Engage Data-Center (no/limited Metric ingest)
- Workbench "stand-alone/single node" architecture with multi Engage Data-Center
- Workbench "Cluster" architecture with multi Engage Data-Center
- Workbench Anomaly Detection (**AD**) with a Workbench "Cluster" HA architecture within a single Engage Data-Center
- Workbench Anomaly Detection (**AD**) HA with a Workbench "Cluster" HA architecture within a multi Engage Data-Center

Workbench Deployment Architecture

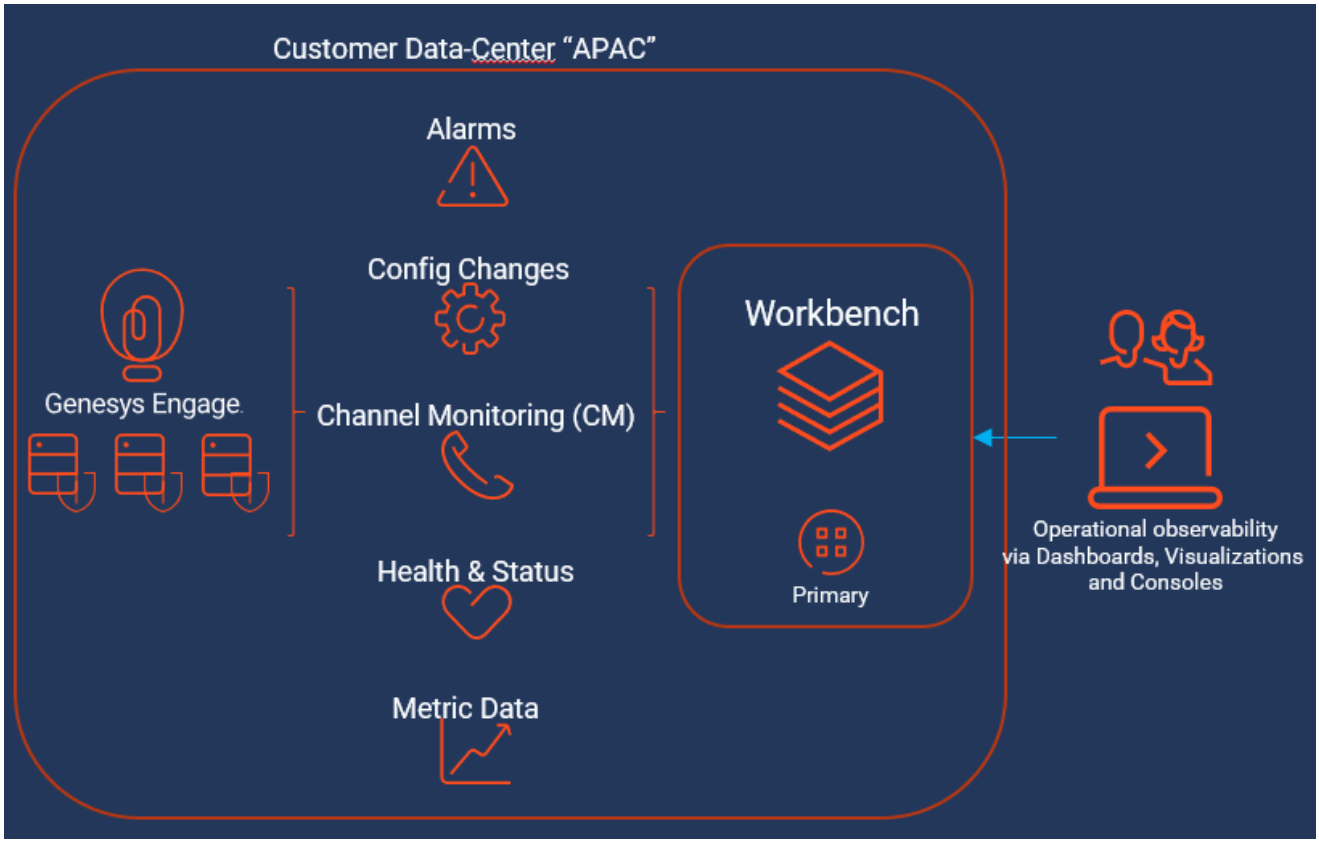
Workbench integrates to the Genesys Engage platform, as such the following Genesys Engage Objects will be required and leveraged by Workbench:

Component	Description/Comments
Genesys Engage **Workbench Client** application/ object	enables Engage CME configured Users to log into Workbench
Genesys Engage **Workbench IO** (Server) application/object	enables integration from Workbench to the Engage CS, SCS and MS
Genesys Engage **Configuration Server** application/object	enables integration from Workbench to the Engage CS; authentication and Config Changes
Genesys Engage **Solution Control Server** application/object	enables integration from Workbench to the Engage SCS; Alarms to WB from SCS
Genesys Engage **Message Server** application/ object	enables integration from Workbench to the Engage MS; Config change ChangedBy metadata
Genesys Engage **SIP Server** application/object (optional)	enables integration from Workbench to the Engage SIP Server enabling the Channel Monitoring feature

Workbench "stand-alone/single node" architecture with single Engage Data-Center

The example architecture below provides the following **WB single Primary node within a single Data-Center** approach:

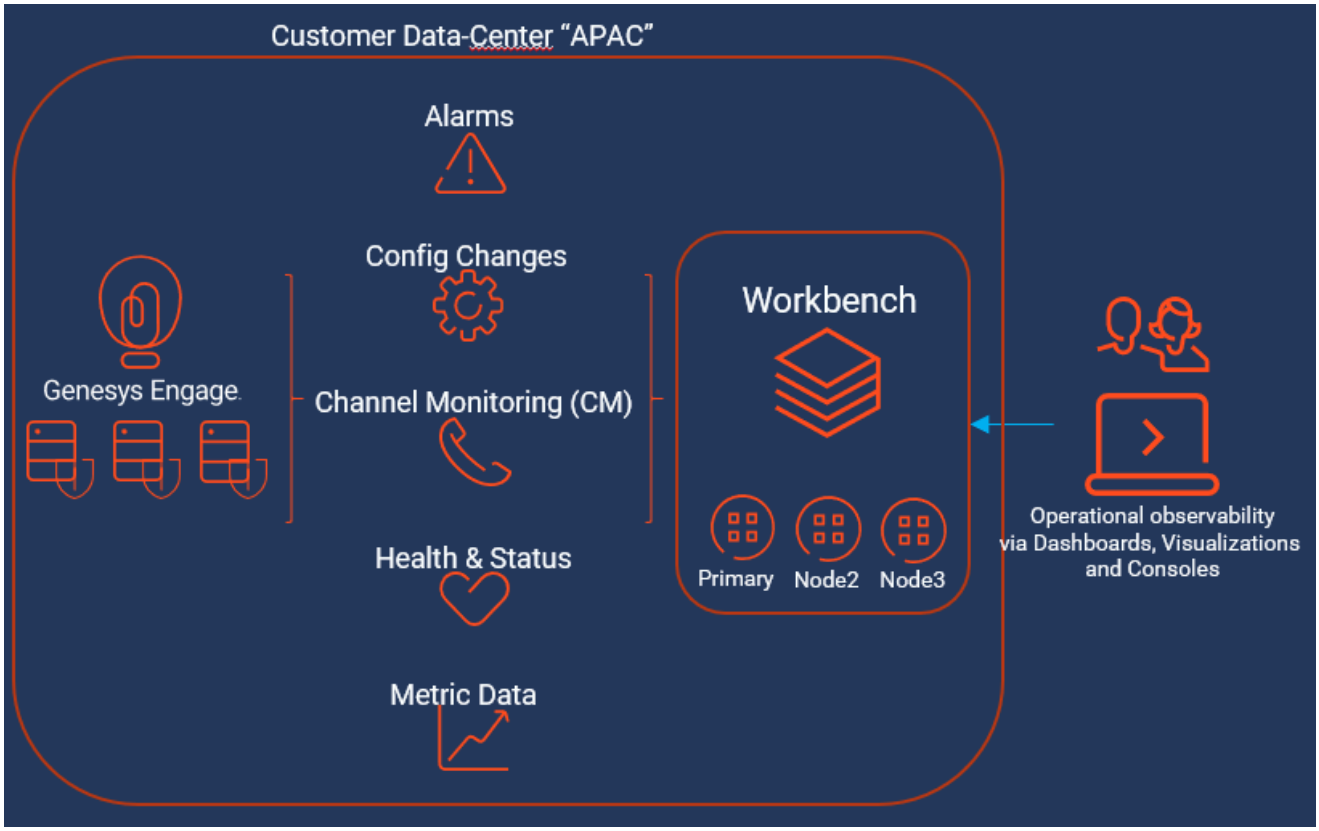
- A Genesys Engage **single** Data-Center/Site (i.e. APAC) deployment
- Workbench integrates into the Engage Master Configuration Server (CS)
- Workbench integrates into the Engage Solution Control Server (SCS) and associated Message Server (MS)
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server
- Workbench Users connect to the Workbench Primary (WB IO application) instance and can visualize the features of WB
- If the Workbench Agent component is installed on any Genesys Application servers (i.e. SIP, URS, FWK etc)
  - the Metric data from those hosts will be sent to the Workbench node for storage, providing visualizations via the Workbench Dashboard feature



Workbench "Cluster" HA architecture with single Engage Data-Center

The example architecture below provides the following **WB "Cluster" within a single Data-Center** approach:

- A Genesys Engage **single** Data-Center/Site (i.e. APAC) deployment
- Workbench Primary node integrates into the Engage Master Configuration Server (CS)
- Workbench Primary node integrates into the Engage Solution Control Server (SCS) and associated Message Server (MS)
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server
- Workbench Users connect into the Workbench Primary (WB IO application) instance and can visualize the features of WB
- For HA resiliency, Workbench Node 2 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)
- For HA resiliency, Workbench Node 3 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)



Important

- Workbench High-Availability (HA) is resiliency of event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)

Workbench "Cluster" HA architecture with multi Engage Data-Center (no/limited Metric ingest)

Warning

- This architecture has no\limited Engage Metric data ingestion by design.

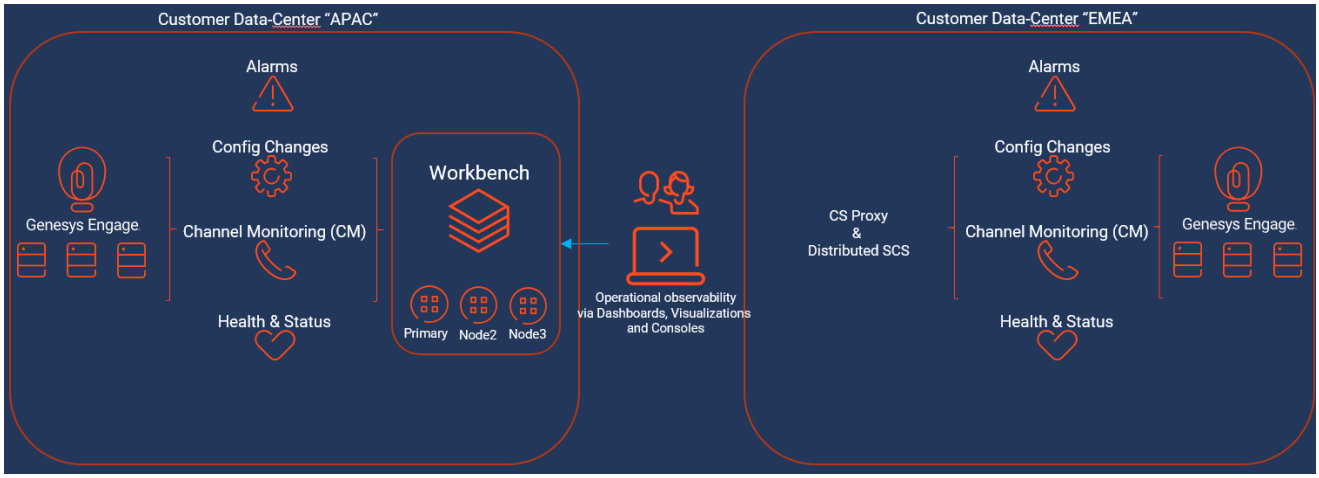
Important

- This architecture is best suited for customers who do NOT wish to ingest Metric data from their Genesys Application Servers (i.e. SIP, URS, FWK etc) but wish to leverage the other features of Workbench via a minimal HA footprint
- The footprint could be reduced further by only deploying a Workbench Primary node at the APAC Data-Center, thereby providing no HA, but offers a minimal Workbench footprint investment.

The example architecture below provides the following **WB Cluster within a multi Data-Center** and **no\limited Engage Metric data ingestion** approach:

- A Genesys Engage **multi** Data-Center/Site (i.e. APAC & EMEA) deployment
- A Workbench Primary, Node 2 and Node 3 Cluster - only installed at the APAC Data-Center
- The Workbench Primary at the APAC Data-Center integrates into the respective **local** Configuration Server
- The Workbench Primary at the APAC Data-center integrates into the respective **local** Solution Control Server and associated Message Server
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server
- EMEA Alarms and Changes events would be ingested into the APAC Workbench Cluster via Engage CS Proxy and Distributed SCS components

- Workbench Users at both APAC and EMEA would connect to the APAC Workbench Primary (WB IO application) instance and can visualize the features of WB
- Workbench Agents would only be installed on the APAC Data-Center, on the Workbench Hosts by default
  - Installing the Workbench Agent Remote component on the Genesys Application Servers in the APAC Data-Center is optional
- Workbench Agents would NOT be installed on the EMEA Data-Center - due to the network Metric event data that would transition over the WAN



Important

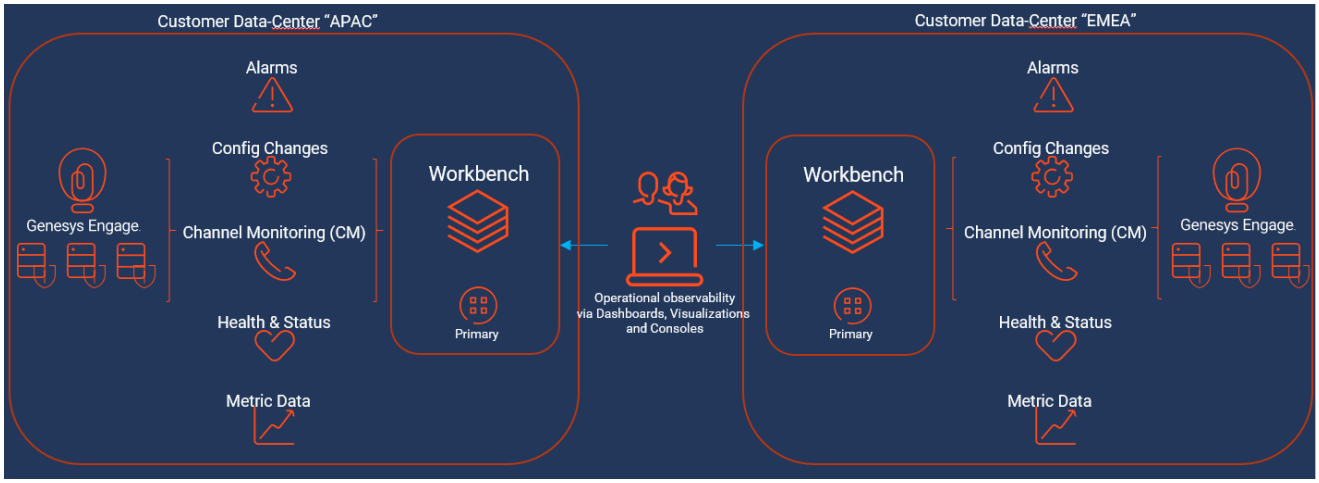
- Workbench High-Availability (HA) is resiliency of event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)

Workbench "stand-alone/single node" architecture with multi Engage Data-Center

The example architecture below provides the following **WB single Primary node within a multi Data-Center** approach:

- A Genesys Engage **multi** Data-Center/Site (i.e. APAC & EMEA) deployment
- Each Workbench Primary at each Data-Center integrates into the respective **local** Configuration Server
- Each Workbench Primary at each Data-center integrates into the respective **local** Solution Control Server and associated Message Server
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server

- Workbench Users would logically connect into their local Workbench Primary (WB IO application) instance and can visualize the features of WB
  - Workbench Users can connect into either their local or remote Data-Center Workbench instances; this provides redundancy
- If the Workbench Agent component is installed on any Genesys Application servers (i.e. SIP, URS, FWK etc)
  - the Metric data from those hosts will be sent to the **local** Workbench node/cluster for storage, providing visualizations via the Workbench Dashboard feature

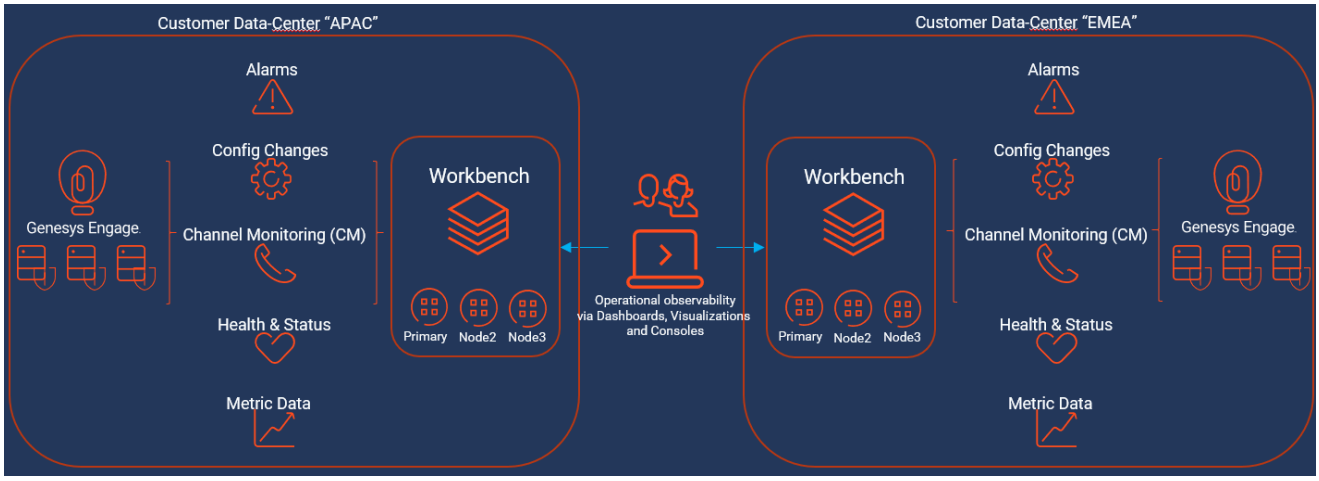


Workbench "Cluster" architecture with multi Engage Data-Center

The example architecture below provides the following **WB Cluster within a multi Data-Center** approach:

- A Genesys Engage **multi** Data-Center/Site (i.e. APAC & EMEA) deployment
- Each Workbench Primary at each Data-Center integrates into the respective **local** Configuration Server
- Each Workbench Primary at each Data-center integrates into the respective **local** Solution Control Server and associated Message Server
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server
- Workbench Users would logically connect into their local Workbench Primary (WB IO application) instance and can visualize the features of WB
  - Workbench Users can connect into either their local or remote Data-Center Workbench instances; this provides redundancy
- If the Workbench Agent component is installed on any Genesys Application servers (i.e. SIP, URS, FWK etc)
  - the Metric data from those hosts will be sent to the **local** Workbench node/cluster for storage, providing visualizations via the Workbench Dashboard feature

- For resiliency, Workbench Node 2 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)
- For resiliency, Workbench Node 3 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)



Important

- Workbench High-Availability (HA) is resiliency of event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)

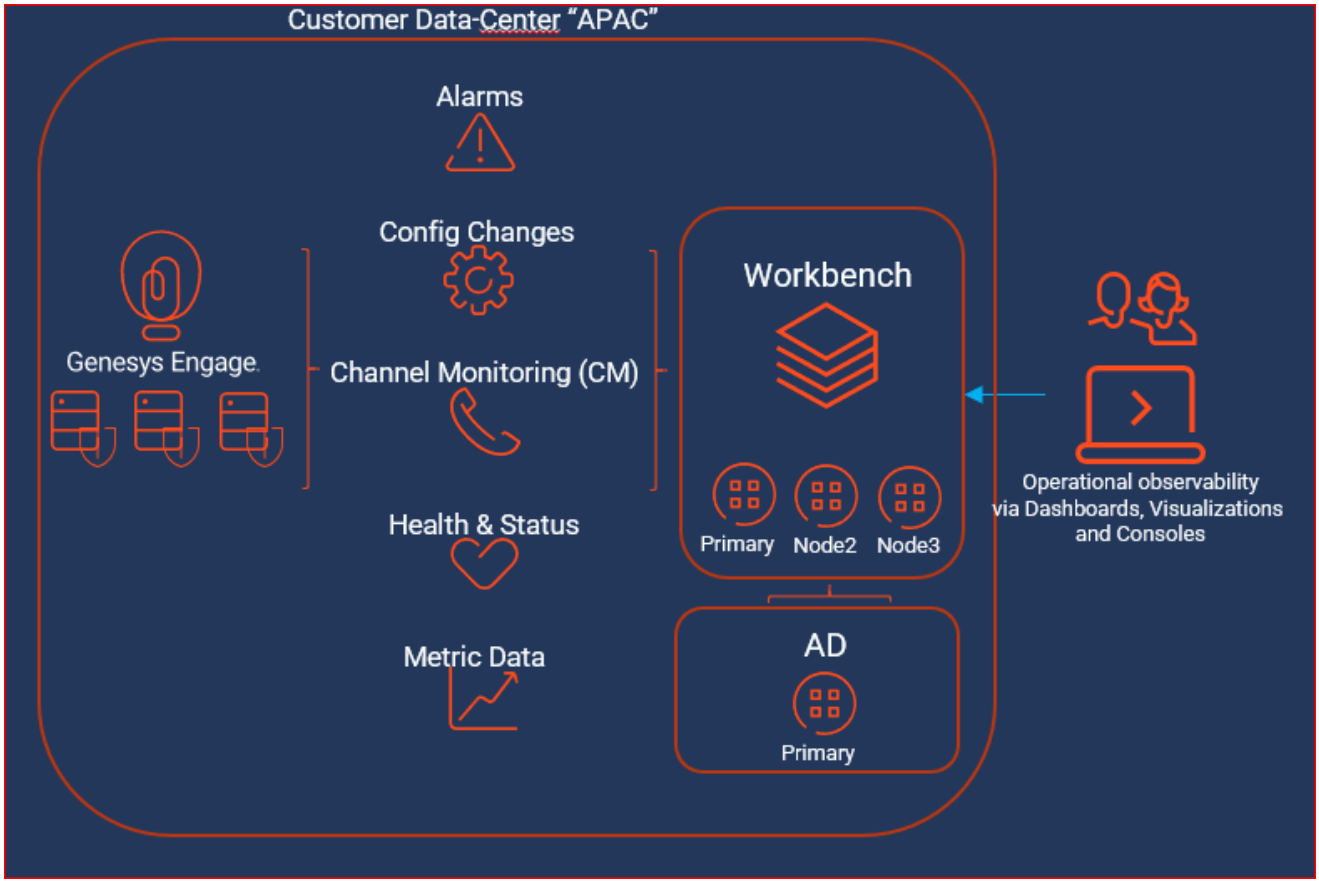
Workbench Anomaly Detection (**AD**) with a Workbench "Cluster" HA architecture within a single Engage Data-Center

The example architecture below provides the following **WB Anomaly Detection (AD) with a WB "Cluster" within a single Data-Center** approach:

- A Genesys Engage **single** Data-Center/Site (i.e. APAC) deployment
- Workbench Primary node integrates into the Engage Master Configuration Server (CS)
- Workbench Primary node integrates into the Engage Solution Control Server (SCS) and associated Message Server (MS)
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the respective Engage SIP Server
- Workbench Users connect into the Workbench Primary (WB IO application) instance and can visualize the features of WB
- For HA resiliency, Workbench Node 2 contains event data (via Workbench Elasticsearch) and

configuration data (via Workbench ZooKeeper)

- For HA resiliency, Workbench Node 3 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)
- Workbench Anomaly Detection (AD) Primary Node



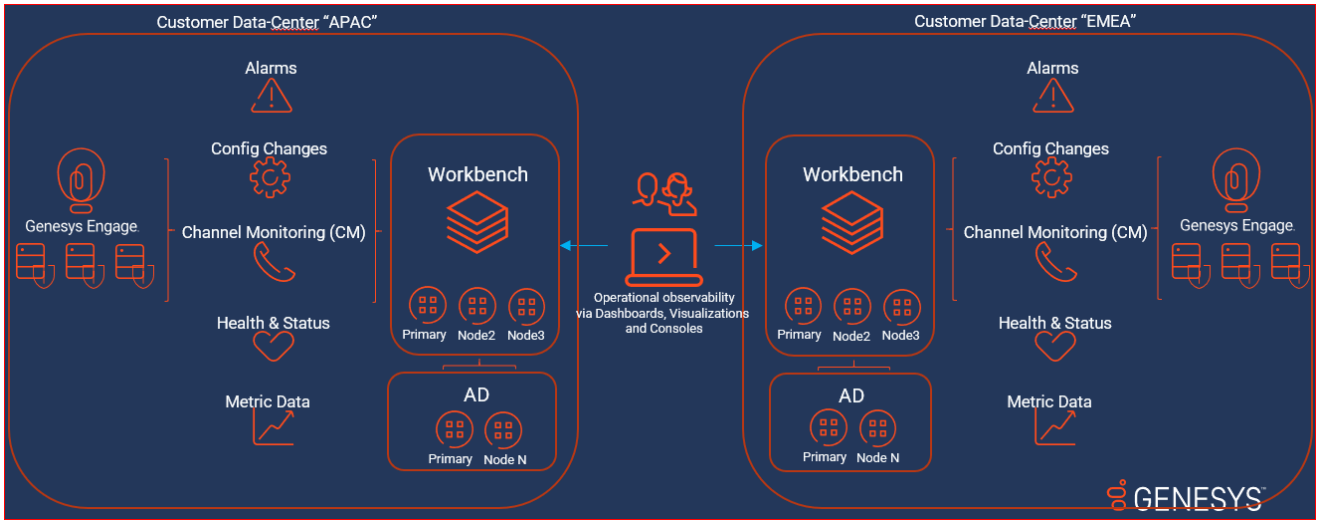
Workbench Anomaly Detection (**AD**) HA with a Workbench "Cluster" HA architecture within a multi Engage Data-Center

The example architecture below provides the following **WB Anomaly Detection (AD) HA with a WB "Cluster" within a multi Data-Center** approach:

- A Genesys Engage **multi** Data-Center/Site (i.e. APAC & EMEA) deployment
- Each Workbench Primary at each Data-Center integrates into the respective **local** Configuration Server
- Each Workbench Primary at each Data-center integrates into the respective **local** Solution Control Server and associated Message Server
- The Workbench Channel Monitoring feature functions via the WB IO application integrating to the

respective Engage SIP Server

- Workbench Users would logically connect into their local Workbench Primary (WB IO application) instance and can visualize the features of WB
  - Workbench Users can connect into either their local or remote Data-Center Workbench instances; this provides redundancy
- If the Workbench Agent component is installed on any Genesys Application servers (i.e. SIP, URS, FWK etc)
  - the Metric data from those hosts will be sent to the **local** Workbench node/cluster for storage, providing visualizations via the Workbench Dashboard feature
- For resiliency, Workbench Node 2 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)
- For resiliency, Workbench Node 3 contains event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)
- Workbench Anomaly Detection (AD) Primary Node and Node 2 - therefore the AD feature is running in HA mode



Workbench Data-Centers

A Workbench (WB) Data-Center (DC), is a logical concept, containing Workbench components that are typically deployed within the same physical location, typically within the same "Data-Center" or "Site".

For example, a WB **distributed** solution, could consist of a 3 x Data-Center deployment, Data-Centers **"APAC"**, **"EMEA"** and **"LATAM"**.

Each WB Data-Center will be running Workbench components, such as:

- Workbench IO

- Workbench Agent
- Workbench Elasticsearch
- Workbench Kibana
- Workbench Logstash
- Workbench ZooKeeper

When installing Workbench, the user has to provide a Data-Center name, post install, the respective Workbench components will be assigned to the Data-Center provided.

Workbench Data-Centers provide:

- logical separation of Workbench components based on physical location
- logical and optimised data ingestion architecture
  - i.e. APAC Metric data from the SIP, URS and GVP Servers will be ingested into the APAC Workbench instance/Cluster
- an hoslitic view of multiple Workbench deployments at different Data-Centers, all synchronised to form a Workbench **distributed** architecture
  - i.e. A user can log into the APAC Workbench instance and visualise Alarms, Changes and Channel Monitoring events/data from not only the local APAC WB instance/Cluster, but also the other **"EMEA"** and **"LATAM"** Data-Centers Workbench instances

> **Important**
>
> - A Workbench host object **cannot** be assigned to a different Data-Center
> - A Genesys Engage host (i.e. SIP, URS, FWK etc) object can be re-assigned to a different Data-Center

Future Workbench 9.x Architectures/Footprints

> **Important**
>
> - Workbench 9.x future architectures/footprints may change when future roadmap features are released; Workbench 9.x roadmap features are subject to change, timescales TBD.

Workbench Agent and Workbench Agent Remote

Important

- Workbench Agent 8.5 is ONLY for LFMT
- Workbench Agent 9.x is ONLY for Workbench 9.x Hosts
- If/when Workbench and LFMT is deployed, both Workbench Agents 8.5 and 9.x would be needed on each remote host
  - The Workbench Agent 8.5 would be required for LFMT to collect log files from the remote hosts (i.e. sip, urs, gvp etc)
  - The Workbench Agent 9.x would be required for Workbench ingestion of data from the remote hosts (i.e. sip, urs, gvp etc)
- Workbench Agent Remote (WAR) 9.x is ONLY deployed on remote Genesys Hosts such as SIP, URS, GVP etc - this components sends Metric data to the Workbench 9.x Server/ Cluster

Workbench Version Alignment

Important

- Workbench Versions on ALL Nodes and at ALL Data-Centers should be running the same release - i.e. do NOT mix 9.0.000.00 with 9.1.000.00.

Workbench Components

Genesys Care Workbench 9.3 comprises of the following components:

- **Workbench IO:**

This component ingests data from multiple data sources such as Genesys Engage Configuration Server (CS), Genesys Engage Solution Control Server (SCS), Genesys Engage Message Server (MS) enabling the user to visualise health, status (via Dashboards, Visualizations, Health-Maps, Alarms/ Changes Consoles) and troubleshoot their Genesys platform.

- **Workbench Agent (WB Hosts):**

This component is installed on each and every *Workbench* host where Workbench components are installed. The WBAgent in 9.0 is used for deployment, configuration, status and control of the Workbench components.

- **Workbench Agent Remote (non WB Hosts):**

This component is installed on each Engage (i.e. non Workbench host) where you wish to send metric events to the Workbench node/Cluster; this then enables observability of host and process CPU, Memory, Disk and Network metric data, providing rich insights and analysis capability into host and process metric utilization, performance and trends.

- **Workbench Kibana:**

This component is the Workbench Client, providing the Workbench UI where users can leverage dedicated Alarms, Changes, Audit and Discover Consoles, Channel Monitoring Call Flows, Dashboards and Visualizations, Health-Maps etc to monitor and troubleshoot their Genesys Engage platform.

- **Workbench Elasticsearch:**

This component is the data event storage feature of Workbench providing a full-text search engine. Alarm, Configuration Change, Channel Monitoring event, Auditing event and Metric event data are all stored within Workbench Elasticsearch.

- **Workbench Logstash:**

This component is a server side ETL data processing pipeline that enables data collection (from a variety of sources i.e. Workbench Agent, Workbench Heartbeat and Workbench Elasticsearch), data transformation and subsequent destination storage (i.e. Workbench Elasticsearch).

- **Workbench Heartbeat:**

This component is used for Workbench component health and status monitoring

- **Workbench Metricbeat:**

This component is used for Metric (i.e. Cpu, Memory, Disk, Network) data collection from Workbench

and Genesys Application Servers (i.e. SIP, URS, GVP etc).

- **Workbench ZooKeeper**:

This component provides and stores Workbench configuration data such as Hosts, Applications, Channel Monitoring configuration, User Preferences etc.

Workbench Agent and Workbench Agent Remote

Important

- Workbench Agent 8.5 is ONLY for LFMT
- Workbench Agent 9.x is ONLY for Workbench 9.x Hosts
- If/when Workbench and LFMT is deployed, both Workbench Agents 8.5 and 9.x would be needed on each remote host
  - The Workbench Agent 8.5 would be required for LFMT to collect log files from the remote hosts (i.e. sip, urs, gvp etc)
  - The Workbench Agent 9.x would be required for Workbench ingestion of data from the remote hosts (i.e. sip, urs, gvp etc)
- Workbench Agent Remote (WAR) 9.x is ONLY deployed on remote Genesys Hosts such as SIP, URS, GVP etc - this components sends Metric data to the Workbench 9.x Server/ Cluster

Elastic Stack

Details of the Elastic stack components that are leveraged by Workbench 9.x can be found here: https://www.elastic.co/

Planning

This chapter provides details on Planning of Genesys Workbench:

- Prerequisites
- Network and Security Considerations
- Sizing
- Downloading Workbench

Prerequisites

Workbench Host/Server Operating System Requirements

Workbench components are supported on hosts with the following Operating Systems:

Platform	Version
Microsoft Windows Server	2012
Microsoft Windows Server	2016
Red Hat Enterprise Linux (RHEL)	7
CentOS	7

Workbench 9.x comprises several components; a network Admin-level account is required that has "Full Control" permissions for all Workbench application related folders.

Warning

- The Workbench Primary and Additional (i.e. Node2 and Node3) hosts/nodes (across ALL Data-Centers) should all be running the same Operating System.
- Workbench uses the Hostname for component configuration
- Please ensure DNS hostname resolution between the Workbench Hosts and the Engage Hosts is accurate and robust
- If the Workbench Hosts have multiple NIC's, please ensure the Hostname resolves to the desired IP Address **prior** to Workbench installation
- Workbench **9.x is limited to a maximum of 100 Hosts** (the global combined Workbench or Engage Hosts), due to delays in loading the Configuration Host and Application objects/details; this limitation will be addressed in the next release of Workbench.
- Genesys support for the OS versions above ends when the respective vendors declare EOL/EOS

Supported Browser

Browser	Version
Google Chrome	latest version is recommended

Genesys Workbench 9 to Engage Integration

Genesys recommends Engage Configuration Server, Solution Control Server, Message Server and SIP Server versions of 8.5+.

Warning

- If your Engage Configuration Servers are configured for HA, please ensure the respective CME Host Objects have the IP Address field configured, else Workbench will fail to install.
- Ensure each and every Engage CME Application has an assigned Template else the Workbench installation will fail.
- Genesys support for the platform versions mentioned on this page ends when the respective vendors declare End of Support.

Warning

- Currently Workbench Agent 9.x uses Port 5067 - this unfortunately clashes with GVP - if your Genesys deployment contains GVP please change the Workbench Agent(s) Port (i.e. to 5068) and restart the Workbench Agent(s) and Workbench Logstash(s) components.
  - This oversight will be addressed in a future Workbench 9.x release

Java Requirements

Workbench 9.x ships/installs with a pre-bundled OpenJDK 11 package, therefore the historical JRE is not mandatory.

Note:

- the Workbench Agent that gets installed on the Workbench Nodes/Hosts utilizes the pre-bundled OpenJDK 11 package
- the Workbench Agent (Remote, WAR) that's installed on “remote” Nodes/Hosts (i.e. SIP, URS, FWK etc) is Go based and therefore does not rely on either OpenJDK or the historical JRE packages

Warning

- If the JAVA_OPTS settings are changed, ensure the **xms** and **xmx** values are different; if the values are the same issues will be encountered when starting Logstash

Network Ports - Workbench Hosts

Workbench components use the network ports below, from a firewall perspective, please review, edit and ensure not already in use.

Warning

- Double-check, these network ports below, that are used by Workbench, are from a firewall perspective, **open and not already in use** by other applications

Workbench Host Ports (i.e. the Primary, Node 2, Node 3, Node N etc hosts)

Port	Component	Comments
8182, **2552**	Workbench IO	• Mandatory to open in firewall for Workbench Users connecting to the Workbench UI • ports 8182 & 2552 can be changed (select custom install to change from these defaults) at install time • ports 8182 & 2552 ports cannot be changed via the WB UI post install
8181	Kibana	• Mandatory to open in firewall for Workbench Users connecting to the Workbench UI • port 8181 can be changed (select custom install to

Port	Component	Comments
		change from these defaults) at install time • port 8181 can be changed via the WB UI post install
9091, **5067**	Workbench Agent & Metricbeat	• only publicly open in the firewall on the Workbench host if/when using a Workbench Cluster • ports 9091 & 5067 can be changed (select custom install to change from these defaults) at install time • ports 9091 & 5067 can be changed via the WB UI post install
9200, 9300	Elasticsearch	• only publicly open in the firewall on the Workbench host if/when using a Workbench Elasticsearch Cluster • port 9200 can be changed via the WB UI post install • port 9300 cannot be changed via the UI post install

9600	Logstash	• only publicly open in the firewall on the Workbench host if/when using:
		  • Workbench Cluster
		  • Workbench Agent Remote components installed on Engage hosts
		• port 9600 can be changed via the WB UI post install

5047	Logstash Status Pipeline (all ports can be changed via the WB UI)	• only publicly open in the firewall on the Workbench host if/when using:
		  • Workbench Cluster
		  • Workbench Agent Remote

Port	Component	Comments
		components installed on Engage hosts • port 5047 can be changed (select custom install to change from these defaults) at install time • port 5047 can be changed via the WB UI post install

5048	Logstash Metrics Pipeline (all ports can be changed via the WB UI)	• only publicly open in the firewall on the Workbench host if/when using:
		  • Workbench Cluster
		  • Workbench Agent Remote components installed on Engage hosts
		• port 5048 can be changed (select custom install to change from these defaults) at install time
		• port 5048 can be changed via the WB UI post install

5077	Heartbeat HTTP Port (all ports can be changed via the WB UI)	• only publicly open in the firewall on the Workbench host if/when using:
		  • Workbench Cluster (all ports can be changed via the WB UI)
		  • Workbench Agent Remote components installed on the Engage hosts
		• port 5077 can be changed (select custom install to change from these defaults) at install time
		• port 5077 can be changed via the WB UI post install

2181, 2888, 3888	ZooKeeper	• only publicly open in the firewall on the Workbench host if/when using Workbench ZooKeeper Cluster

Port	Component	Comments
		• ports 2181, 2888 and 3888 can be changed via the WB UI post install

Network Ports - Non-Workbench Hosts (i.e. SIP, URS, FWK etc hosts)

Port(s)	Component
9091, **5067**	Workbench Agent & Metricbeat on the remote Engage (i.e. SIP, URS, FWK etc Hosts)

- Workbench Agent/Metricbeat installed on the Genesys Application Servers will send metric data to the local WB Data-Center instance/Cluster

Important

- The ports above can be edited via the Workbench Configuration Console - and selecting/ editing the respective Workbench application object

Warning

- Ensure the Ports are reviewed, edited, opened and not in use prior to starting the Workbench installation

Hardware Sizing Requirements

Please review the **Sizing** section for Workbench hardware requirements.

Linux Pre-installation Steps

For Linux based installations, some Operational System settings are required to enable support of Elastic Search, a key components of Workbench 9.

1. Run the command **ulimit -a**. This should print something like the following:

```
bash-4.2$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 31152
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 8192
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 4096
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

2. Make the following changes:

- Run the command **sudo vi /etc/security/limits.conf**
- Add the following lines to the bottom. <username> is the current username.
  - <username> - nofile 131070
  - <username> - nproc 8192
  - <username> - memlock unlimited
- Logout and log back in.
- Run the command **sudo sysctl -w vm.max_map_count=262144**
- Run the command **sudo vi /etc/sysctl.conf** and add the line **vm.max_map_count=262144** to the bottom.

3. Exit the current terminal window and open a new one.

4. Run the command **ulimit -a**. This should print something like the following:

```
bash-4.2$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 31152
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 131070
pipe size            (512 bytes, -p) 8
```

```
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 8192
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

5. Ensure the values **max user processes=8192** and **open files=131070** from Step 4.

RHEL 7.x - specific steps

The following change is needed only for machines running Red Hat Enterprise Linux Server release 7.x.

For the Workbench services to start correctly after a machine reboot, it is necessary to run the following commands:

1. sudo visudo (enter the sudo password when prompted)
2. Locate the line “Defaults requiretty” in the opened file
3. Comment it out by placing a “#” at the beginning to make it read “#Defaults requiretty”
4. :wq<Enter> to save the changes and exit.

Alternatively, upon reboot of the machine, these services can be manually started in the following sequence:

service WB_Elasticsearch_9.1.000.00 start

service WB_ZooKeeper_9.1.000.00 start

service WB_Kibana_9.1.000.00 start

service WB_Agent_9.1.000.00 start

service WB_IO_9.1.000.00 start

Sizing

Warning

- It's imperative you review, plan and define the details below before installing Workbench; failure to do so could result in a Workbench re-installation
- Review and complete each sub-section below before moving onto the next

Warning

- Consider that if/when upgrading Workbench, the Workbench Host(s) "free" disk space requires at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.

- Workbench can be deployed as a single-node/host or as a multi-node/host cluster.
- The Workbench multi-node cluster deployment is available to support high-availability and/or environments that have a high volume of events/metrics.
- Multiple Data-Centers are supported, where Workbench can be deployed as single-node/host or as a cluster per Data-Center.
- Workbench deployments across Data-Centers can then be connected and synced in real-time to provide holistic visibility of the Alarms, Changes, Channel Monitoring and Auditing features.
- To determine the number of Workbench nodes/hosts, and the resource requirements for each, please follow the steps below.

Warning

The Workbench 9.x Sizing steps below should be followed for each Data-Center where Workbench will be deployed.

1. Calculate Workbench Node/Host Disk Space

Based on the number of Hosts (i.e. Engage SIP, URS, FWK etc) that Workbench will ingest Metric data

from, review the table below to determine the respective disk space required for each Workbench Host at a given Data-Center:

Number of Hosts • **to ingest Metric data from**	**Total Disk Space** • **assuming a 30 day Workbench data Retention Period, a 60 second Metric collection frequency, and a 80% high-water mark for ElasticSearch**
1-50	300 GB
51-100	600 GB
101-150	900 GB
150+	1.2 TB [+300 GB for every 50 hosts > 200]

Note the Total Disk Space = _____ (used for next steps)

> ### Warning
>
> - Currently Workbench **9.x is limited to a maximum of 100 Hosts** (the global combined Workbench or Engage Hosts), the table above details beyond the 100 Host limit for future Workbench sizing context.

2. Only if/when the default Retention Period and Metric Frequency settings are changed

The table in section 1 above, assumes the Workbench default data Retention Period of **30 days** and a Workbench Agent/Remote Metric collection frequency of every **60 seconds**.

If these default Retention Period and Metric Frequency values require modification, please re-calculate the **Total Disk Space**, by using the scale factors below:

- Retention Scale Factor = [New Retention Period Days] / 30
- Metric Frequency Scale Factor = 60 / [New Collection Frequency Seconds]
- Re-calculated **Total Disk Space** = Disk Space (from the section 1 table above) * Retention Scale Factor * Metric Frequency Scale Factor

Important

- The global Workbench Retention Period is editable via Workbench Configuration\General\ Retention Period\Workbench Data Retention Period (Days)
- The Metric Frequency collection setting can be changed on each Workbench Agent and Workbench Agent Remote application via:
  - Workbench Configuration\Applications\Application Name (i.e. WB_Agent_Primary)\MetricBeat Host Metrics\Host Metric Collection Frequency (seconds)
  - Workbench Configuration\Applications\Application Name (i.e. WB_Agent_Primary)\MetricBeat Associated Application Metrics\Application/Process Metric Collection Frequency (seconds)

3. Determine the Workbench Node/Host Count

Using the **Total Disk Space** calculation from the previous step, next determine the required number of Workbench Nodes/Hosts:

Total Disk Space from Step 1 or 2 above	Number of Workbench Nodes/Hosts Required
is **less than 2.5 TB**	A single (1) Node/Host Workbench can be used
is **greater than 2.5 TB** OR if **Workbench High Availability** is required	A 3 x Nodes/Hosts Workbench Cluster is required

Important

- Workbench High-Availability (HA) is resiliency of event data (via Workbench Elasticsearch) and configuration data (via Workbench ZooKeeper)

4. Workbench Node/Host Resources

This section details the per Workbench Node/Host recommended resources based on the previous steps:

Type	Specification

Workbench Primary Node/Host
• be it single Node or part of a 3 Node Cluster
	• CPU: 10 Cores/Threads
	• Memory: 24 GB
	• NIC: 100 MB
	• Disk:
	  • if a single Workbench Node/Host = **Total Disk Space** from Step 1 or 2 above
	  • if part of a Workbench 3 Node Cluster = divide the **Total Disk Space** from Step 1 or 2 above by **3**
	  • The Total Disk Space is divided by 3 due to the Workbench Cluster deployment architecture

Non Workbench Primary Nodes/Hosts • that are part of a Workbench Cluster	• CPU: 10 Cores/Threads • Memory: 16 GB • NIC: 100 MB • Disk: Total Disk Space from Step 1 or 2 above / 3 • The Total Disk Space is divided by 3 due to the Cluster deployment architecture

Important

- The following Memory allocation is need for each Workbench Elasticsearch Node/Host in the deployment.
- Please review ES Heap Settings for details on configuring the RAM for each Workbench Elasticsearch instance.

Total Disk Space per Node/Host	Dedicated Workbench Elasticsearch Memory Required
< 100 GB	2 GB RAM
100 - 750 GB	4 GB RAM
750 - 1.5 TB	6 GB RAM
1.5 - 2.5 TB	8 GB RAM

> **Important**
>
> - If/when **Total Disk Space** is greater than 2.5 TB per Node/Host, please raise a Genesys Customer Care Case for consultation/guidance.

Required Number of additional Node(s)/Host(s) at each Workbench Data-Center

Workbench currently supports ingesting Metric data from a maximum of 100 Hosts.

Required Number of WB additional Nodes/Hosts	Number of Hosts sending Metric data to Workbench	Frequency of Metrics being sent from each Host to Workbench
0 (WB on Primary host)	100	60 (default)
1 (WB on Primary host and Logstash on the additional node)	100	30
1 (WB on Primary host and Logstash on the additional node)	100	10

Example 1 - Ingest from 10 Engage Hosts - 30 day Retention Period - 60 second Metric Frequency

A production Workbench deployment ingesting Metric data from 10 Engage Hosts:

- Number of Hosts to ingest Metric data from = 10
- Retention Period = 30 days (default)
- Metric Frequency Collection = 60 seconds (default)
- Total Disk Space = 300 GB

- 1 x Workbench Node/Host
  - CPU: 10 Cores
  - RAM: 24 GB

- NIC: 100 MB
- DISK: 300 GB
- DEDICATED Elasticsearch RAM: 4 GB

Example 2 - Ingest from 30 Engage Hosts - 7 day Retention Period - 10 second Metric Frequency

A production Workbench deployment ingesting Metric data from 30 Engage Hosts:

- Number of Hosts to ingest Metric data from = 30
- Retention Period = 7 days
  - therefore re-calculated **Retention Scale Factor** is 7 (days) / 30 => **0.23**
- Metric Frequency Collection = 10 seconds
  - therefore re-calculated **Metric Frequency Scale Factor** is 60 / 10 => **6**
- Re-calculated Total Disk Space is 300 GB * 0.23 * 6 => **414 GB**

- 1 x Workbench Node/Host
  - CPU: 10 Cores
  - RAM: 24 GB
  - NIC: 100 MB
  - DISK: 414 GB
  - DEDICATED Elasticsearch RAM: 4 GB

Example 3 - Ingest from 90 Engage Hosts - 90 day Retention Period - 30 second Metric Frequency

A production Workbench HA deployment ingesting Metric data from 90 Engage Hosts:

- Number of Hosts to ingest Metric data from = 90
- Retention Period = 90 days
  - therefore re-calculated **Retention Scale Factor** is 90 (days) / 30 => **3**
- Metric Frequency Collection = 30 seconds

    - therefore re-calculated **Metric Frequency Scale Factor** is 60 / 30 => **2**
- Re-calculated Total Disk Space is 600 GB * 3 * 2 => **3600 GB (~3.5 TB)**

- 3 x Workbench Nodes/Hosts required given Total Disk Space is greater than 2.5 TB
- Workbench Primary
    - CPU: 10 Cores
    - RAM: 24 GB
    - NIC: 100 MB
    - DISK: 1200 GB (1.2 TB on each Node/Host given the Cluster architecture)
    - DEDICATED Elasticsearch RAM: 8 GB
- Workbench Nodes 2 and 3
    - CPU: 10 Cores
    - RAM: 16 GB
    - NIC: 100 MB
    - DISK: 1200 GB (1.2 TB on each Node/Host given the Cluster architecture)
    - DEDICATED Elasticsearch RAM: 8 GB

Network and Security Considerations

Security Considerations

Login Authentication Requirement

- Workbench uses Genesys Configuration Server authentication.
- To login to Workbench, each user needs a valid Configuration Server User Name and Password with Read and Execute permissions to use the Workbench Client (i.e. "WB9_Client") application.

Network Considerations

Data ingested by Workbench (including Alarm, Changes, Channel Monitoring and Metric events) from the Genesys Engage platform is stored locally in the customer environment; the customer is responsible for protecting this data.

Outbound Network Connectivity Requirements (Remote Alarm Monitoring (RAM) Subscribers)

In some customer environments, outbound network connectivity is restricted. If you subscribe to the Remote Alarm Monitoring (RAM) service from Genesys Care, you will need to enable minimal connectivity for Workbench to send alarms from the Remote Alarm Monitoring service to Genesys for processing. This processing includes routing alarms to Genesys support analysts and displaying alarm notifications in the Genesys Care Mobile App.

The outbound connectivity should allow connectivity from the Workbench host/server to "alarm.genesys.com" (208.79.170.12) on port 443; you may need to engage your networking or security team to enable this connectivity.

> **Important**
>
> - This Remote Alarm Monitoring connectivity requirement only applies if you are using the Remote Alarm Monitoring Service with Workbench.

Downloading Workbench

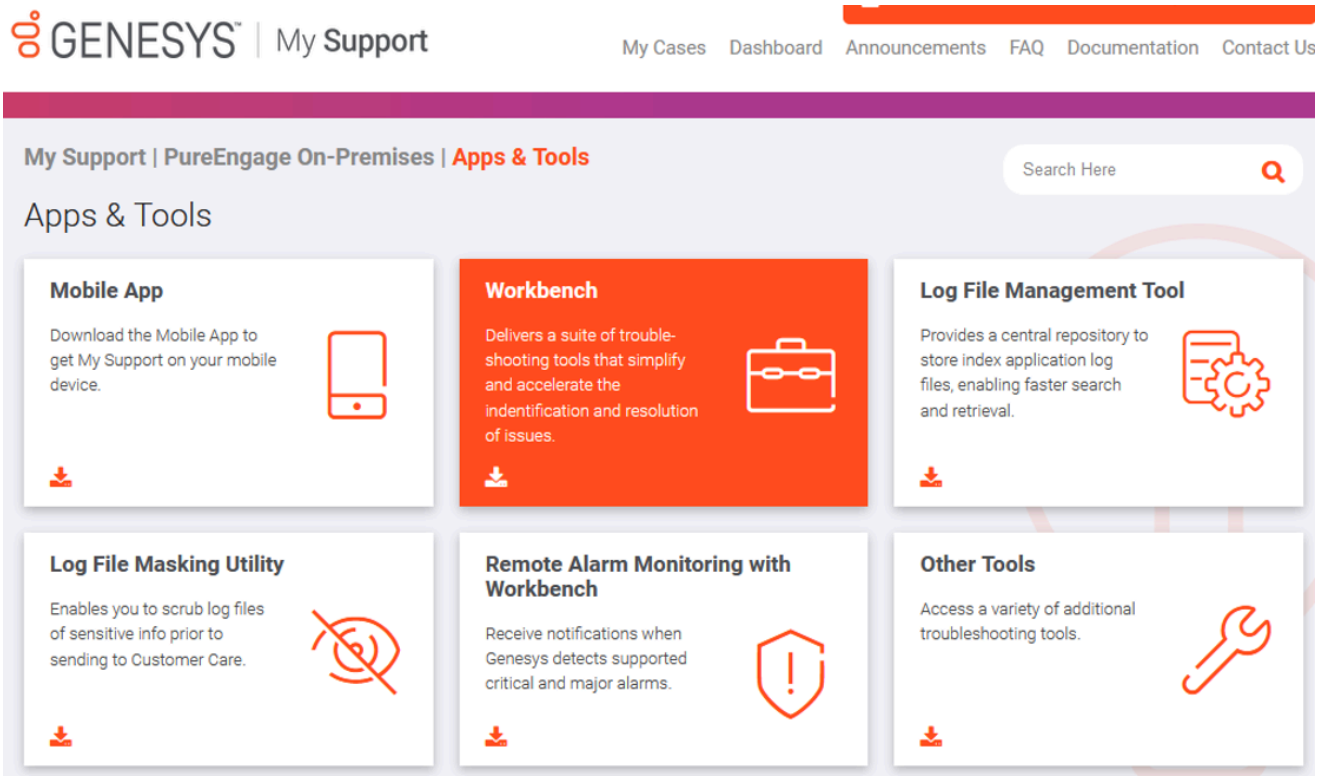
Follow these steps to download Workbench:

1. Login to My Support.
2. Click **Continue to your Dashboard** button.
3. On the *Dashboard* screen, select the **Apps and Tools** tile.
4. On the *Apps and Tools* screen, select the **Workbench** tile.
5. On the *Genesys Care Workbench* screen, click **Download Workbench** link.
6. On the *Terms and Conditions* screen, click the checkbox to accept the Terms and Conditions, and click **Download**.
7. On the *zip* screen, click **Download** again.

The result of the above is, depending on the target Workbench host(s) Operating System, a locally downloaded:

- **Workbench_9.x.xxx.xx_WINDOWS.zip** file
- **Workbench_9.x.xxx.xx_LINUX.tar.gz** file

Please now review the **Planning** and **Prerequisites** sections of this document before continuing to the Deployment sections.


GENESYS | My Support
My Cases
Dashboard
Announcements
FAQ
Documentation
Contact Us
My Support | PureEngage On-Premises | Apps & Tools
Search Here
Apps & Tools
Mobile App
Download the Mobile App to get My Support on your mobile device.
Workbench
Delivers a suite of trouble-shooting tools that simplify and accelerate the indentification and resolution of issues.
Log File Management Tool
Provides a central repository to store index application log files, enabling faster search and retrieval.
Log File Masking Utility
Enables you to scrub log files of sensitive info prior to sending to Customer Care.
Remote Alarm Monitoring with Workbench
Receive notifications when Genesys detects supported critical and major alarms.
Other Tools
Access a variety of additional troubleshooting tools.

Deployment

This chapter provides details on the deployment of Genesys Workbench.

It contains the following sections:

- Pre-Installation Steps
- Workbench Installation - Windows
- Workbench Installation - Linux
- Workbench Agent on Remote Hosts Installation
- Post Installation Configuration
- Uninstalling Workbench

Pre - Installation Steps

Genesys Engage Application Object Requirements

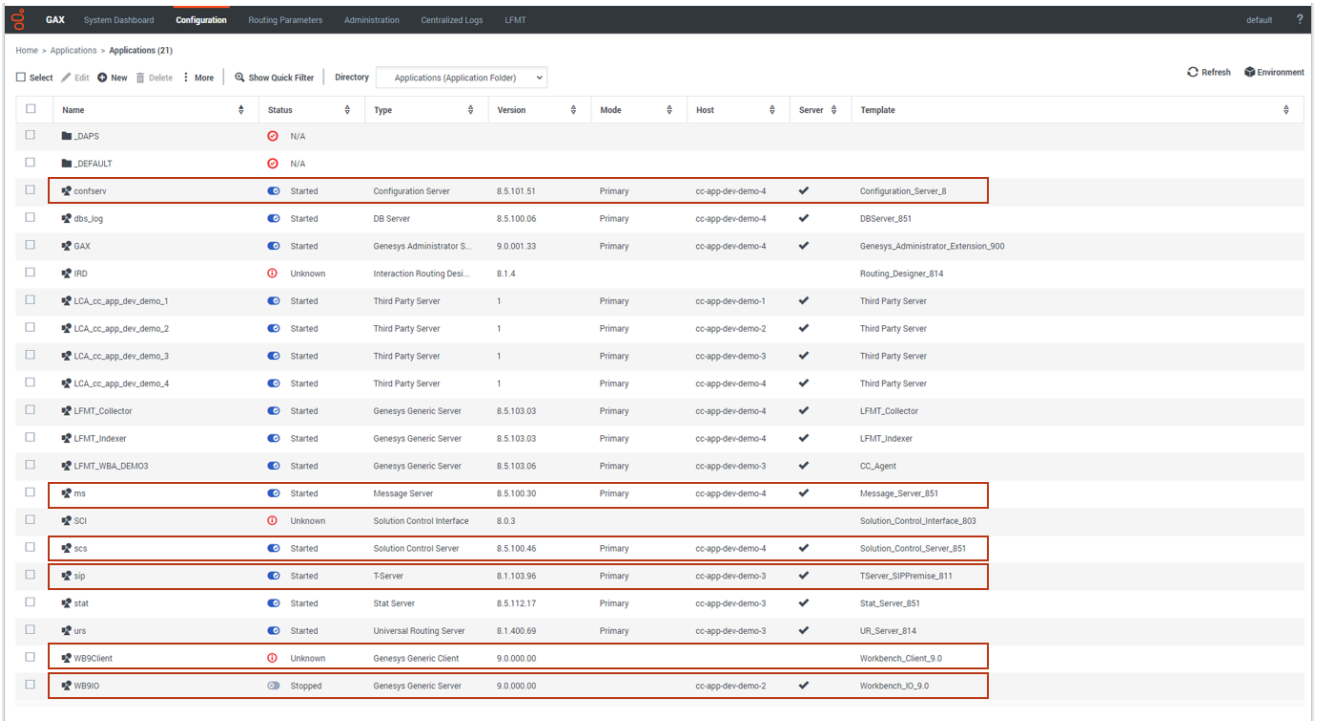
Workbench integrates to the Genesys Engage platform, as such the following Genesys Engage Objects will be required and leveraged by Workbench:

Component	Description/Comments
Genesys Engage **Workbench Client** application/ object	enables Engage CME configured Users to log into Workbench
Genesys Engage **Workbench IO** (Server) application/object	enables integration from Workbench to the Engage CS, SCS and MS
Genesys Engage **Configuration Server** application/object	enables integration from Workbench to the Engage CS; authentication and Config Changes
Genesys Engage **Solution Control Server** application/object	enables integration from Workbench to the Engage SCS; Alarms to WB from SCS
Genesys Engage **Message Server** application/ object	enables integration from Workbench to the Engage MS; Config change ChangedBy metadata
Genesys Engage **SIP Server** application/object (optional)	enables integration from Workbench to the Engage SIP Server enabling the Channel Monitoring feature *Workbench integrates to SIP Server only and not SIP Server Proxy

Warning

- Ensure each and every Engage CME Application has an assigned Template else the Workbench installation will fail.
- Ensure Engage CME Hosts Objects have an IP address assigned else the Workbench installation will fail.

Example CME objects:



Genesys Engage Application Configuration Pre-installation Steps

Please follow the sections below to:

- Import the Workbench **Installation Package** using GAX
- Provision the Workbench 9 **IO** (Server) Application using GAX
- Provision the Workbench 9 **Client** using GAX
- Provision the Workbench 9 Client **Role** using GAX

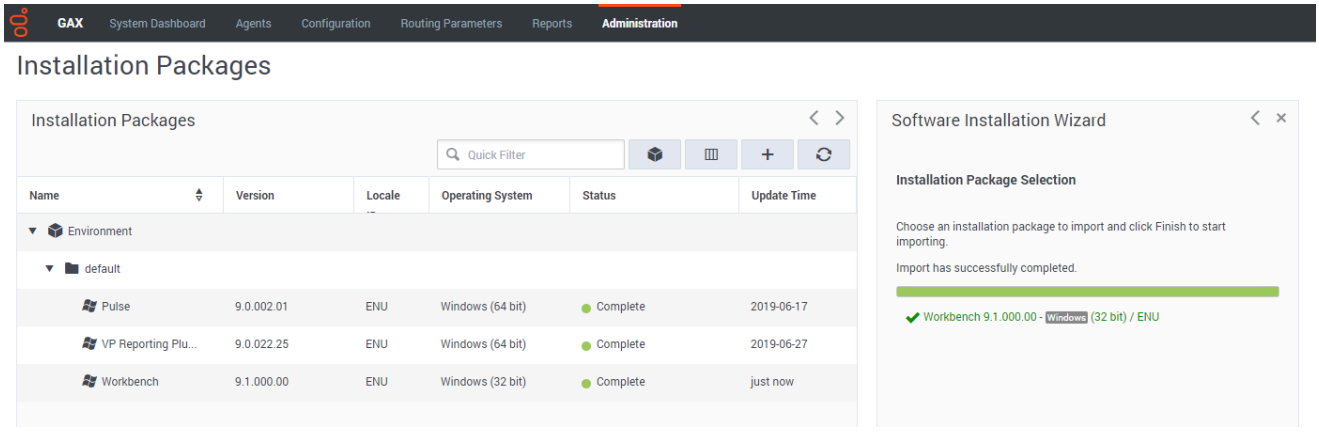
Workbench Installation Package Import using GAX

The following steps provide a guide to importing the mandatory GAX Workbench 9 Installation Package containing the Workbench 9 Templates and Applications configuration:

1. **Login** into GAX
2. Navigate to **Administration**
3. Click **New**
4. **Select** the **Installation Package Upload (includes templates)** option
5. Click **Next**

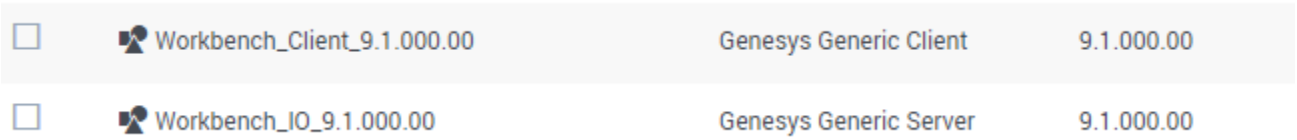
6. Click **Choose File**
7. Browse to the extracted **Workbench_9.x.xxx.xx_Pkg** folder
8. Double-click into the **templates** folder
9. Double-click into the **wb_9.x_gax_ip_template** folder
10. Double-click the **Workbench_9.x_GAX_Template_IP.zip** file
11. Click **Finish**
12. Click **Close** when the import has successfully completed

Example Workbench Installation Package:

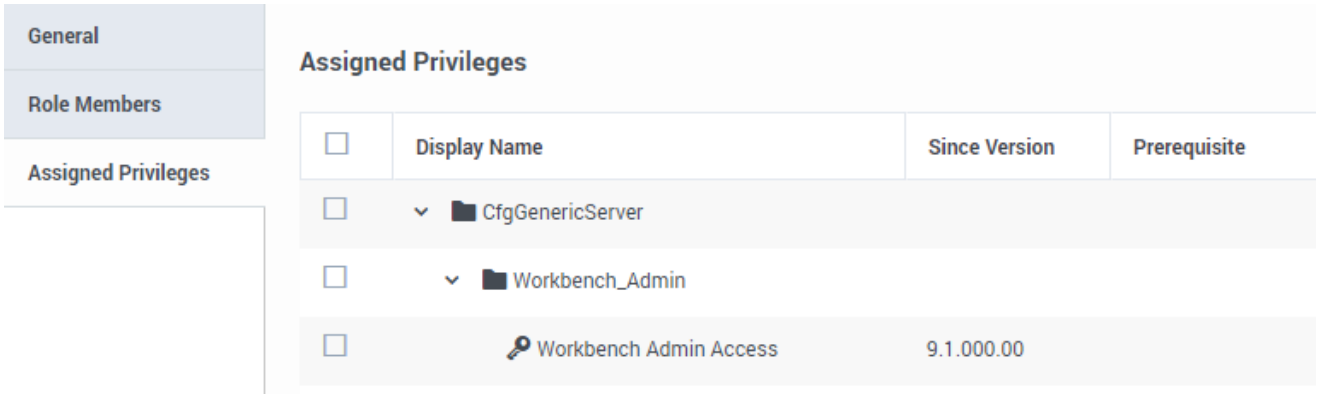


The procedure above will provide the:

IO and Client Templates:



Workbench Admin Role:



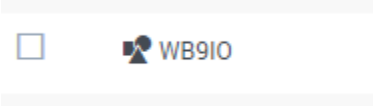
Provisioning the Workbench IO (Server) Application using GAX

This Workbench IO (Server) Application is used by Workbench to integrate to Genesys Engage components such as Configuration Server.

1. Log into **GAX**
2. Navigate to **Configuration**.
3. In the **Environment** section, select **Applications**.
4. In the **Applications** section, select **New**.
5. In the **New Properties** pane, complete the following:
    1. If not already, select the **General** tab
    2. In the **Name** field, enter an Workbench IO Application **Name** i.e. **WB9IO**
    3. Click on the **Template** field and navigate and select the **Workbench_IO_9.x.xxx.xx** Template
    4. In the **Working Directory** field, enter "**...**" (period character)
        1. Not explicitly required for Workbench 9, but a mandatory CME field
    5. In the **Command Line** field, enter "**...**" (period character)
        1. Not explicitly required for Workbench 9, but a mandatory CME field
    6. In the **Host** field, select the host where Workbench Primary will be installed.
    7. In the **Connections** tab, click the **Add** icon to establish connections to the following applications:
        1. (Optional) The primary or proxy Configuration Server from which the configuration settings will be retrieved. This is only required if connecting to Configuration Server via TLS. See the Genesys Security Deployment Guide for further instructions. **Note:** The security certificates must be generated using the SHA-2 secure hash algorithm.
6. Click **Save** to save the new application.

The Workbench IO (Server) Application (i.e. "WB9IO") configuration has now been completed; this

enables Workbench to Genesys Engage integration both from an installation and run-time perspective.



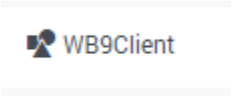
> **Important**
>
> - For a successful Workbench installation/run-time, the System/User Account for the Workbench IO application must have **Full Control** permissions.
> - The "WB9IO" Application will have a dummy [temp] Section/KVP due to mandatory prerequisite packaging.

Provisioning the Workbench Client Application using GAX

This Workbench Client Application is used by Workbench for Client Browser connections to Workbench, without it, no Users can log into Workbench.

1. Log into **GAX**
2. Navigate to **Configuration**.
3. In the **Environment** section, select **Applications**.
4. In the **Applications** section, select **New**.
5. In the **New Properties** pane, complete the following:
    1. If not already, select the **General** tab
    2. In the **Name** field, enter an Workbench Client Application **Name** i.e. **WB9Client**
    3. Click on the **Template** field and navigate and select the **Workbench_Client_9.x.xxx.xx** Template
6. Click **Save** to save the new application.

The Workbench Client (i.e. **WB9Client**) Application configuration has now been completed; this enables Users to login to Workbench.



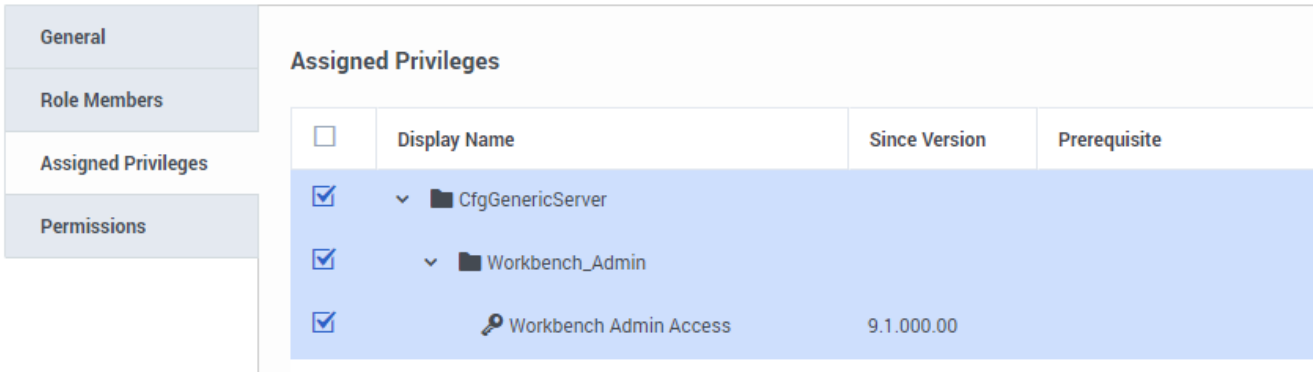
> **Important**
>
> - The "WB9IO" (Server) Application (or equivalent name) will have a dummy [temp] Section due to mandatory prerequisite packaging.

Provisioning the Workbench Client **Role** using GAX

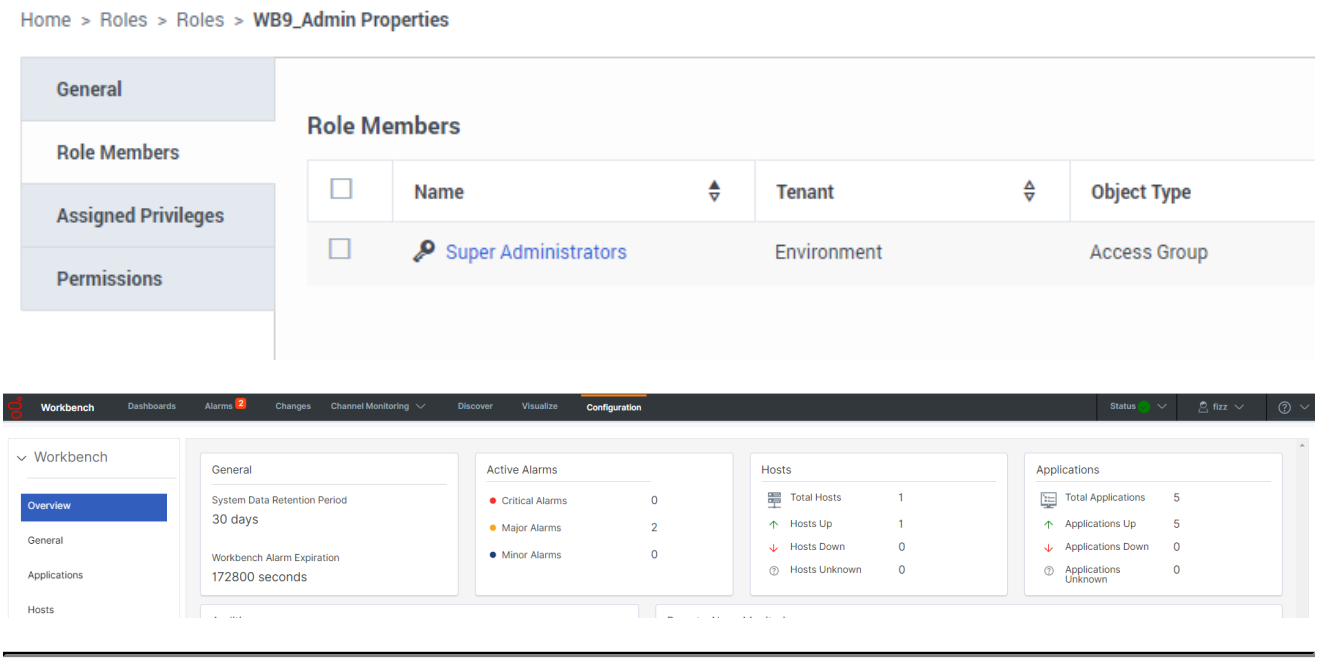
1. Log into **GAX**
2. Navigate to **Configuration**.
3. In the **Accounts** section, select **Roles**.
4. In the **Roles** section, select **New**.
5. Select **None** in the drop down for Role Template
6. Click OK
    1. If not already, select the **General** tab
    2. In the **Name** field, enter a Workbench Administrator Role Name - i.e. "**WB9_Admin**"
    3. In the **Description** field, enter "When assigned to Users, grants access to the Workbench\ Configuration Console."
    4. Select the **Role Members** tab
    5. Add your relevant **Access Group(s)** and/or **Person(s)**
    6. Select the **Assigned Privileges** tab
    7. Check the **Workbench Admin Access** checkbox
7. click **Save**

The **WB9_Admin** Role has been created.

Therefore, certain assigned Users, will now have visibility/access to the Workbench Configuration Console, enabling the Configuration of Workbench Applications, Settings and Features.



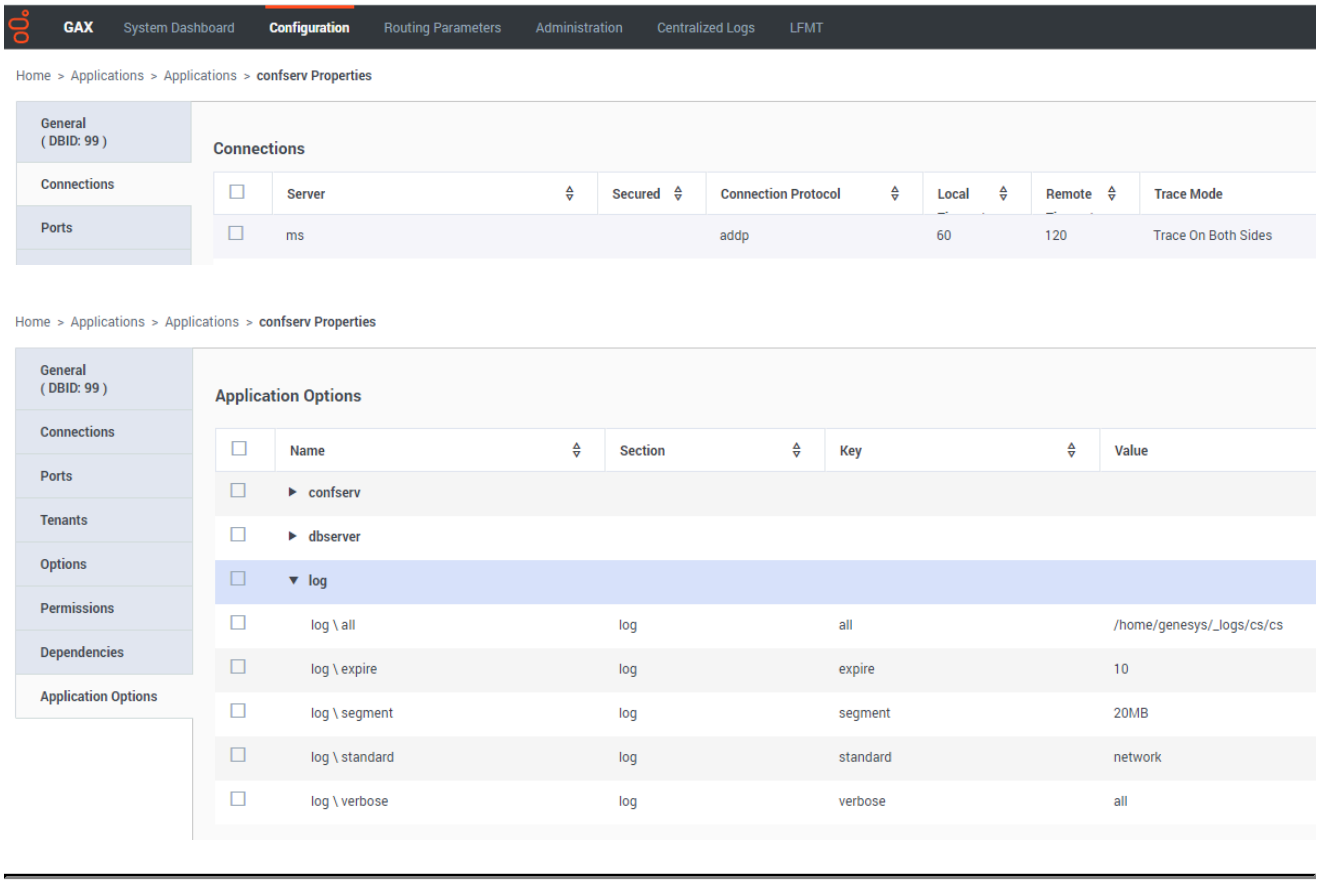
An example of the "Super Administrators" Access Group being assigned the "WB9_Admin" Role:



Changes Console **ChangedBy** field for Genesys Engage Changes

For the Changes Console **ChangedBy** field to be accurate (not "N/A"), the following Genesys Engage configuration is required:

- A connection from the respective Genesys Engage Configuration Server or Configuration Server Proxy to the Genesys Engage Message Server that Workbench is connected to.
- If not already, **standard=network** added to the **log** section of the Configuration Server or Configuration Server Proxy that Workbench is connected to.


GAX
System Dashboard
Configuration
Routing Parameters
Administration
Centralized Logs
LFMT
Home > Applications > Applications > confserv Properties
General (DBID: 99)
Connections
Ports
Connections
Server
Secured
Connection Protocol
Local
Remote
Trace Mode
ms
addp
60
120
Trace On Both Sides
Home > Applications > Applications > confserv Properties
General (DBID: 99)
Connections
Ports
Tenants
Options
Permissions
Dependencies
Application Options
Application Options
Name
Section
Key
Value
confserv
dbserver
log
log \ all
log
all
/home/genesys/_logs/cs/cs
log \ expire
log
expire
10
log \ segment
log
segment
20MB
log \ standard
log
standard
network
log \ verbose
log
verbose
all

Workbench Installation - Windows - Primary Node

The Workbench installation files will be contained in the Genesys My Portal obtained downloaded compressed file.

Review this link for details on downloading Workbench: Downloading Workbench

Important

1. Workbench requires the installation of a Primary Node at each and every Data-Center.
2. The Workbench Primary Node must be installed prior to installing Workbench Additional Nodes.
3. Workbench ships with its own pre-bundled Java distribution, OpenJDK11; all Workbench components will be configured through the installation to use this Java distribution and should not affect any other components that may be installed on the host.
4. The Workbench installation uses the Ant Installer component, if during the Workbench installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.
5. Use an **Administrator** level account when running the Workbench *install.bat* file.
6. Genesys does not recommend installation of its components via Microsoft Remote Desktop
7. If the Workbench installation is cancelled mid completion, please ensure the Workbench install directory is cleaned/purged **prior** to attempting another install

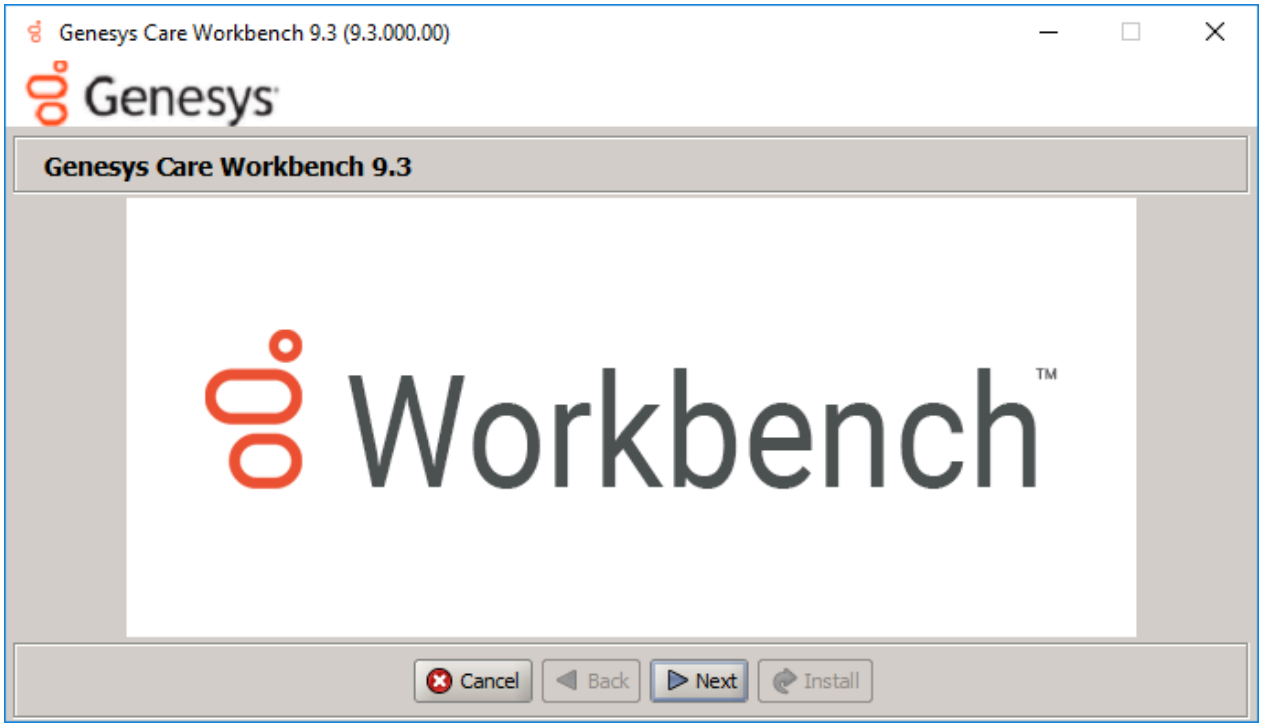
Warning

- Workbench uses the Hostname for component configuration
- Please ensure hostname resolution between Workbench and Engage Hosts is accurate and robust
- If the Workbench Hosts have multiple NIC's, please ensure the Hostname resolves to the desired IP Address prior to Workbench installation

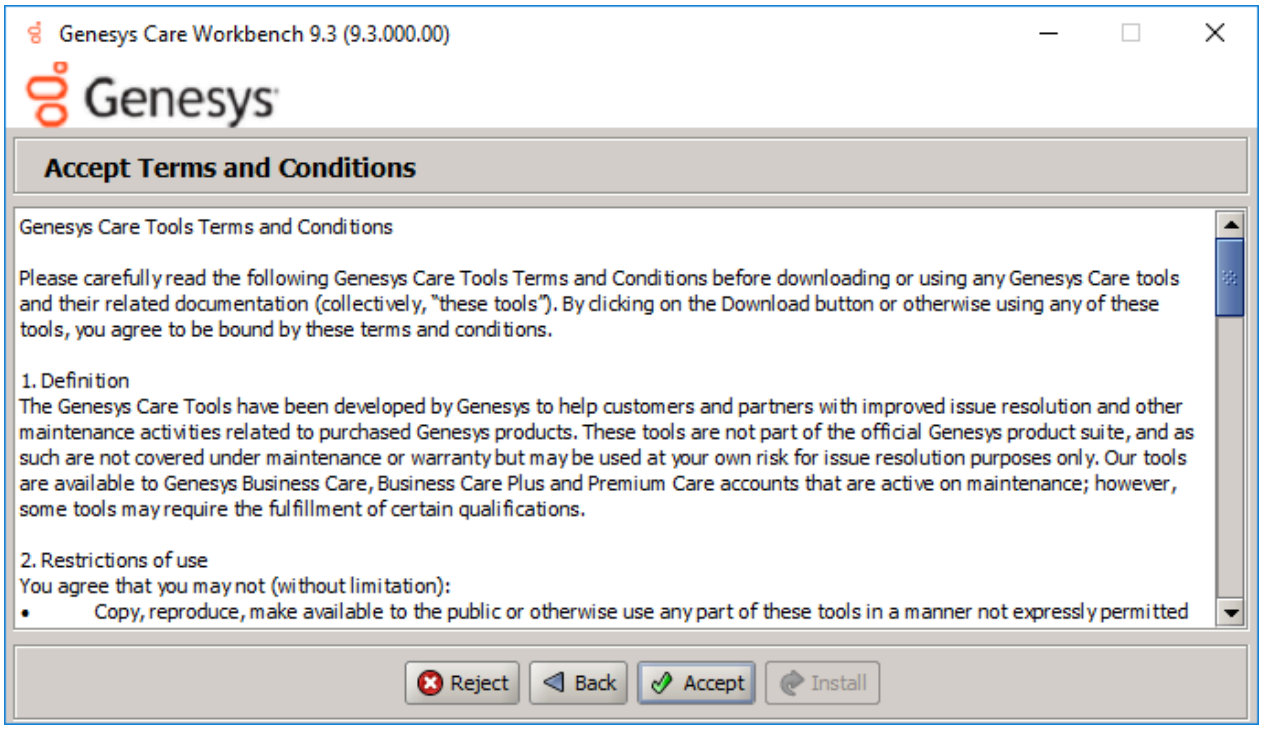
Please use the following steps to install Workbench **9.x.xxx.xx**.

1. Extract the downloaded **Workbench_9.x.xxx.xx_WINDOWS.zip** compressed zip file.
2. Navigate into the **Workbench_9.x.xxx.xx_WINDOWS\ip\windows** folder.
3. Extract the **Workbench_9.x.xxx.xx_Installer_Windows.zip** compressed zip file.
4. Navigate into the **Workbench_9.x.xxx.xx_Installer_Windows** folder.
5. Open a Command/Powershell Console **As Administrator** and run **install.bat**.

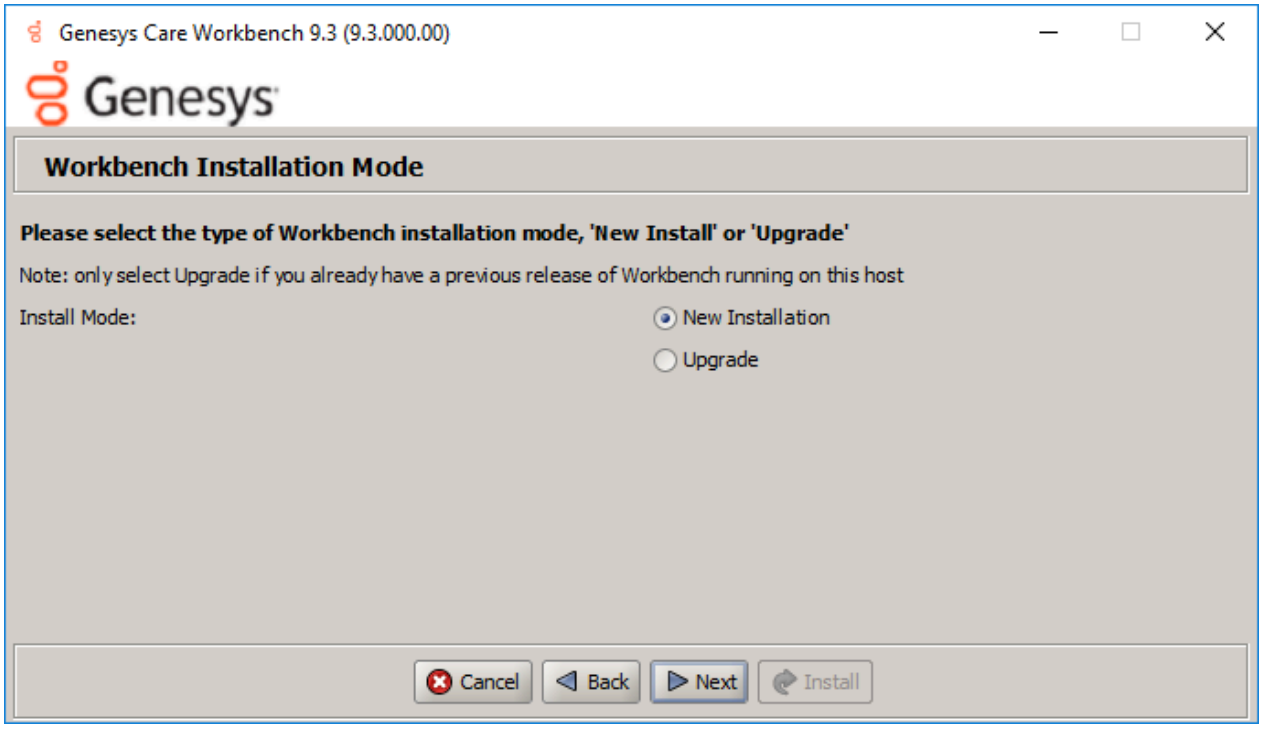
6. Click **Next** on the **Genesys Care Workbench 9.x** screen to start the Workbench installation.



7. Review and if in agreement, click **Accept** to the **Genesys Terms and Conditions** to continue.



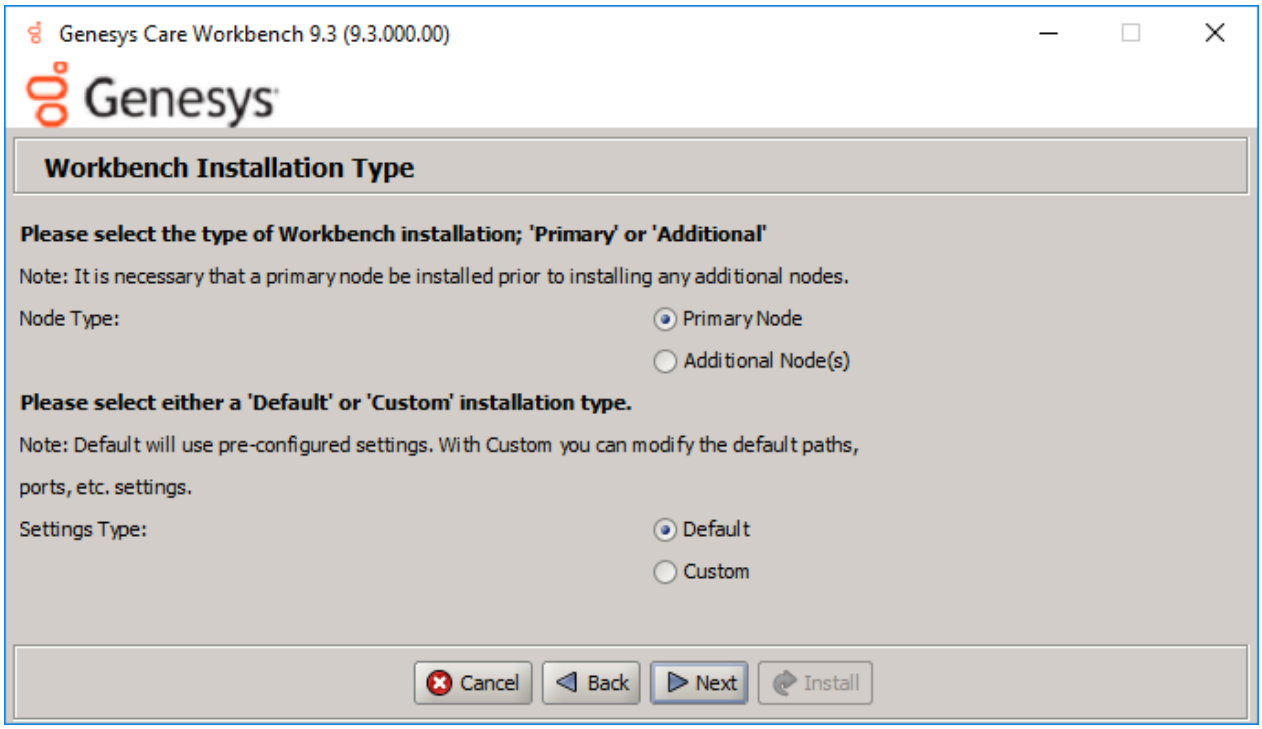
8. Select **New Installation** on the Installation Mode screen



9. Select the **Installation Type**

- The next Workbench **Installation Type** screen contains multiple Workbench installation options; Workbench contains multiple components:
  - Workbench IO
  - Workbench Agent
  - Workbench Elasticsearch
  - Workbench Kibana
  - Workbench Logstash
  - Workbench Heartbeat
  - Workbench ZooKeeper.
- Select **Primary Node** (given we're installing the first, Primary, Workbench node/components).
- Next, choose between the **Default** or **Custom** installation type.
  - For the **Default** type, the respective Workbench component **default** (including binaries, paths, config, ports etc) options will be used.
  - Or, if required, you can change these default options (paths, config, ports etc) by selecting a **Custom** install.

> ### Important
>
> - The Workbench Primary Node installation must/will include ALL of the Workbench components above
>   - Therefore if/when **Primary Node** is selected, ALL mandatory Workbench Primary components above will be installed on the host.



Once you've selected the appropriate options, click **Next**.

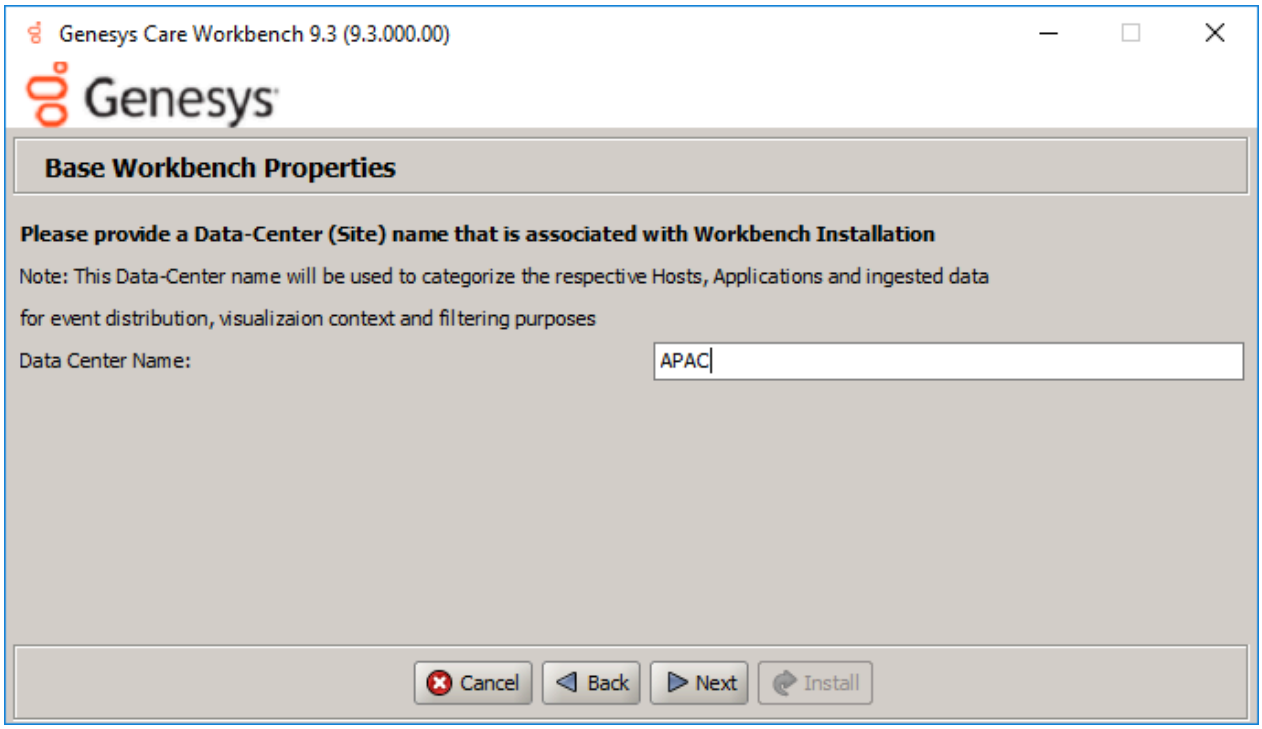
> **Important**
>
> - For High Availability (HA), you can install additional Workbench application nodes/ components
> - The installation of additional Workbench components has been covered in the section "Workbench Installation - Windows - Additional Node".

10. Provide the Workbench **Data-Center** name (i.e. "EMEA" or "LATAM" or "Chicago" - do NOT use "default")

> **Important**
>
> - Workbench Data-Centers is a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes
> - Each Workbench host, and the respective applications within that host, are assigned

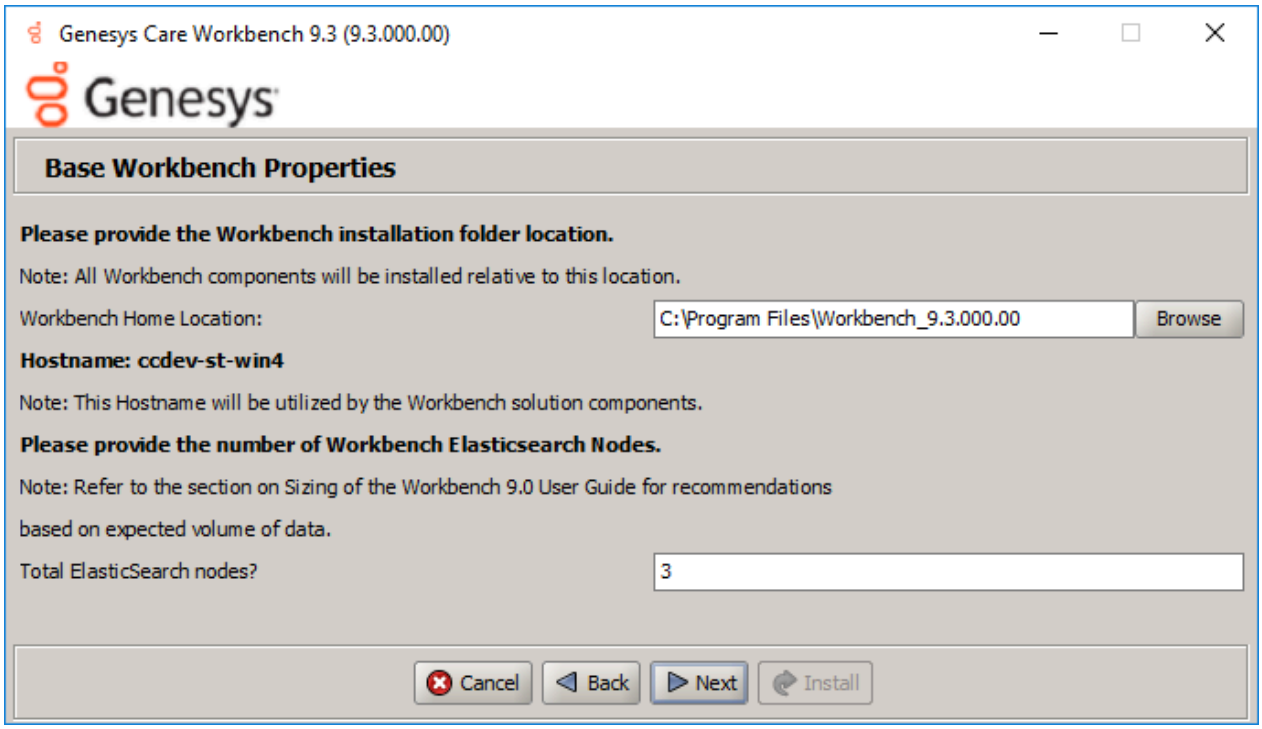
to a Data-Center, this is mandatory

- Note: The Data-Center name is **case-sensitive**, limited to a maximum of **10**, Alphanumeric and underscore characters only.



Once the Data-Center name has been entered, click **Next**.

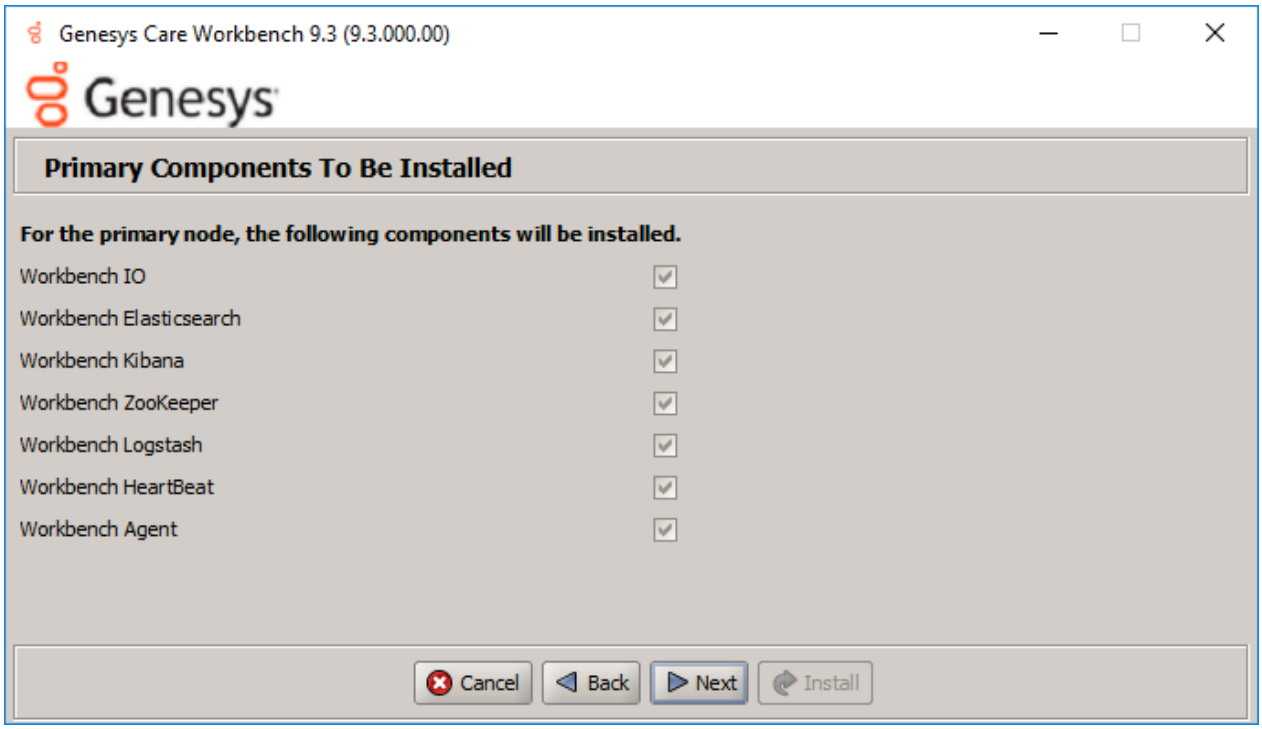
11. The next **Base Workbench Properties** screen provides basic information that is relevant to all Workbench components
    - This is required irrespective of whether the installation is *Primary* or *Additional* and if *Default* or *Custom* was chosen.
    - Provide the **Workbench Home Location** folder where Workbench components will be installed (i.e. "C:\Program Files\Workbench_9.x.xxx.xx").
    - Review the network **Hostname** - this should be accessible/resolvable within the domain
    - Based on the Planning/Sizing section, enter the **Total** number of Workbench **Elasticsearch Nodes** to be used by the Workbench solution.
        - The default 3 Elasticsearch Node value is correct even if a 1 x Workbench stand-alone architecture is being deployed; this enables future expansion if/when needed.



Once all required information is added, click **Next**.

> **Important**
>
> The Elasticsearch component is bundled with Workbench and is used to store all of the ingested data related to Workbench. An instance of Elasticsearch is installed through the Workbench Primary Node installation; For other, HA node instances, you can use the Workbench installer and proceed through the Workbench Additional Node(s) installation.

12. The next **Primary Components To Be Installed** screen lists the Workbench components that will be installed for the Primary Node
    - ALL the Workbench components to be installed are selected by default, since these are mandatory



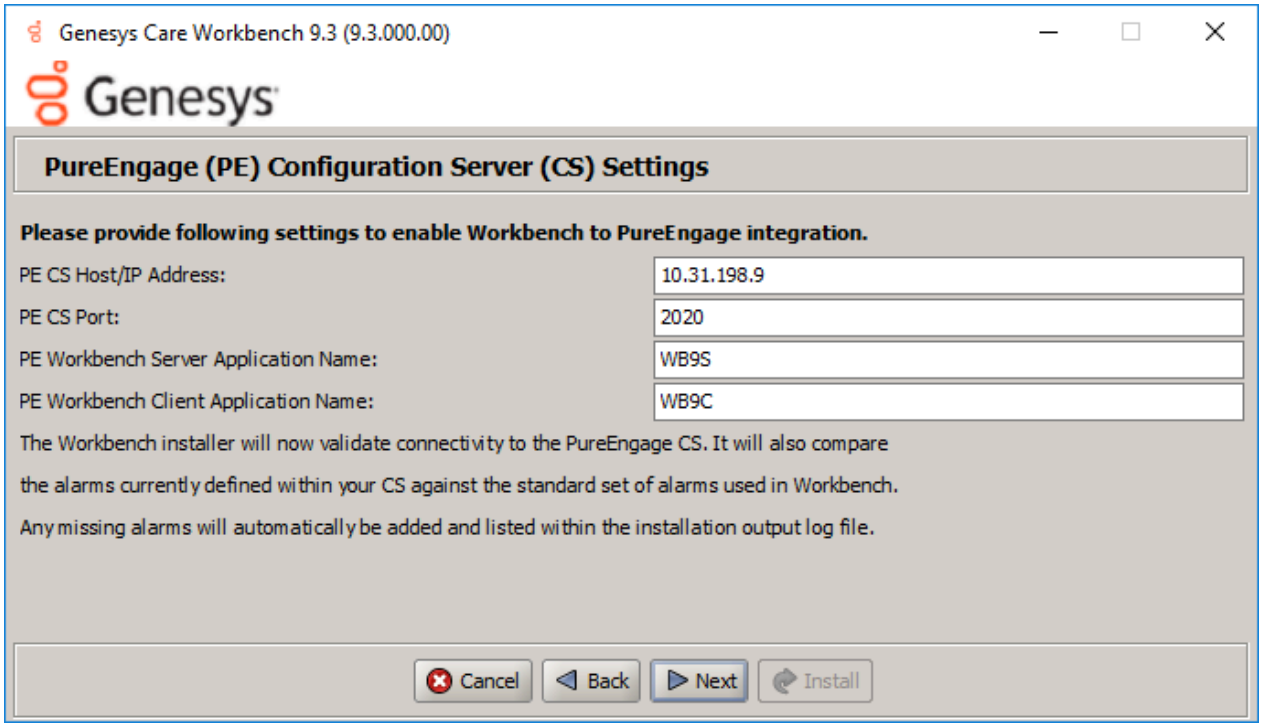
Press **Next** to continue.

> **Important**
> The Workbench Agent is installed regardless of whether this is a Primary or Additional Node(s) installation.

13. The next **PureEngage (PE) Configuration Server (CS) Settings** screen relates to the Workbench to Genesys Engage integration:
    - Provide the **Genesys Engage Configuration Server Hostname/IP address**
    - Provide the **Genesys Engage Configuration Server Port** (i.e. 2020)
    - Provide the **Genesys Engage Workbench Server Application Name** (i.e. "WB9IO")
    - Provide the **Genesys Engage Workbench Client Application Name** (i.e. "WB9Client")

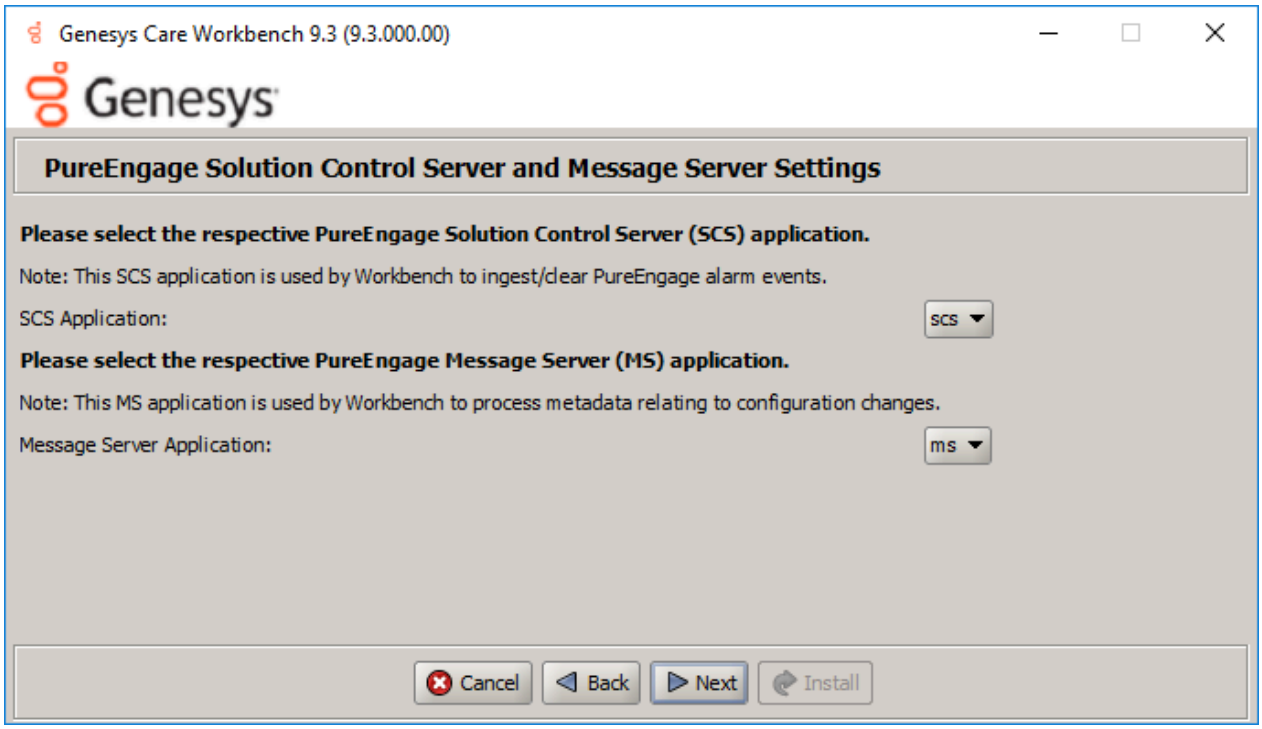
> **Important**
> The Workbench Server and Client applications must have been previously created/

existing in the Genesys Engage Configuration Server; please review the Planning and Deployment\Planning section of this document for more details. From a Workbench perspective these Applications are case-sensitive therefore please verify case/spelling.



Once complete, verify the settings, click **Next**.

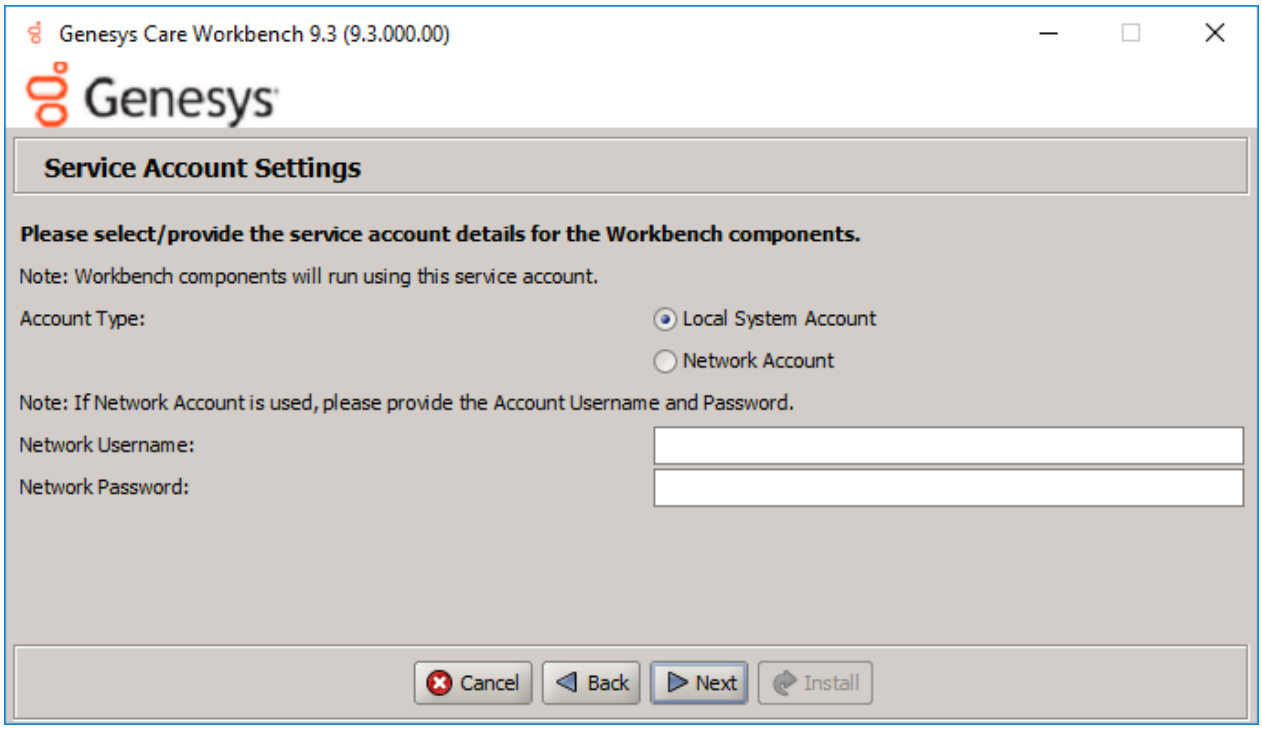
14. The next **Genesys Engage Solution Control Server and Message Server Settings** screen enables selection of the Genesys Engage **Solution Control Server** (SCS) and **Message Server** (MS) applications to which Workbench will connect.



Select the relevant Genesys Engage SCS and MS applications, based on the associated Configuration Server from the previous screen, for Workbench to connect to and click **Next**.

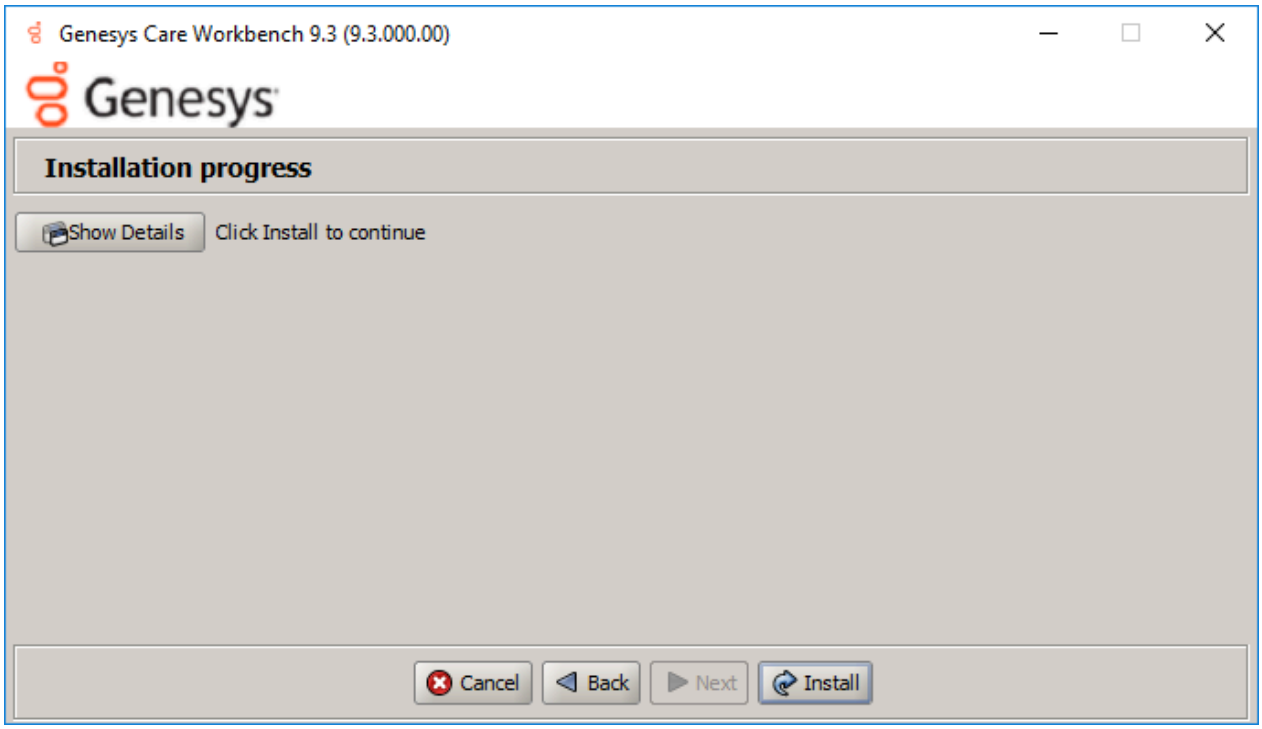
15. The next **Service Account Settings** screen enables the selection of either **System** or **Network** Account.

    The Workbench components are installed and executed as *Services*. Select either Local System Account or a Network Account; if Network Account is selected, provide the Username and Password to be used.



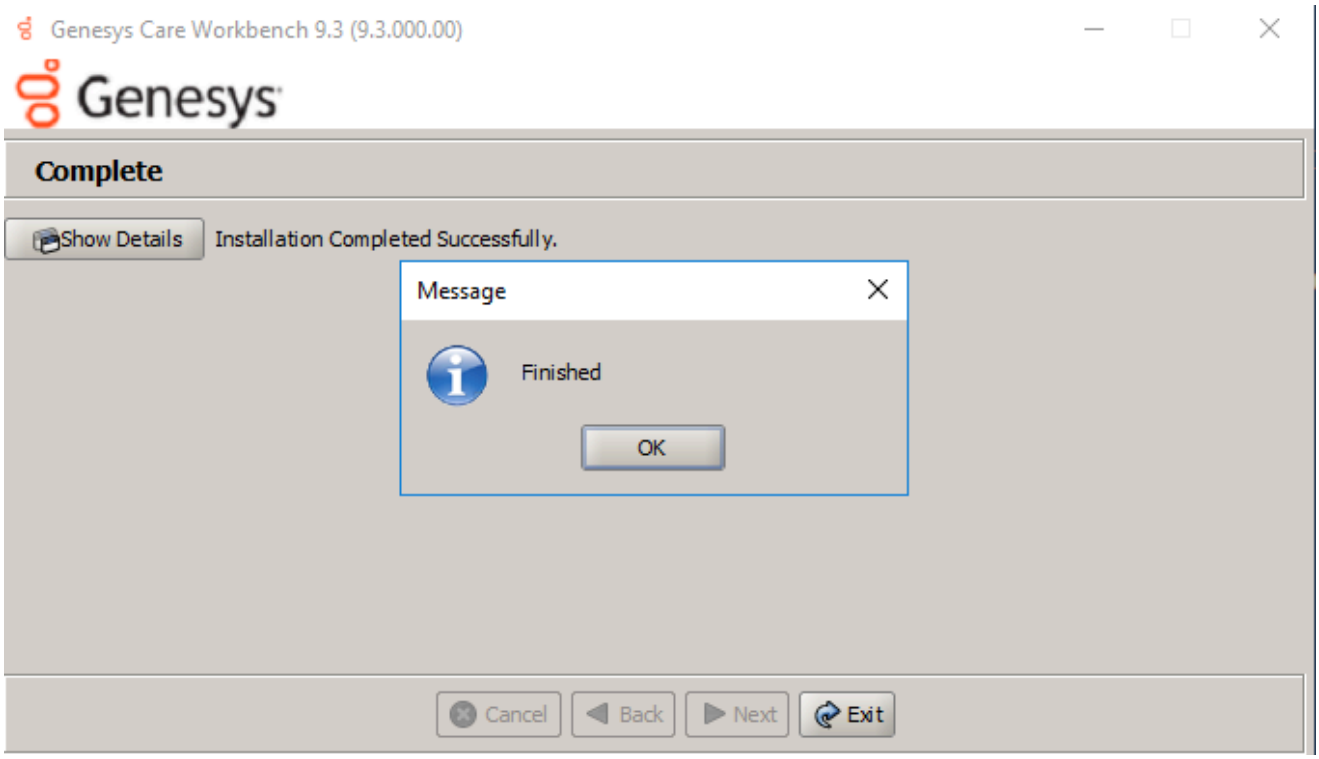
Once complete, click **Next**.

16. With all the workbench options now configured, press **Install** to start the Workbench installation process.



> **Tip**
>
> The **Show Details** button allows you to review the steps the installer is taking to install the Workbench component(s). This is also a good source for any errors that may be observed.

When the Workbench installation completes the dialog below will be presented.



Click **OK** and **Exit** to close the installation dialogs.

Workbench Login

Navigate to **http://<WORKBENCH_HOST>:8181** to login (Engage CME credentials) to Workbench.

On initial Workbench login you'll be presented with the Workbench "Home Dashboard".

> ### Tip
>
> - The <WORKBENCH_PORT> (default 8181) can be changed via the custom installation.

Workbench Primary Node/Host - Windows Services

The Workbench Primary Node/Host will contain the following Windows Services:

- Genesys Workbench.IO 9.x.xxx.xx
- Genesys Workbench Elasticsearch 9.x.xxx.xx
- Genesys Workbench ZooKeeper 9.x.xxx.xx
- Genesys Workbench Kibana 9.x.xxx.xx
- Genesys Workbench Logstash 9.x.xxx.xx
- Genesys Workbench Metricbeat 9.x.xxx.xx
- Genesys Workbench Agent 9.x.xxx.xx
- Genesys Workbench Heartbeat 9.x.xxx.xx

Stopping/Starting Workbench

To stop Workbench, stop the Workbench Services in this order:

- Genesys Workbench.IO 9.x.xxx.xx
- Genesys Workbench Kibana 9.x.xxx.xx
- Genesys Workbench Metricbeat 9.x.xxx.xx
- Genesys Workbench Elasticsearch 9.x.xxx.xx
- Genesys Workbench ZooKeeper 9.x.xxx.xx
- Genesys Workbench Agent 9.x.xxx.xx
- Genesys Workbench Logstash 9.x.xxx.xx
- Genesys Workbench Heartbeat 9.x.xxx.xx

To start Workbench, start the Workbench Services in this order.

- Genesys Workbench.IO 9.x.xxx.xx
- Genesys Workbench Elasticsearch 9.x.xxx.xx
- Genesys Workbench ZooKeeper 9.x.xxx.xx
- Genesys Workbench Kibana 9.x.xxx.xx
- Genesys Workbench Logstash 9.x.xxx.xx
- Genesys Workbench Metricbeat 9.x.xxx.xx
- Genesys Workbench Agent 9.x.xxx.xx
- Genesys Workbench Heartbeat 9.x.xxx.xx

Workbench Installation - Windows - Additional Node

As per the Sizing section, if Workbench data and configuration redundancy and service high availability is required, Genesys recommends a **3+** (3 minimum Multi/Cluster) Node/Host Workbench deployment.

> ### Warning
>
> - Before commencing these Workbench Additional Node instructions, ensure the Workbench Primary Node has been successfully installed
> - Workbench supports a **1** or **N** (**minimum 3** with **odd** number increments) Node architecture
>   - Deploying only a Workbench Primary and Workbench Node 2 architecture will cause future upgrade issues likely resulting in a reinstall of Workbench

Workbench Additional Node - Installation

Please use the following steps to install Workbench Additional Nodes on Windows Operating Systems.

1. On the respective **2nd Workbench Additional Node/Host**, extract the downloaded Workbench installation compressed zip file.
2. Within the extracted folder, open a Command/Powershell Console **As Administrator** and run **install.bat**.
3. Click **Next** on the **Genesys Care Workbench 9.x** screen
4. Review and if you agree click **Accept** on the **Term's & Condition's** screen
5. Select **New Installation** on the **Workbench Installation Mode** screen
    1. Click **Next**
6. On the **Workbench Installation Type** screen
    1. Select **Additional Node**
    2. If required change from the default **Default** installation to **Custom** (complete the Custom config according to your needs)
    3. Click **Next**
7. On the **Base Workbench Properties** screen

1. Provide the **Workbench Home Location** folder where Workbench components will be installed (i.e. " C:\Program Files\Workbench_9.1.000.00").
2. Review the network **Hostname** - this should be accessible/resolvable within the domain
3. Click **Next**

8. On the **Additional Components To Be Installed** screen:
    1. Ensure the **Workbench Elasticsearch** option is are checked (for HA of the ingested Workbench data i.e. Alarms, Changes, Channel Monitoring etc)
    2. Ensure the **Workbench ZooKeeper** option is checked (for HA of the Workbench configuration settings)
        1. Workbench ZooKeeper Cluster supports a **maximum of 5 Nodes**
    3. If required, based on the Planning/Sizing exercise, ensure the **Workbench Logstash** option is checked
    4. Workbench Agent is checked by default; it's a mandatory requirement for any hosts running Workbench 9.x components
    5. Provide the **Primary Node ZooKeeper IP and Port** - i.e. **10.20.30.1:2181**

> **Warning**
>
> Due to a Port validation limitation, please ensure the ZooKeeper Port is correct before pressing Enter; a race-condition could occur if not correctly entered.

    6. click **Next**
9. Click **Next** on the **Service Account** screen
    1. unless Network Account is required
10. Click **Install**
11. Click **OK** on the **Finished** dialog
12. Click **Exit**

Repeat the above for the respective **3rd** (or ALL **N** nodes) Workbench Additional Node/Host

Checkpoint

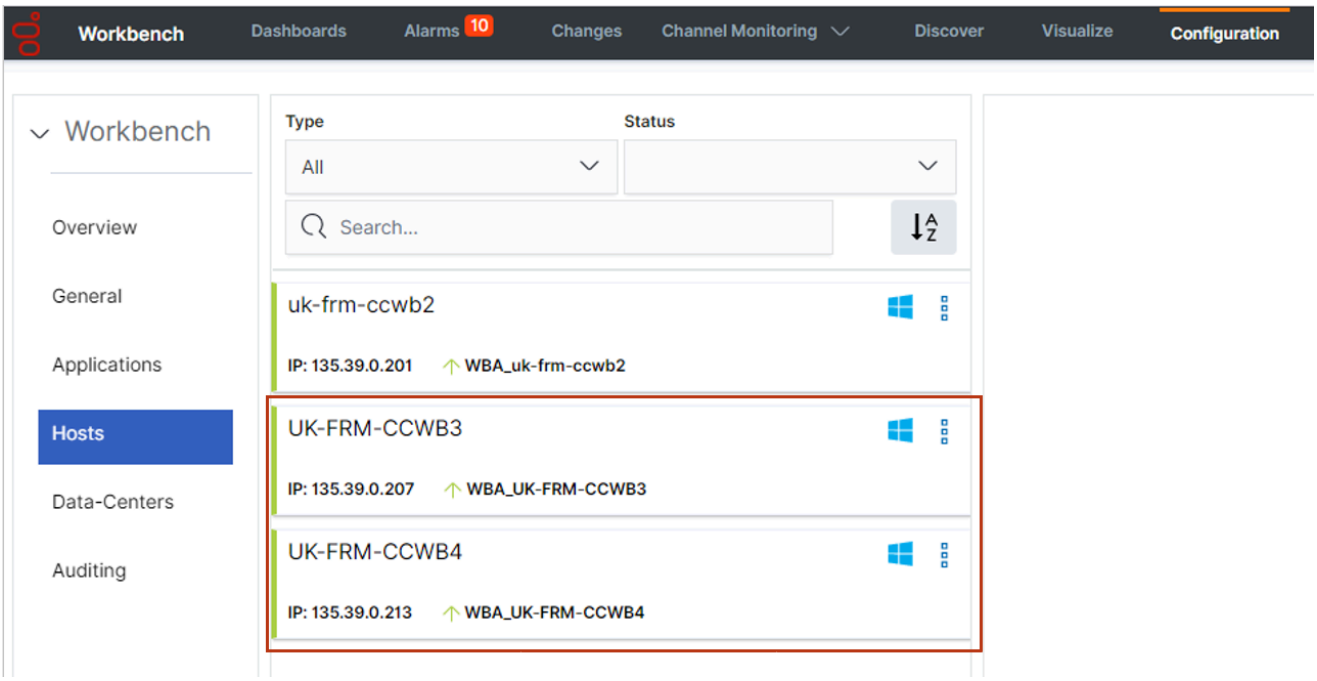
> **Important**
>
> - Based on the instructions above, within the Workbench Configuration\Hosts and Workbench Configuration\Applications menus there should now be additional Hosts and

Applications

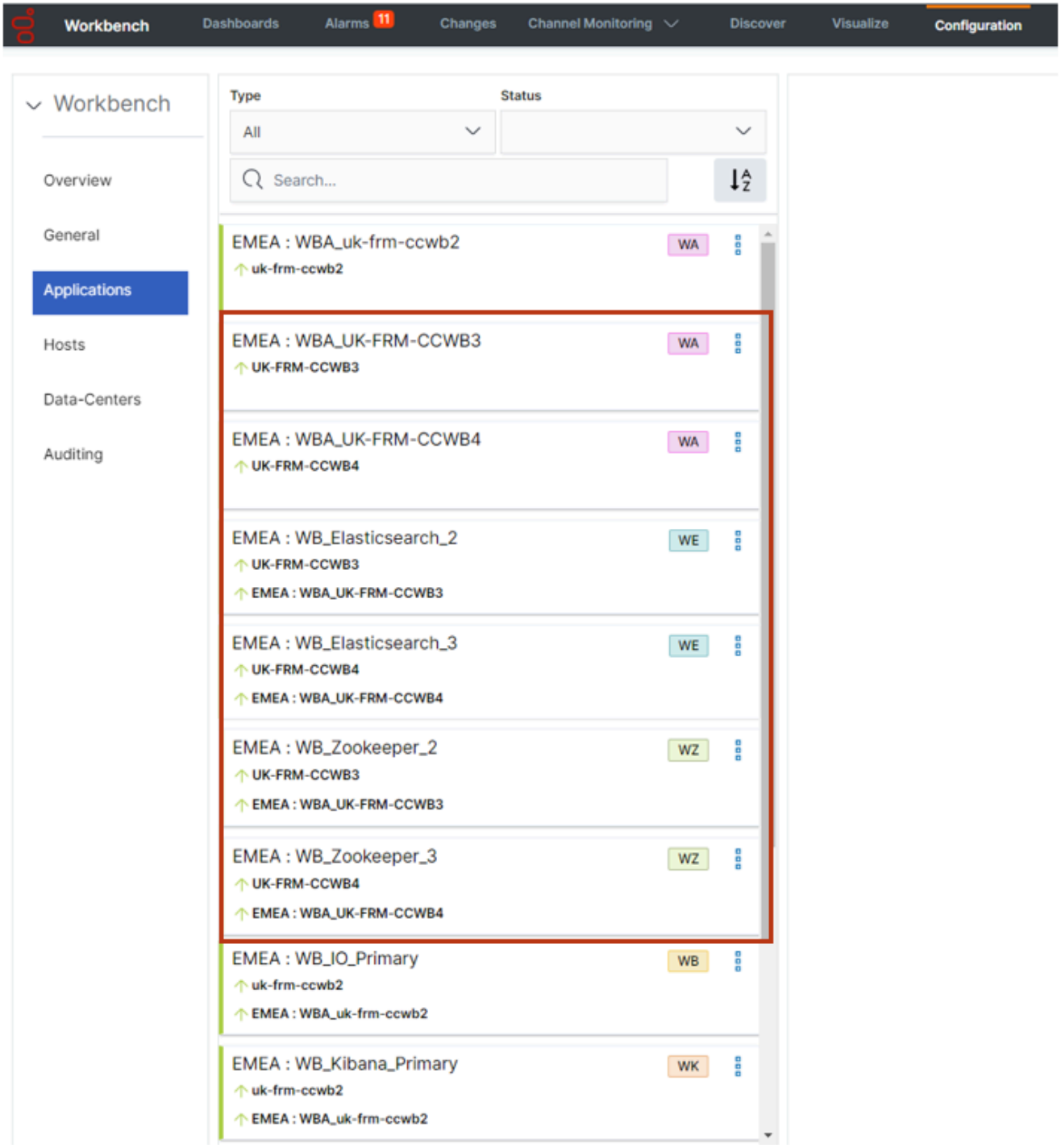
- The number of additional workbench Hosts and Applications will vary based on your sizing architecture and the selections you made during the installation of additional components
- Currently additional Workbench components have been installed on their respective Hosts, the next step is to form the Workbench Cluster which will provide HA of ingested event data (Workbench Elasticsearch) and HA of Workbench Configuration data (Workbench ZooKeeper).
- Do not form the Workbench Cluster until all Workbench Additional Nodes have had their additional respective components installed

As an example, following the installation of Workbench Additional Node 2 and Node 3, the additional Hosts and Applications are highlighted below:

Hosts



Applications


Workbench
Dashboards
Alarms 11
Changes
Channel Monitoring
Discover
Visualize
Configuration
Workbench
Overview
General
Applications
Hosts
Data-Centers
Auditing
Type
All
Status
Search...
EMEA : WBA_uk-frm-ccwb2
WA
uk-frm-ccwb2
EMEA : WBA_UK-FRM-CCWB3
WA
UK-FRM-CCWB3
EMEA : WBA_UK-FRM-CCWB4
WA
UK-FRM-CCWB4
EMEA : WB_Elasticsearch_2
WE
UK-FRM-CCWB3
EMEA : WBA_UK-FRM-CCWB3
EMEA : WB_Elasticsearch_3
WE
UK-FRM-CCWB4
EMEA : WBA_UK-FRM-CCWB4
EMEA : WB_Zookeeper_2
WZ
UK-FRM-CCWB3
EMEA : WBA_UK-FRM-CCWB3
EMEA : WB_Zookeeper_3
WZ
UK-FRM-CCWB4
EMEA : WBA_UK-FRM-CCWB4
EMEA : WB_IO_Primary
WB
uk-frm-ccwb2
EMEA : WBA_uk-frm-ccwb2
EMEA : WB_Kibana_Primary
WK
uk-frm-ccwb2
EMEA : WBA_uk-frm-ccwb2

Workbench ZooKeeper Cluster - Configuration

Warning

- Before configuring the Workbench ZooKeeper Cluster, ensure ALL Workbench Additional Node components have been installed

Important

- Before configuring the Workbench Cluster, ensure ALL Workbench Agent and Workbench ZooKeeper components are Up (Green)
- For the Workbench ZooKeeper configuration, use **IP Address:PORT** and not Hostname:Port
- Workbench ONLY supports ODD number of additional nodes (i.e. 1, 3, 5 etc) within a Workbench Cluster architecture
- Ensure ALL "N" Workbench Additional Nodes are installed/configured before forming the final Workbench Cluster
- Workbench does not support scaling post Workbench Cluster formation
  - For example, if you form a 3 Node Workbench ZooKeeper Cluster, you cannot increase to a 5 Node ZooKeeper Cluster - as such please ensure your Workbench planning and sizing is accurate before completing your Workbench ZooKeeper Cluster formation, else a reinstall may be required

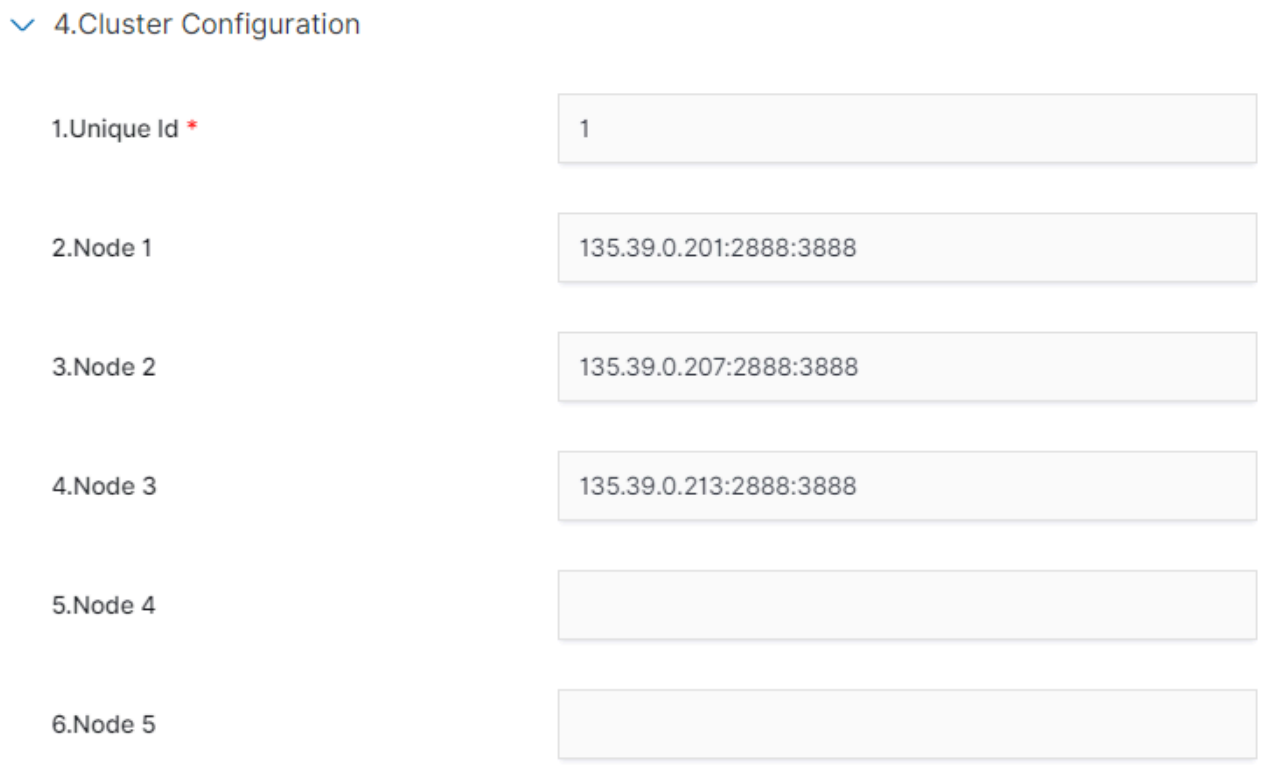
1. Navigate to the **Primary ZooKeeper** application, i.e. **EMEA : WB_ZooKeeper_Primary**
   1. Expand Configuration Section **4.Cluster Configuration**
   2. In the **Node 1** field enter the Primary Workbench ZooKeeper Hostname **<IPAddress>:2888:3888**
   3. In the **Node 2** field enter the Workbench Additional ZooKeeper Node 2 Hostname **<IPAddress>:2888:3888**
   4. In the **Node 3** field enter the Workbench Additional ZooKeeper Node 3 Hostname **<IPAddress>:2888:3888**
   5. Click **Save**

Important

- Wait for 3 minutes and refresh (F5) the Chrome Browser

- Workbench 9 should now have a Workbench ZooKeeper clustered environment providing HA of Workbench Configuration

An example Workbench Cluster Configuration being:



Warning

- Workbench ZooKeeper Cluster supports a maximum of 5 Nodes

Workbench Elasticsearch Cluster - Configuration

Warning

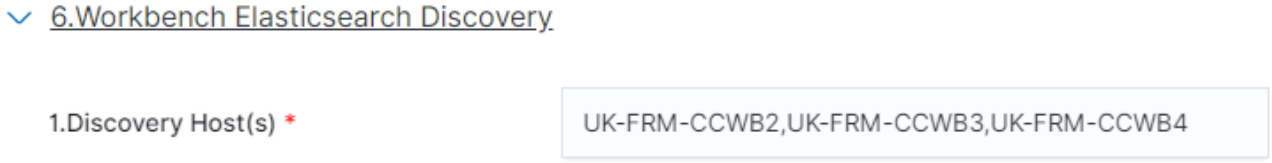
- Before configuring the Workbench Elasticsearch Cluster, ensure ALL Workbench Additional Node components have been installed

Important

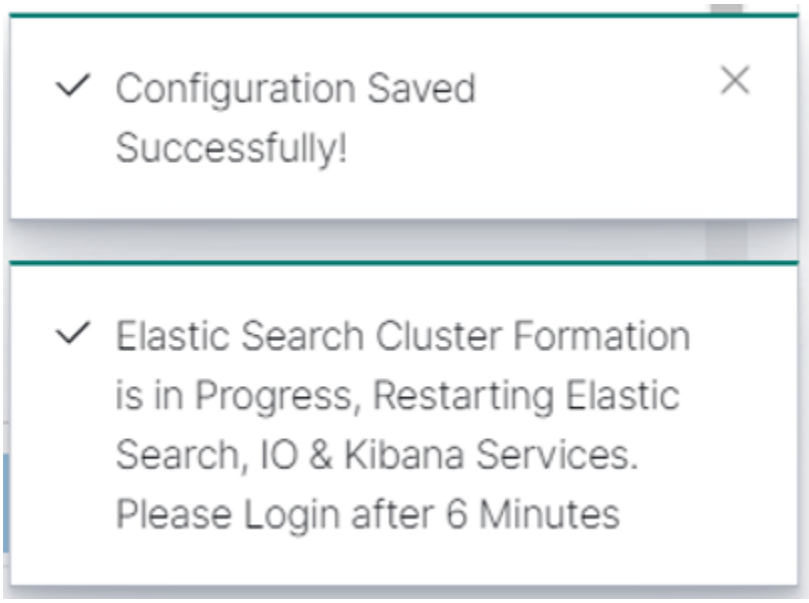
- Before configuring the Workbench Cluster, ensure ALL Workbench Agent and Workbench Elasticsearch components are Up (Green)
- Fully Qualified Domain Name (FQDN) is NOT supported - either use **Hostname** or **IP Address** and not FQDN
- Workbench ONLY supports odd number of additional nodes (i.e. 1, 3, 5, 7, 9 etc) within a Cluster deployment
- Ensure ALL "N" Additional Nodes are installed before forming the final Workbench Cluster
- Workbench does not support scaling post Workbench Cluster formation
  - For example, if you form a 3 Node Workbench Elasticsearch Cluster, you cannot increase to a 5 Node Elasticsearch Cluster - as such please ensure your Workbench planning and sizing is accurate before completing your Workbench Elasticsearch Cluster formation, else a reinstall may be required

1. Navigate to the **Primary Elasticsearch** application, i.e. **EMEA : WB_Elasticsearch_Primary**
   1. Expand Configuration Section **6.Workbench Elasticsearch Discovery**
   2. In the **Discovery Host(s)** field enter the value from the associated **Section 5 - [Workbench Elasticsearch Identifiers/Network Host]** field of ALL Elasticsearch applications (i.e. WB-1,WB-2,WB-3)
   3. Click **Save**

Example configuration being:



Post clicking ''Save'' you will see the popup notification below:



Important

- Logout of Workbench (Chrome Browser session)
- Wait for a minimum of 6 minutes for the Workbench Elasticsearch Cluster formation to complete
- Login to Workbench
- Workbench 9 should now have a Workbench Elasticsearch Clustered environment providing HA of Workbench ingested event data

Test Health of Workbench Elasticsearch Cluster Status

Check the health status of the Workbench Elasticsearch Cluster:

In a Chrome Browser navigate to:

http://<WB-VM-X>:9200/_cluster/health?pretty

or

1. Or using Windows Powershell curl
    1. Execute **curl -Uri "<WB-VM-X>:9200/_cluster/health?pretty"**
2. or using Linux CURL
    1. Execute **curl "http://<WB-VM-X>:9200/_cluster/health?pretty"**

Where <WB-VM-X> is the **Workbench Primary**, **Node 2** or **Node 3** Host.

Elasticsearch Cluster health should be reporting **Green**.

Typical expected output:


```
{
 "cluster_name" : "GEN-WB-Cluster",
 "status" : "green",
 "timed_out" : false,
 "number_of_nodes" : 3,
 "number_of_data_nodes" : 3,
 "active_primary_shards" : 29,
 "active_shards" : 58,
 "relocating_shards" : 0,
 "initializing_shards" : 0,
 "unassigned_shards" : 0,
 "delayed_unassigned_shards" : 0,
 "number_of_pending_tasks" : 0,
 "number_of_in_flight_fetch" : 0,
 "task_max_waiting_in_queue_millis" : 0,
 "active_shards_percent_as_number" : 100.0
}
```

Workbench Installation - Linux - Primary Node

The Workbench installation files will be contained in the Genesys My Portal obtained downloaded compressed file.

Review this link for details on downloading Workbench: Downloading Workbench

Important

1. Workbench requires the installation of a Primary Node at each and every Data-Center.
2. The Workbench Primary Node must be installed prior to installing Workbench Additional Nodes.
3. Workbench ships with its own pre-bundled Java distribution, OpenJDK11; all Workbench components will be configured through the installation to use this Java distribution and should not affect any other components that may be installed on the host.
4. The Workbench installation uses the Ant Installer component, if during the Workbench installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.
5. **Use a non root account** with sudo permissions when running the Workbench **install.sh** file.
6. If the Workbench installation is cancelled mid completion, please ensure the Workbench install directory is cleaned/purged **prior** to attempting another install

Warning

- When installing Workbench on Linux ensure you **use a non root account** with sudo permissions for all the commands below - **DO NOT USE THE <ROOT> ACCOUNT**.

Warning

- Workbench uses the Hostname for component configuration

- Please ensure hostname resolution between Workbench and Engage Hosts is accurate and robust
- If the Workbench Hosts have multiple NIC's, please ensure the Hostname resolves to the desired IP Address prior to Workbench installation

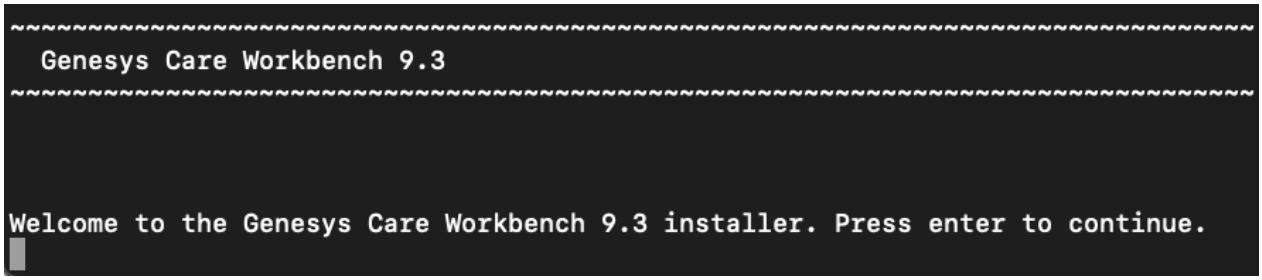
Please use the following steps to install Workbench **9.x.xxx.xx** on Linux:

1. Run **tar zxf Workbench_9.x.xxx.xx_LINUX.tar.gz** to extract the downloaded *Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz* compressed file.
2. Navigate into the **ip\linux** folder.
3. Run **tar zxf Workbench_9.x.xxx.xx_Installer_Linux.tar.gz** - to extract the *Workbench_9.x.xxx.xx_linux.tar.gz* compressed tar file.

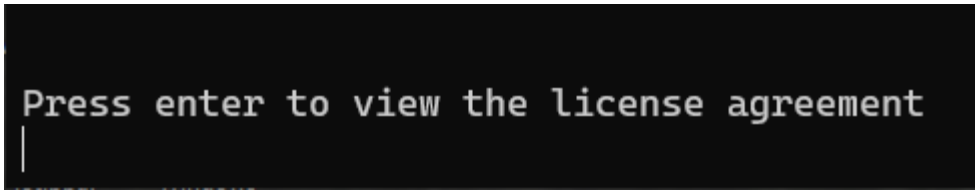
> **Warning**
>
> - **For the next command please ensure you do not prefix with sudo**

4. Run **./install.sh** (**DO NOT** prefix *./install.sh* with *sudo*)

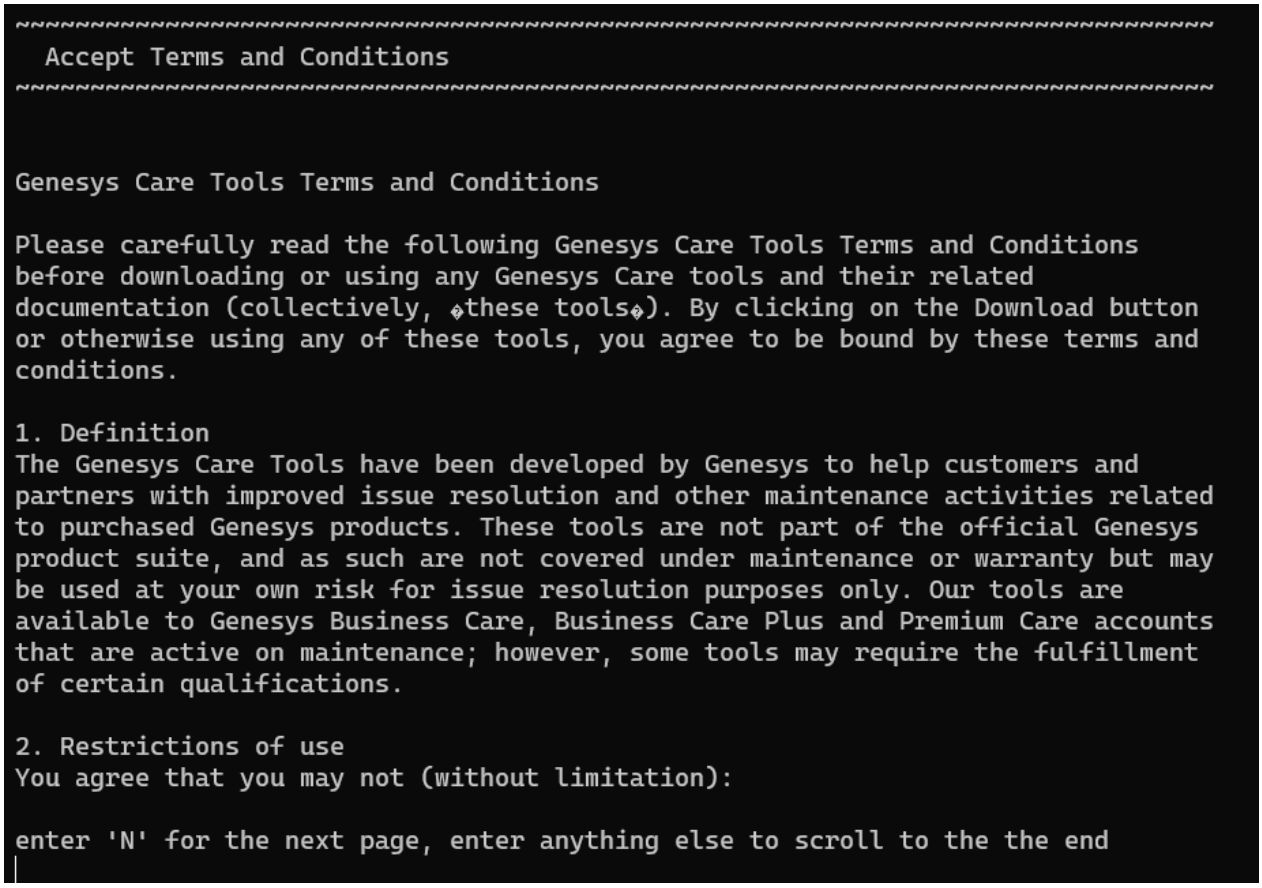
5. Genesys Care Workbench - Installation
   - Press **Enter** on the **Genesys Care Workbench 9.x** screen to start the Workbench installation.



6. Genesys Workbench license agreement.
   - Press **Enter** to view the Genesys Workbench license agreement



7. Review license agreement
   - Enter **N** for the next page, or press anything else to scroll to the end of the Terms and Conditions



8. Genesys Workbench **Terms and Conditions**
   - If you agree to the Genesys Workbench Terms and Conditions, press **Enter** (default=Y) or enter **Y** to continue.

```
YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE GENESYS CARE TOOLS IS AT
YOUR SOLE RISK.  THE GENESYS CARE TOOLS ARE PROVIDED ⁄AS IS⁄ AND WITHOUT
WARRANTY OF ANY KIND.  GENESYS EXPRESSLY DISCLAIMS ALL WARRANTIES AND/OR
CONDITIONS EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND
FITNESS FOR A PARTICULAR PURPOSE.  GENESYS DOES NOT WARRANT THAT THE USE OF THE
GENESYS CARE TOOLS WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY DEFECTS WILL
BE CORRECTED.  NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY GENESYS SHALL
CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY.  CUSTOMER
ASSUMES THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES,
SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.  THIS DISCLAIMER DOES NOT
LIMIT OR EXCLUDE ANY LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY GENESYS⁄
NEGLIGENCE.
Limitation of Liability.
GENESYS SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY
CUSTOMER OR ANY USER OF THE GENESYS CARE TOOLS.  UNDER NO CIRCUMSTANCES,
INCLUDING NEGLIGENCE, SHALL GENESYS BE LIABLE FOR ANY INCIDENTAL, SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LIMITED
GRANT OF RIGHTS.  SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL
OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Do you accept the license? Y or N   [default:Y]
```

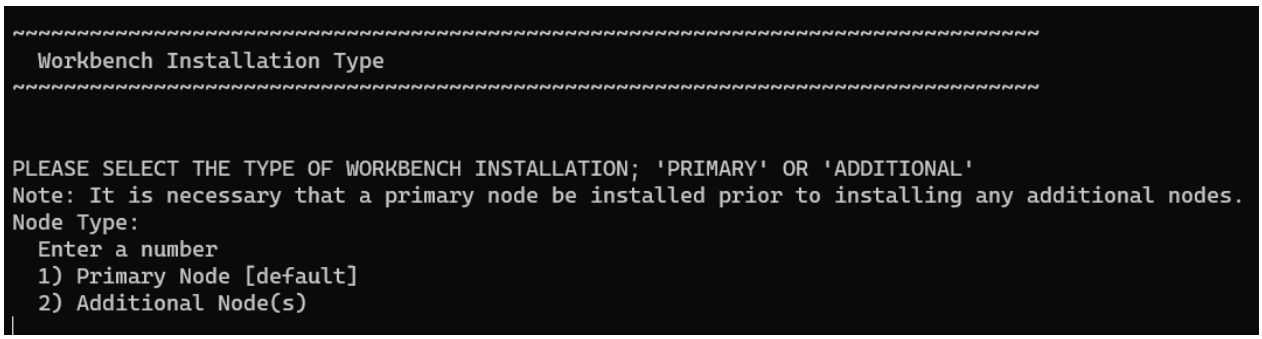
9. Workbench Installation Mode
   - There are 2 Installation Modes:
     - **New Installation** - no Workbench 9.x components are yet running on this host/node
     - **Upgrade** - you already have Workbench 9.x components running on this host/node and wish to upgrade
   - Press **Enter** or enter **1** for **New Installation** given this is a new Workbench Primary Node installation and not an upgrade.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Workbench Installation Mode
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE SELECT THE TYPE OF WORKBENCH INSTALLATION MODE, 'NEW INSTALL' OR 'UPGRADE'
Note: only select Upgrade if you already have a previous release of Workbench running on this host
Install Mode:
  Enter a number
  1) New Installation [default]
  2) Upgrade
```

10. Workbench Installation Type

- There are 2 Installation Types:
  - **Primary Node** - there are currently no Workbench components running on this host/node
  - **Additional Node** - you're installing additional Workbench components on this host/node to form a Workbench Cluster
- Press **Enter** or enter **1** for **Primary Node**, given this is a Workbench Primary Node installation and not an Additional node.

> **Important**
>
> - The Workbench Primary Node installation must/will include ALL of the Workbench components below:
>   - Workbench IO
>   - Workbench Agent
>   - Workbench Elasticsearch
>   - Workbench Kibana
>   - Workbench Logstash
>   - Workbench Heartbeat
>   - Workbench ZooKeeper
> - Therefore if/when **Primary Node** is selected, ALL mandatory Workbench Primary components above will be installed on the host.



11. **DEFAULT** or **CUSTOM** installation
    - Install Workbench with Default or Custom settings:
      - **Default** - the respective Workbench components **Default** settings will be used.
        - default settings being binaries, paths, config, ports etc
      - **Custom** - or, if required, you can change the default settings by selecting a **Custom** install.

- In the example below, **1** was entered for the **Default** installation; the respective Workbench component **default** (including binaries, paths, config, ports etc) settings will be used.

```
PLEASE SELECT EITHER A 'DEFAULT' OR 'CUSTOM' INSTALLATION TYPE.
Note: Default will use pre-configured settings. With Custom you can modify the default paths,
ports, etc. settings.
Settings Type:
  Enter a number
  1) Default [default]
  2) Custom
```

Or, if required, Enter **2** for Custom; to allow modification of the default settings (paths, config, ports etc) via multiple component screens

12. Workbench **DATA-CENTER** name

- Workbench Data-Centers are a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes
  - Enter the **Data-Center name** for this Workbench node (i.e. "EMEA", "LATAM", "Chicago" - do NOT use "default")
    - Note: The Data-Center name is **case-sensitive**, limited to a maximum of **10**, Alphanumeric and underscore characters only.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Base Workbench Properties
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE PROVIDE A DATA-CENTER (SITE) NAME THAT IS ASSOCIATED WITH WORKBENCH INSTALLATION
Note: This Data-Center name will be used to categorize the respective Hosts, Applications and ingested data
for event distribution, visualizaion context and filtering purposes
Data Center Name:   [default:]
EMEA
```

> **Important**
>
> - Workbench Data-Centers is a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes
> - Each Workbench host, and the respective applications within that host, are assigned to a Data-Center, this is mandatory

13. Workbench Base Properties - Installation Path
    - The destination installation path to which the Workbench components will be copied
        - Enter the Workbench component **installation path** (press Enter to accept the default of **/opt/Genesys/Workbench_9.1.000.00**)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Base Workbench Properties
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE PROVIDE THE WORKBENCH INSTALLATION FOLDER LOCATION.
Note: All Workbench components will be installed relative to this location.
Workbench Home Location:   [default:/opt/Genesys/Workbench_9.3.000.00]
```

14. Workbench Base Properties - Hostname
    - The Hostname of the machine is displayed for reference

```
Hostname: cc-app-dev-demo-1
Note: This Hostname will be utilized by the Workbench solution components.
```

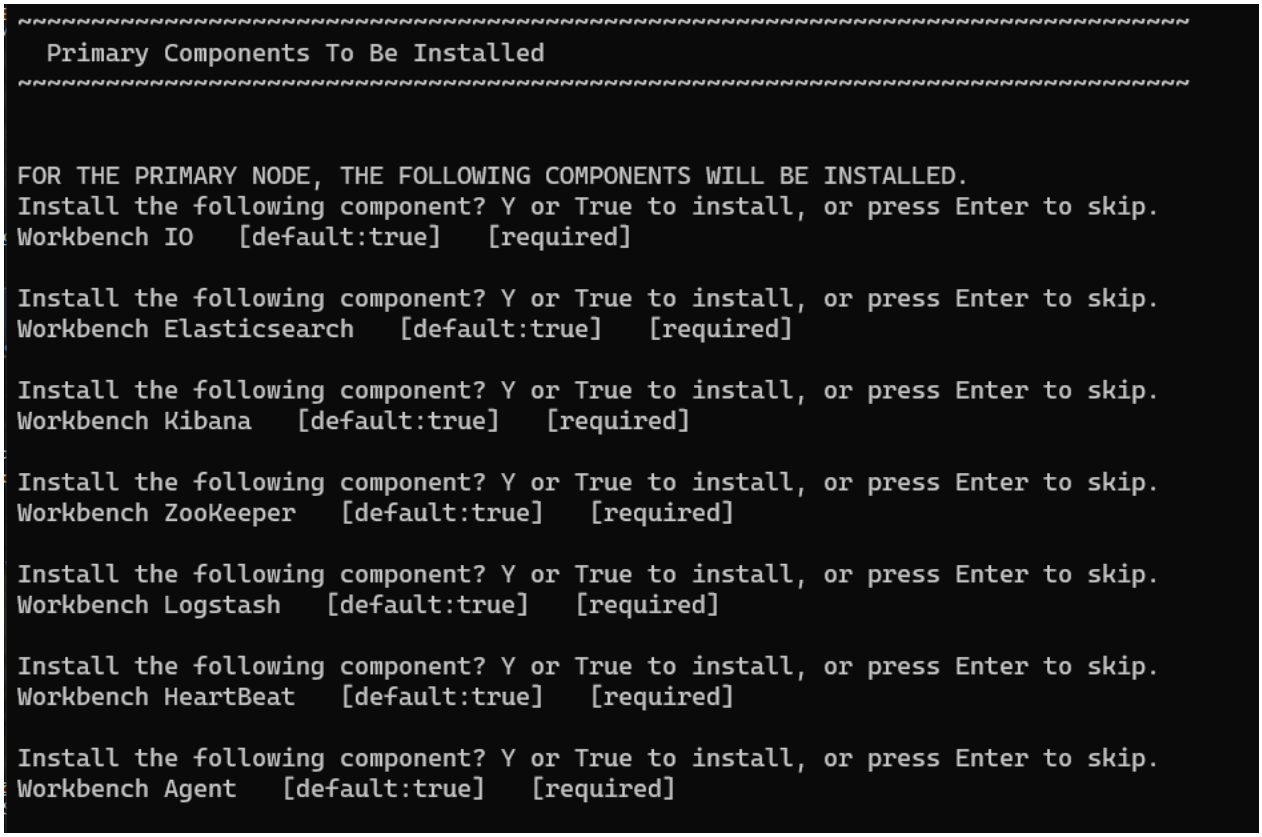
15. Workbench Base Properties - Number of Elasticsearch Nodes
    - The number of Workbench Elasticsearch Nodes to use for this deployment
        - Enter the Total **Number of Workbench Elasticsearch Nodes** for this Data-Center (press Enter to accept the default of **3**, which is correct even if you are deploying a single node)

```
PLEASE PROVIDE THE NUMBER OF WORKBENCH ELASTICSEARCH NODES.
Note: Refer to the section on Sizing of the Workbench 9.0 User Guide for recommendations
based on expected volume of data.
Total ElasticSearch nodes?   [default:3]
```

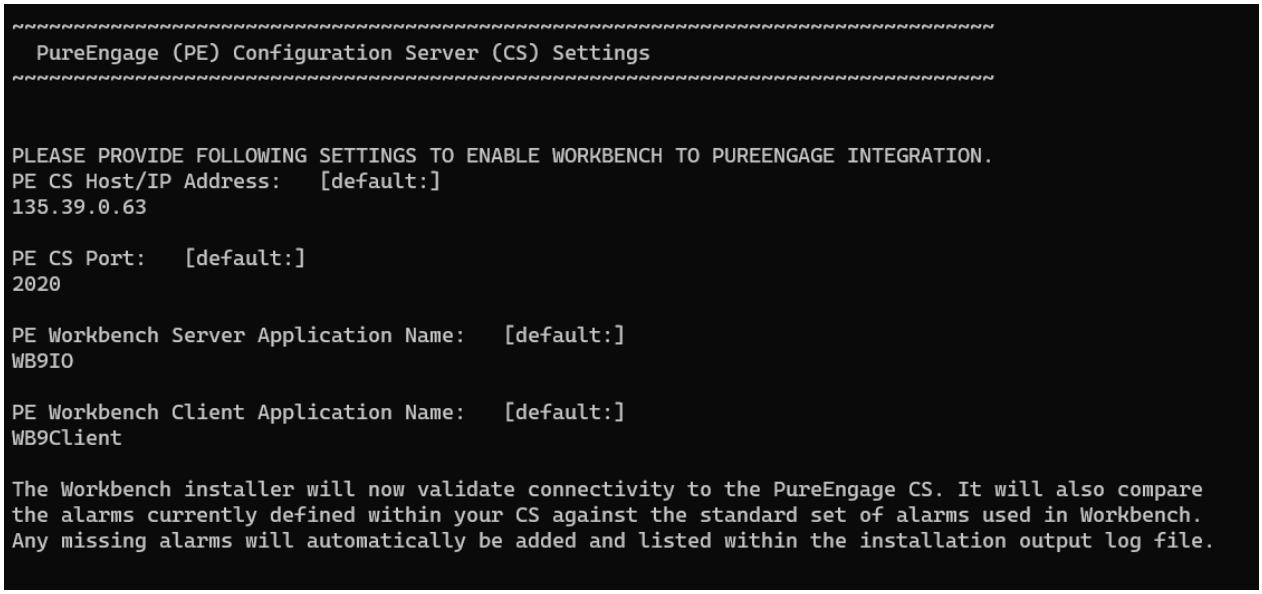
Important

The Elasticsearch component is bundled with Workbench and is used to store all of the ingested data related to Workbench. An instance of Elasticsearch is installed through the Workbench Primary Node installation; For other, HA node instances, you can use the Workbench installer and proceed through the Workbench Additional Node(s) installation.

16. Components to be Installed
    - Information on which Workbench components are being installed on this host/node



17. PureEngage Configuration Server Hostname/IP, Port and Workbench IO/Client application objects
    - The Engage settings to which this Workbench node will integrate too
    - Enter the:
        - Genesys Engage Configuration Server Hostname/IP address
        - Genesys Engage Configuration Server Port (i.e. 2020)
        - Genesys Engage Workbench Server Application Name (i.e. "WB9IO")
        - Genesys Engage Workbench Client Application Name (i.e. "WB9Client")



> **Important**
>
> The Workbench Server and Client applications must have been previously created/existing in the Genesys Engage Configuration Server; please review the Planning and Deployment\Planning section of this document for more details. From a Workbench perspective these Applications are case-sensitive therefore please verify case/spelling.

18. PureEngage Settings - Solution Control Server (SCS) and Message Server (MS)
    - The Engage SCS and MS settings to which this Workbench node will integrate too
      - Enter the corresponding number relevant to Genesys Engage SCS and MS applications for Workbench to connect to based on the associated Configuration Server previously supplied.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  PureEngage Solution Control Server and Message Server Settings
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE SELECT THE RESPECTIVE PUREENGAGE SOLUTION CONTROL SERVER (SCS) APPLICATION.
Note: This SCS application is used by Workbench to ingest/clear PureEngage alarm events.
SCS Application:
  view available options
  1) sjo_scs_a
  2) frm_scs_a
  3) bne_scs_a
  4) spo_scs_a
  5) man_scs_a
  Enter a number
2

PLEASE SELECT THE RESPECTIVE PUREENGAGE MESSAGE SERVER (MS) APPLICATION.
Note: This MS application is used by Workbench to process metadata relating to configuration.
changes.
Message Server Application:
  view available options
  1) sjo_msgserver_a
  2) frm_msgserver_a
  3) bne_msgserver_a
  4) frm_msgserver_scs_a
  5) spo_msgserver_a
  6) man_msgserver_a
  Enter a number
2
```

19. Installation Progress
    - The progress of the Workbench installation

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Installation progress
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

20. Installation Complete
    - The completion of the Workbench installation

```
BUILD SUCCESSFUL
Total time: 4 minutes 23 seconds
Finished
```

Initial Workbench Login - Linux

Navigate to **http://<WORKBENCH_HOST>:8181** to login (Engage CME credentials) to Workbench.

On initial Workbench login you'll be presented with the Workbench "Home Dashboard".

> ### Tip
>
> - The <WORKBENCH_PORT> (default 8181) can be changed via the Custom installation.

Workbench Primary Node/Host - Linux Services

The Workbench Primary node/host will contain the following Linux Services:

- WB_Agent_9.x.xxx.xx
- WB_Elasticsearch_9.x.xxx.xx
- WB_Heartbeat_9.x.xxx.xx
- WB_Kibana_9.x.xxx.xx
- WB_Logstash_9.x.xxx.xx
- WB_Metricbeat_9.x.xxx.xx
- WB_ZooKeeper_9.x.xxx.xx

As an example, executing **sudo service --status-all | grep WB** would yield:

Status of WB_Agent_9.x.xxx.xx ...
WB_Agent_9.x.xxx.xx is running
Status of WB_Elasticsearch_9.x.xxx.xx ...
WB_Elasticsearch_9.x.xxx.xx is running
Status of WB_Heartbeat_9.x.xxx.xx ...
WB_Heartbeat_9.x.xxx.xx is running
WB_IO_9.x.xxx.xx is running (3195).
Status of WB_Kibana_9.x.xxx.xx ...
WB_Kibana_9.x.xxx.xx is running
Status of WB_Logstash_9.x.xxx.xx ...
WB_Logstash_9.x.xxx.xx is running

```
Status of WB_Metricbeat_9.x.xxx.xx ...
WB_Metricbeat_9.x.xxx.xx is running
Status of WB_ZooKeeper_9.x.xxx.xx ...
WB_ZooKeeper_9.x.xxx.xx is running
```

Stopping/Starting Workbench

To stop Workbench, stop the Workbench Services in this order:

- WB_IO_9.x.xxx.xx
- WB_Kibana_9.x.xxx.xx
- WB_Metricbeat_9.x.xxx.xx
- WB_Elasticsearch_9.x.xxx.xx
- WB_ZooKeeper_9.x.xxx.xx
- WB_Agent_9.x.xxx.xx
- WB_Logstash_9.x.xxx.xx
- WB_Heartbeat_9.x.xxx.xx

To start Workbench, start the Workbench Services in this order.

- WB_IO_9.x.xxx.xx
- WB_Elasticsearch_9.x.xxx.xx
- WB_ZooKeeper_9.x.xxx.xx
- WB_Kibana_9.x.xxx.xx
- WB_Logstash_9.x.xxx.xx
- WB_Metricbeat_9.x.xxx.xx
- WB_Agent_9.x.xxx.xx
- WB_Heartbeat_9.x.xxx.xx

Workbench Installation - Linux - Additional Node

As per the Sizing section, if Workbench data and configuration redundancy and service high availability is required, Genesys recommends a 3 (Multi/Cluster) Node/Host Workbench deployment.

Warning

1. Before commencing these Additional Node instructions, ensure the **Workbench Primary Node** has been **successfully** installed
2. Workbench only supports a 1 or 3+ (odd increments) Node architecture; deploying only a Workbench Primary and Workbench Node 2 architecture will cause future upgrade issues

Warning

- **Use a non root account** with sudo permissions for all the commands below - **DO NOT USE THE <ROOT> ACCOUNT**.

Workbench Additional Node - Installation

Please use the following steps to install Workbench Additional Nodes on Linux Operating Systems

1. On the respective **2nd Workbench Additional Node/Host**
2. Run **tar zxf Workbench_9.x.xxx.xx_LINUX.tar.gz** to extract the downloaded *Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz* compressed file.
3. Navigate into the **ip\linux** folder.
4. Run **tar zxf Workbench_9.x.xxx.xx_Installer_Linux.tar.gz** - to extract the *Workbench_9.x.xxx.xx_linux.tar.gz* compressed tar file.
5. Run the command **./install.sh** (DO NOT prefix *./install.sh* with *sudo*)
6. On the **Genesys Care Workbench 9.x**

    1. Press **Enter** to continue.

7. License Agreement
    1. Press **Enter** to view the Term’s & Conditions

8. Review the Term’s & Conditions/License Agreement
    1. Press **Enter** to **scroll to the end**
    2. Or press **N** and **Enter** to review on a page-by-page basis
    3. Press **Enter** (default=Y) to accept the T&C's/license agreement and continue with the installation if you agree to the T&C's,

9. On the **Installation Mode** screen
    1. Press **Enter** for **New Installation** (default)

10. On the **Installation Type** screen
    1. Press **2** and **Enter** for **Additional Node**

11. On the **DEFAULT** or **CUSTOM** screen
    1. Press **Enter** to continue with the respective Workbench components **Default** settings (binaries/paths, config, ports etc)
    2. Or Press **2** and **Enter** to provide **Custom** settings (binaries/paths, config, ports etc)

12. On the **Base Workbench Properties - Workbench Home Location** screen
    1. Press **Enter** to accept the default installation path of **/opt/Genesys/Workbench_9.x.xxx.xx**
    2. Or type the new installation path (i.e. /home/genesys/gcti/WB9.x.xxx.xx)

13. On the **Base Workbench Properties - Hostname** screen
    1. Review the Hostname automatically populated by the Workbench installer

14. On the **Additional Components To Be Installed - - Workbench Elasticsearch** screen
    1. Press **[y/Y]** and **Enter** to install Workbench Elasticsearch on this host/node **or** Press **Enter** to skip (default) installation of this component

15. On the **Additional Components To Be Installed - Workbench ZooKeeper** screen
    1. Press **[y/Y]** and **Enter** to install Workbench ZooKeeper on this host/node **or** Press **Enter** to skip (default) installation of this component

16. On the **Additional Components To Be Installed - Workbench Logstash** screen
    1. Press **[y/Y]** and **Enter** to install Workbench Logstash on this host/node **or** Press **Enter** to skip (default) installation of this component

> **Important**
>
> Workbench Agent will be installed on this host/node as its a mandatory requirement for any Workbench host/node

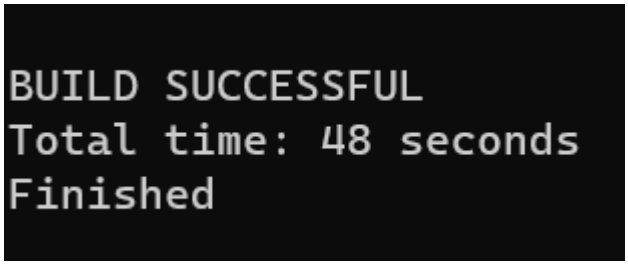
17. On the **Additional Components To Be Installed - Workbench Primary ZooKeeper IP Address/ Port** screen

> **Warning**
>
> Due to a Port validation limitation, please ensure the ZooKeeper Port is correct before pressing Enter; a race-condition could occur if not correctly entered.

    1. Type the Primary ZooKeeper IP:PORT (i.e. 10.20.30.40:2181) and press **Enter**

18. The Workbench Additional Node installation will now progress

19. The Workbench Additional Node installation is complete



Checkpoint

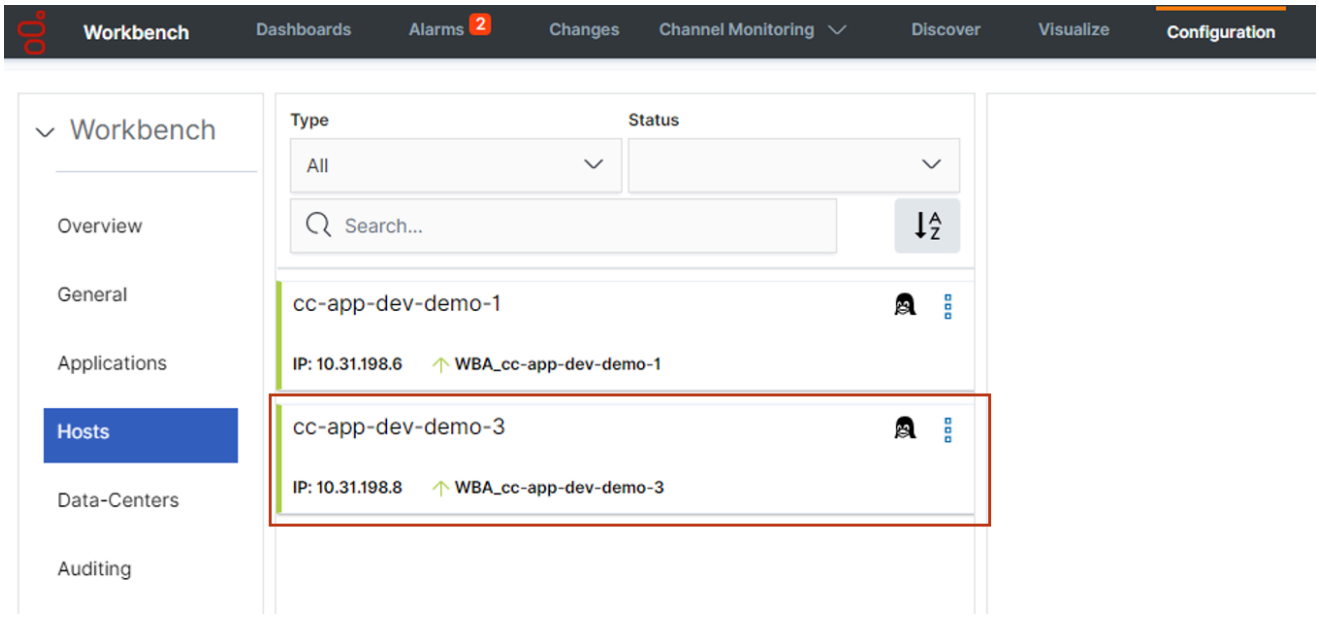
> **Important**
>
> - Based on the instructions above, within the Workbench Configuration\Hosts and Workbench Configuration\Applications menus there should now be additional Hosts and Applications
> - The number of additional Workbench Hosts and Applications will vary based on your sizing architecture and the selections you made during the installation of additional components
> - Currently additional Workbench components have been installed on their respective

Hosts, the next step is to form the Workbench Cluster which will provide HA of ingested event data (Workbench Elasticsearch) and HA of Workbench Configuration data (Workbench ZooKeeper).

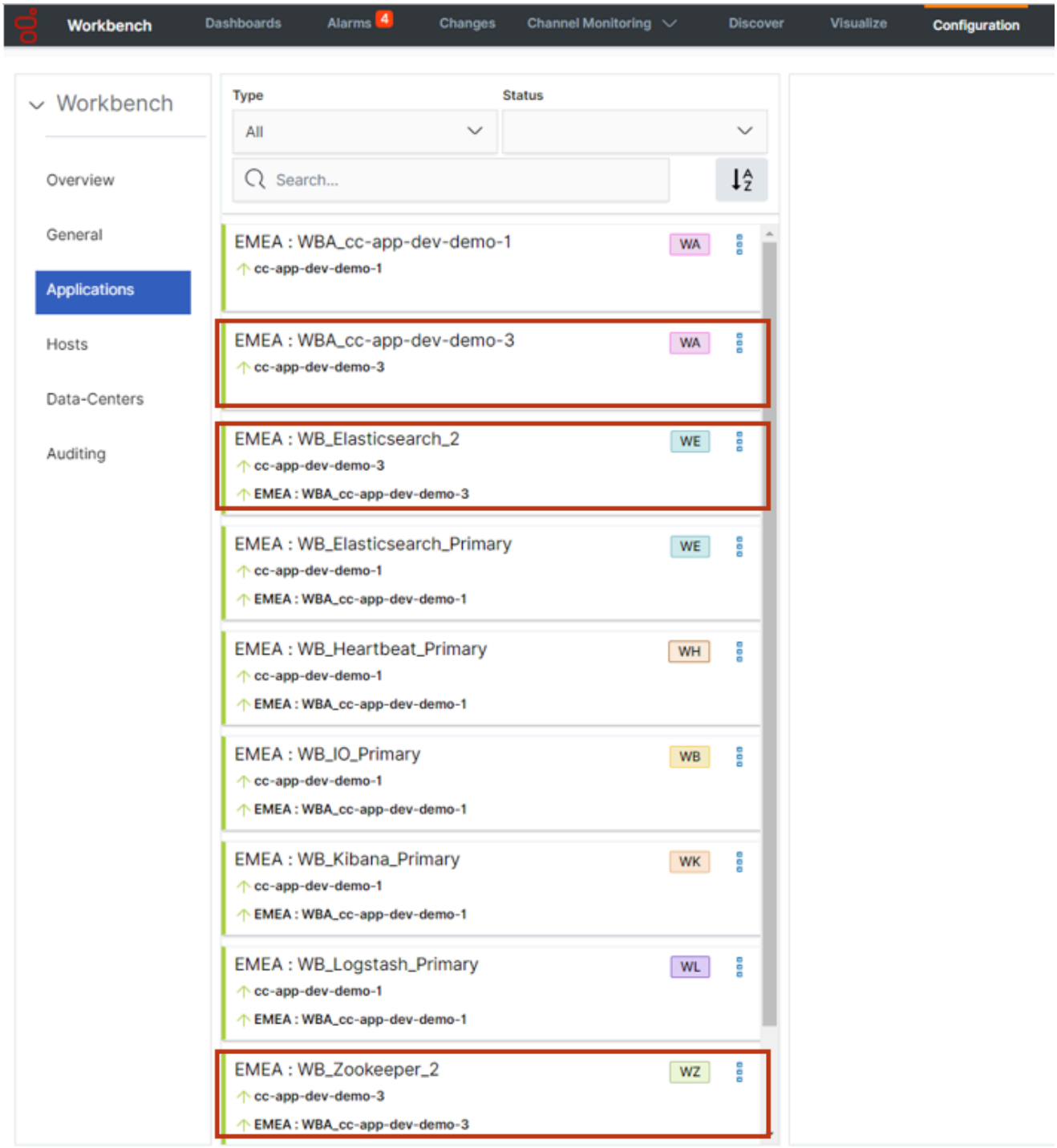
- Do not form the Workbench Cluster until all Workbench Additional Nodes have had their additional respective components installed

As an example, following the installation of Workbench Additional Node 2, the additional Hosts and Applications are highlighted below:

Hosts



Applications


Workbench
Dashboards
Alarms 4
Changes
Channel Monitoring
Discover
Visualize
Configuration
Workbench
Overview
General
Applications
Hosts
Data-Centers
Auditing
Type
All
Status
Search...
EMEA : WBA_cc-app-dev-demo-1
WA
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-3
WA
cc-app-dev-demo-3
EMEA : WB_Elasticsearch_2
WE
cc-app-dev-demo-3
EMEA : WBA_cc-app-dev-demo-3
EMEA : WB_Elasticsearch_Primary
WE
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Heartbeat_Primary
WH
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_IO_Primary
WB
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Kibana_Primary
WK
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Logstash_Primary
WL
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Zookeeper_2
WZ
cc-app-dev-demo-3
EMEA : WBA_cc-app-dev-demo-3

Workbench ZooKeeper Cluster - Configuration

Warning

- Before configuring the Workbench ZooKeeper Cluster, ensure ALL Workbench Additional Node components have been installed

Important

- Before configuring the Workbench Cluster, ensure ALL Workbench Agent and Workbench ZooKeeper components are Up (Green)
- For the Workbench ZooKeeper configuration, use **IP Address:PORT** and not Hostname:Port
- Workbench ONLY supports ODD number of additional nodes (i.e. 1, 3, 5 etc) within a Workbench Cluster architecture
- Ensure ALL "N" Workbench Additional Nodes are installed/configured before forming the final Workbench Cluster
- Workbench does not support scaling post Workbench Cluster formation
  - For example, if you form a 3 Node Workbench ZooKeeper Cluster, you cannot increase to a 5 Node ZooKeeper Cluster - as such please ensure your Workbench planning and sizing is accurate before completing your Workbench ZooKeeper Cluster formation, else a reinstall may be required

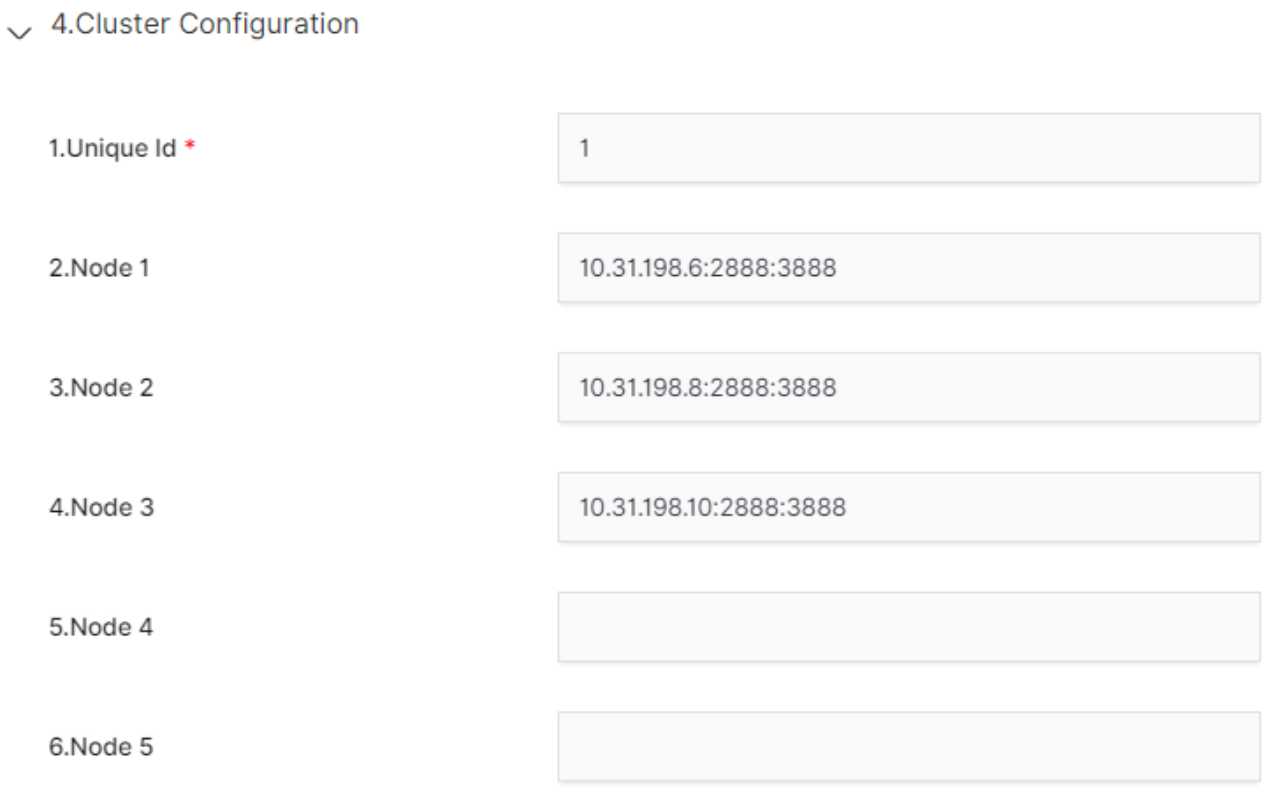
1. Navigate to the **Primary ZooKeeper** application, i.e. **EMEA : WB_ZooKeeper_Primary**
   1. Expand Configuration Section **4.Cluster Configuration**
   2. In the **Node 1** field enter the Primary Workbench ZooKeeper Hostname **<IPAddress>:2888:3888**
   3. In the **Node 2** field enter the Workbench Additional ZooKeeper Node 2 Hostname **<IPAddress>:2888:3888**
   4. In the **Node 3** field enter the Workbench Additional ZooKeeper Node 3 Hostname **<IPAddress>:2888:3888**
   5. Click **Save**

Important

- Wait for 3 minutes and refresh (F5) the Chrome Browser

- Workbench 9 should now have a Workbench ZooKeeper clustered environment providing HA of Workbench Configuration

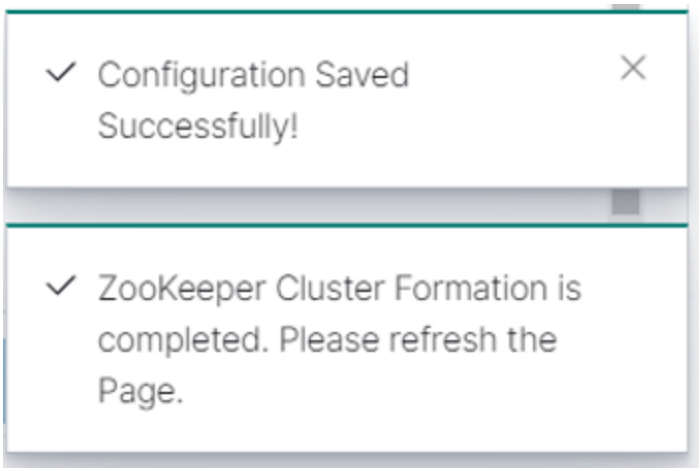
An example Workbench Cluster Configuration being:



Warning

- Workbench ZooKeeper Cluster supports a maximum of 5 Nodes

After clicking **Save** the ZooKeeper Cluster formation process will progress and complete:



Workbench Elasticsearch Cluster - Configuration

Warning

- Before configuring the Workbench Elasticsearch Cluster, ensure ALL Workbench Additional Node components have been installed

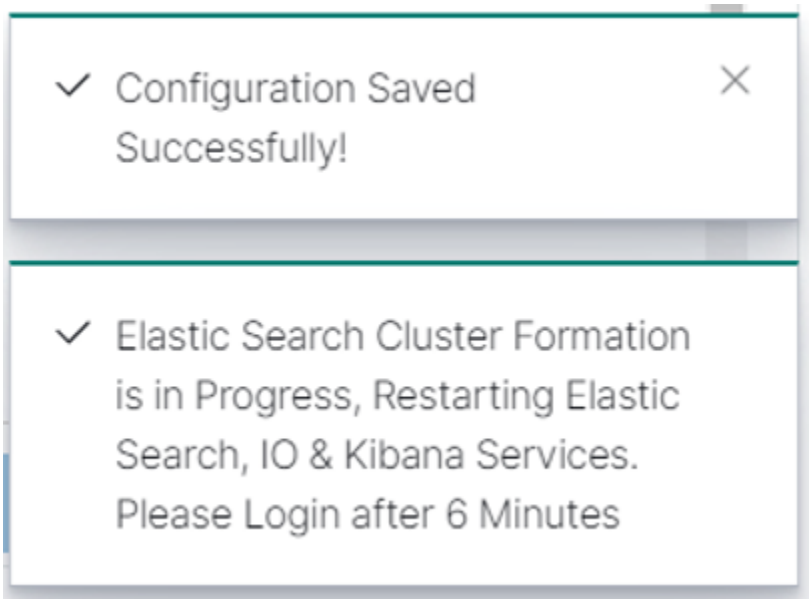
Important

- Before configuring the Workbench Cluster, ensure ALL Workbench Agent and Workbench Elasticsearch components are Up (Green)
- Fully Qualified Domain Name (FQDN) is NOT supported - either use **Hostname** or **IP Address** and not FQDN
- Workbench ONLY supports odd number of additional nodes (i.e. 1, 3, 5, 7, 9 etc) within a Cluster deployment
- Ensure ALL "N" Additional Nodes are installed before forming the final Workbench Cluster
- Workbench does not support scaling post Workbench Cluster formation
    - For example, if you form a 3 Node Workbench Elasticsearch Cluster, you cannot increase to a 5 Node Elasticsearch Cluster - as such please ensure your Workbench planning and sizing is accurate before completing your Workbench Elasticsearch Cluster formation, else a reinstall may be required

1. Navigate to the **Primary Elasticsearch** application, i.e. **EMEA : WB_Elasticsearch_Primary**
    1. Expand Configuration Section **6.Workbench Elasticsearch Discovery**
    2. In the **Discovery Host(s)** field enter the value from the associated **Section 5 - [Workbench Elasticsearch Identifiers/Network Host]** field of ALL Elasticsearch applications (i.e. WB-1,WB-2,WB-3)
    3. Click **Save**

Example configuration being:

Post clicking ''Save'' you will see the popup notification below:



> **Important**
>
> - Logout of Workbench (Chrome Browser session)
> - Wait for a minimum of 6 minutes for the Workbench Elasticsearch Cluster formation to complete
> - Login to Workbench
> - Workbench 9 should now have a Workbench Elasticsearch Clustered environment providing HA of Workbench ingested event data

Test Health of Workbench Elasticsearch Cluster Status

Check the health status of the Workbench Elasticsearch Cluster:

In a Chrome Browser navigate to:

http://<WB-VM-X>:9200/_cluster/health?pretty

or

1. Or using Windows Powershell curl
    1. Execute **curl -Uri "<WB-VM-X>:9200/_cluster/health?pretty"**
2. or using Linux CURL
    1. Execute **curl "http://<WB-VM-X>:9200/_cluster/health?pretty"**

Where <WB-VM-X> is the **Workbench Primary**, **Node 2** or **Node 3** Host.

Elasticsearch Cluster health should be reporting **Green**.

Typical expected output:

{

```
"cluster_name" : "GEN-WB-Cluster",
"status" : "green",
"timed_out" : false,
"number_of_nodes" : 3,
"number_of_data_nodes" : 3,
"active_primary_shards" : 29,
"active_shards" : 58,
"relocating_shards" : 0,
"initializing_shards" : 0,
```

```
 "unassigned_shards" : 0,
 "delayed_unassigned_shards" : 0,
 "number_of_pending_tasks" : 0,
 "number_of_in_flight_fetch" : 0,
 "task_max_waiting_in_queue_millis" : 0,
 "active_shards_percent_as_number" : 100.0

}
```

Workbench Agent Remote [WAR] (for non Workbench Hosts)

Workbench 9.1 adds a Metric data ingestion feature that enables observability of host and process CPU, Memory, Disk and Network metric data, providing rich insights and analysis capability into host and process metric utilization, performance and trends.

For example, the **Workbench Agent Remote** component can be deployed on Engage hosts, for example, SIP/URS/STAT or Framework (CS, SCS, MS, DBS etc) Genesys Application Hosts.

Overview

With the **Workbench Agent Remote** (WAR) installed on a **Remote Host (non Workbench)**, it's main function is to send Host and Process Metric event data to the local Data-Center Workbench instance/Cluster for visibility via the Workbench Dashboards and Visualizations.

Workbench Agent Remote also has an auto-upgrade capability, therefore installing Workbench Agent Remote is a one time exercise, when new Workbench or Workbench Agent Remote versions are released, the respective Workbench Agent Remote components can be automatically upgraded; please see the section below for more details on the Workbench Agent Auto Upgrade feature.

Workbench Agent and Workbench Agent Remote

Important

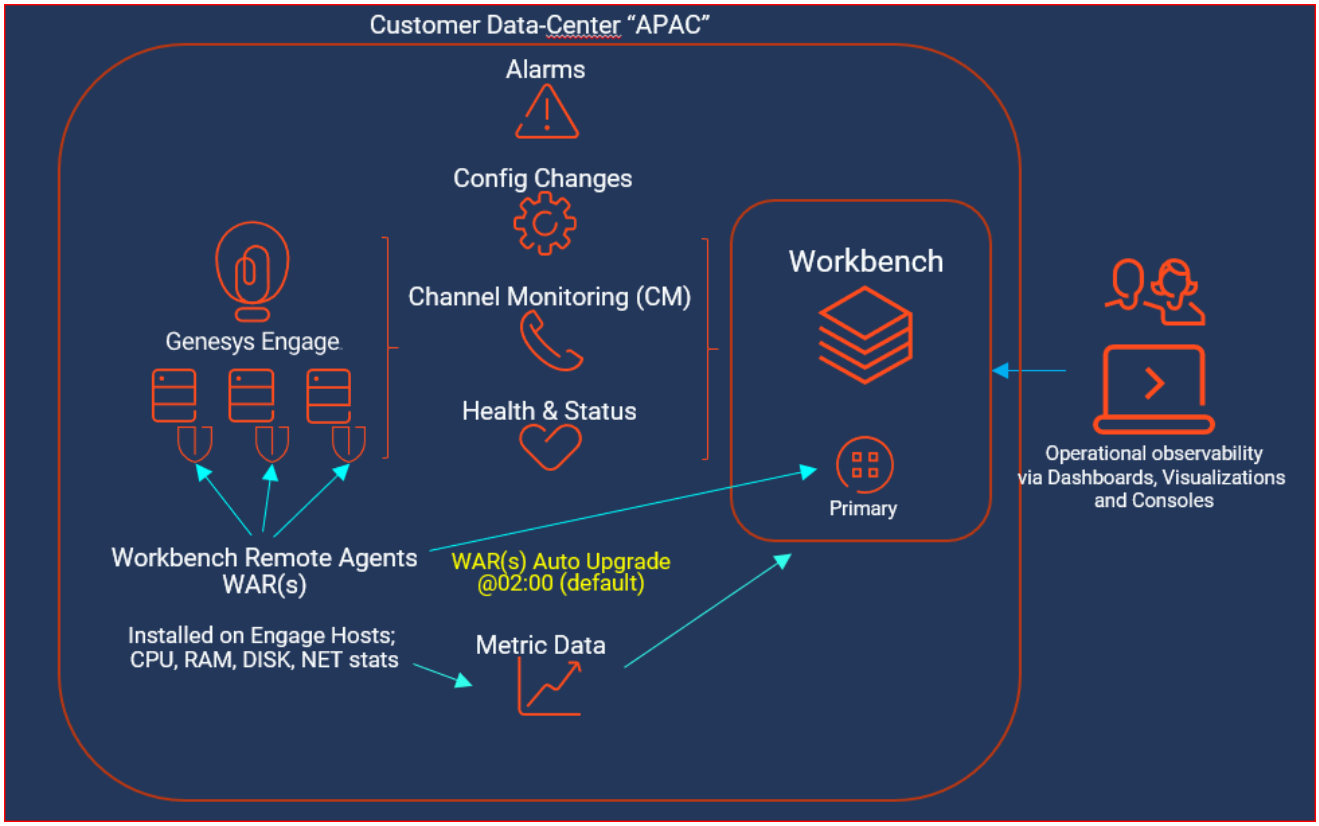
- Workbench Agent 8.5 is ONLY for LFMT
- Workbench Agent 9.x is ONLY for Workbench 9.x Hosts
- If/when Workbench and LFMT is deployed, both Workbench Agents 8.5 and 9.x would be needed on each remote host
  - The Workbench Agent 8.5 would be required for LFMT to collect log files from the remote hosts (i.e. sip, urs, gvp etc)
  - The Workbench Agent 9.x would be required for Workbench ingestion of data from the remote hosts (i.e. sip, urs, gvp etc)
- Workbench Agent Remote (WAR) 9.x is ONLY deployed on remote Genesys Hosts such as SIP, URS, GVP etc - this components sends Metric data to the Workbench 9.x Server/

Cluster

- It's recommended not to change any Workbench Agent Remote configuration from the default settings, due to a limitation that when upgrading Workbench, all the Workbench Agent Remote configuration will be reverted back to the default settings.

Architecture

Workbench Cluster with a single Engage Data-Center

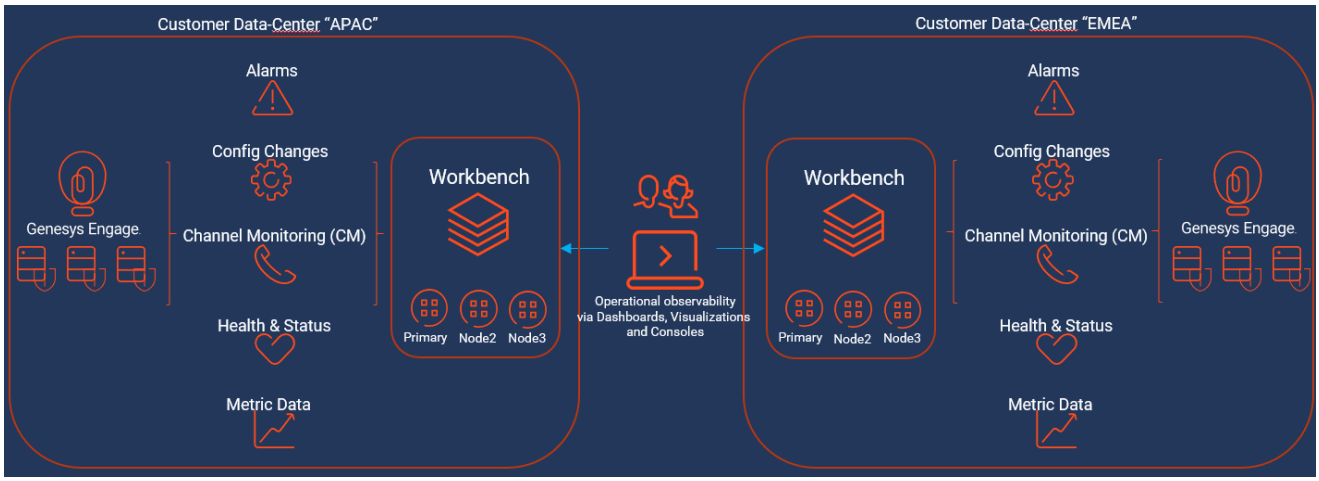


Important

- Workbench Agent Remote has an Auto-Upgrade feature, thereby the Workbench Agent

Remote is a one time install with subsequent upgrades being autonomous (upgrade check performed at 02:00 by default).

Workbench Cluster with a multi Engage Data-Center



Important

- Users can only visualize Dashboard Metric data based on the Data-Center they're logged into
- .i.e. A User logged into the APAC Workbench instance/Cluster cannot view Metric data for EMEA - they need to log into the EMEA Workbench instance/Cluster

Components - Run-time

The Workbench Agent Remote **Run-time** components consist of:

- **Workbench Agent Remote** - executable installed as a Service
  - Start a HTTP Server for WB_IO_Primary communication
  - Sends initial configuration of the Workbench Agent Remote to Workbench ZooKeeper

- Schedules an upgrade if/when an upgrade notification is received from WB_IO_Primary
- Downloads any new Workbench Agent Remote package, from WB_IO_Primary
- Validates the checksum of the downloaded package

- **Workbench Agent Metricbeat** - executable installed as a Service
  - Transmits Host and Application Metric data to the Workbench instance/Cluster
  - Metric data is visible via Workbench Dashboards and Visualizations
- **Workbench Agent Updater** - executable installed as a Service
  - Installs and starts the Metricbeat Service
  - Installs any new updates on the Workbench Agent Remote or the Metricbeat Services.
  - If the upgrade fails, a rollback to the previous version of the Workbench Agent Remote is performed.

Components - Installation

The Workbench Agent Remote **Installation** components consist of:

- **installer.exe** (Windows) / **installer** (Linux)
  - This executable file initiates the **silent** installation of the Workbench Agent Remote component on the respective remote host
- **install_config.json** (both Windows and Linux)
  - This file:
    - contains mandatory configuration used by the installer/uninstall files
    - is auto generated when the Workbench Primary Node is installed
    - can be edited - i.e. change the installation folder or ports
    - should be edited if/when certain Workbench component configuration is changed

The above components are **stored on the Workbench Primary Host/Node**, within directories:

Windows

- **<WB_HOME_FOLDER>\Karaf\resources\windows\wbagent_9.x.xxx.xx_installscripts** directory (Windows)
  - i.e. *C:\Program Files\Workbench_9.x.xxx.xx\Karaf\resources\windows\wbagent_9.x.xxx.xx_installscripts*

Linux

- **<WB_HOME_FOLDER>/Karaf/resources/linux/wbagent_9.x.xxx.xx_installscripts** directory (Linux)
  - i.e. */opt/Genesys/Workbench_9.x.xxx.xx/Karaf/resources/linux/wbagent_9.x.xxx.xx_installscripts*

Installation Pre-Requisites

Warning

- Ensure the Workbench IO application (i.e. WB_IO_Primary is up and running before running the Workbench Agent Remote installer
  - if the WB_IO_Primary application is down, the WAR components will be installed but the associated configuration will be incomplete, resulting in a need to uninstall/install
- From a firewall perspective, ensure you open the ports below on any remote Host that will be running the **Workbench Agent Remote** component.
  - For WB 9.0 to 9.2, ports **9091** and **5067**
  - For WB 9.3, ports **9091** and **6067**

Installation of Workbench Agent Remote on Windows Hosts

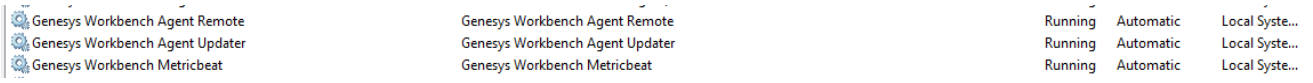
- Copy the 2 x Pre-Install **Workbench Agent Remote** Windows component files detailed above:
  - from the **<WB_HOME_FOLDER>\Karaf\resources\windows\wbagent_9.x.xxx.xx_installscripts** directory on the Workbench Primary Host/Node
  - to **C:\tmp\Workbench_Agent_Remote** (or equivalent) directory of the remote Windows Host(s) - i.e. the Genesys Engage SIP Server Host
  - **cd** to **C:\tmp\Workbench_Agent_Remote**
- Run **installer.exe** (cmd) or **.\installer.exe** (PS) as Administrator
  - The output/progress/result from running the executable can be found in **agent_install.log**

```
PS C:\tmp\Workbench_Agent_Remote> ls


    Directory: C:\tmp\Workbench_Agent_Remote


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/18/2020   9:51 PM        8527360 installer.exe
-a----        11/20/2020   1:02 PM           1270 install_config.json


PS C:\tmp\Workbench_Agent_Remote> .\installer.exe
PS C:\tmp\Workbench_Agent_Remote>
```

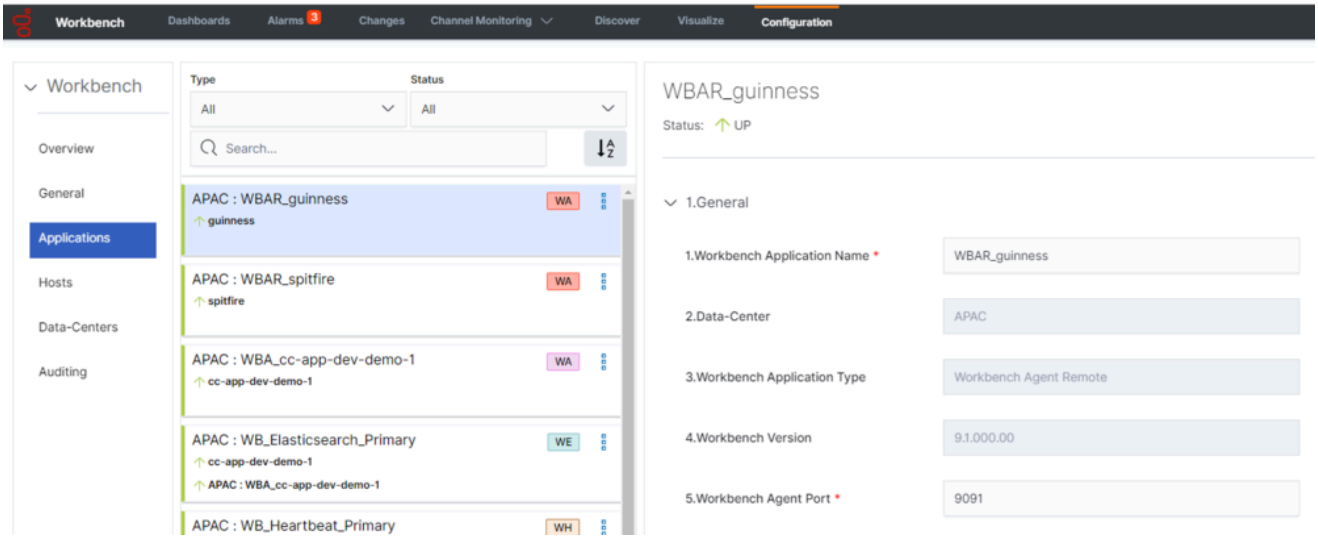
The above action has created 3 Windows Services:

- Genesys Workbench Agent Remote
- Genesys Workbench Metricbeat
- Genesys Workbench Agent Updater

> ### Warning
>
> - For each Workbench Agent Remote installation, the Heartbeat component is restarted, this will affect the status displayed of ALL Workbench components - therefore, post Workbench Agent Remote installation, please wait several minutes for the Workbench Heartbeat component to restart and status to recover.



Example of a new Workbench Agent Remote object in Workbench post installation



Installation of Workbench Agent Remote on Linux Hosts

- Copy the 2 x Pre-Install **Workbench Agent Remote** Linux component files detailed above:
  - from the **<WB_HOME_FOLDER>/Karaf/resources/linux/wbagent_9.x.xxx.xx_installscripts** directory on the Workbench Primary Host/Node
  - to the **home/genesys/tmp/Workbench_Agent_Remote** (or equivalent) directory of the remote Linux Host(s) - i.e. the Genesys Engage SIP Server Host
  - **cd** to **home/genesys/tmp/Workbench_Agent_Remote**
- Run **sudo ./installer** (as a *sudo* privileged user)

> ## Warning
>
> - Run **sudo ./installer** (as a *sudo* privileged user)

- - The output/progress/result from running the executable can be found in **agent_install.log**

```
fizz spitfire ~/tmp/Workbench_Agent_Remote 2020-11-20 13:18:34
%ll
total 11M
-rw-rw-r--. 1 fizz fizz 1.3K Nov 20 13:02 install_config.json
-rwxrwxr-x. 1 fizz fizz  11M Nov 18 21:51 installer

fizz spitfire ~/tmp/Workbench_Agent_Remote 2020-11-20 13:18:37
%sudo ./installer
[sudo] password for fizz:
```

The above action has created 3 Linux Services:

- Genesys_Workbench_Agent_Remote
- Genesys_Workbench_Agent_Updater
- Genesys_Workbench_Metricbeat

List/manage the Genesys services using:

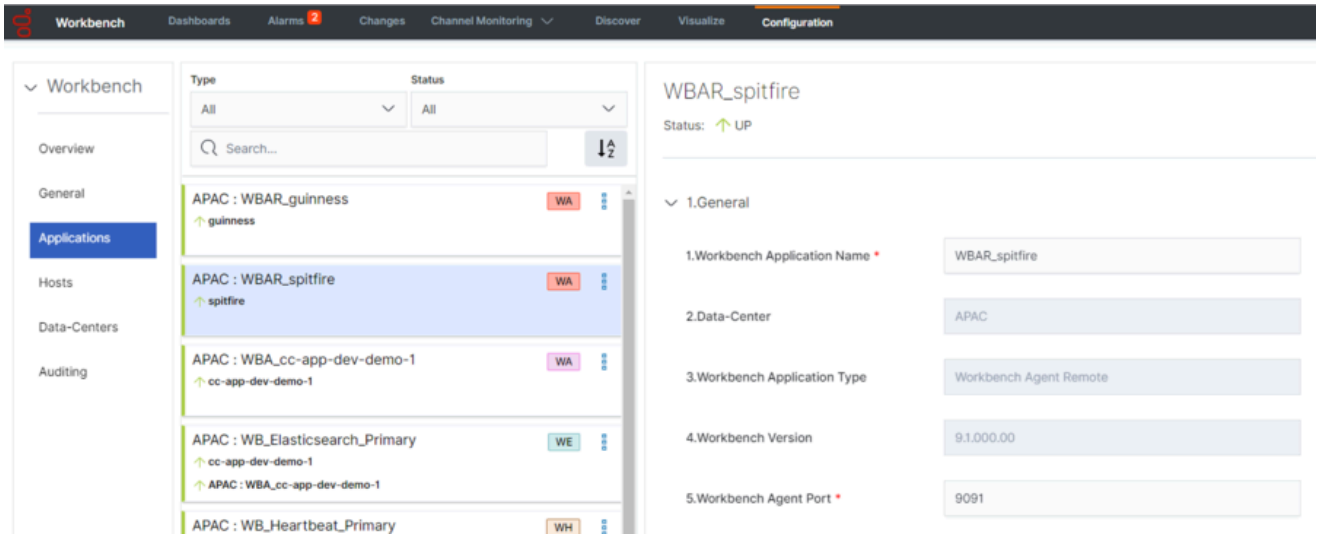
- $ systemctl list-units --type=service --state=active | grep Genesys
- $ systemctl status Genesys_Workbench_Agent_Remote
- $ systemctl stop Genesys_Workbench_Agent_Remote
- $ systemctl start Genesys_Workbench_Agent_Remote

```
%systemctl list-units --type=service --state=active | grep Genesys
Genesys_Workbench_Agent_Remote.service               loaded active running Genesys Workbench Agent Remote
Genesys_Workbench_Agent_Updater.service              loaded active running Genesys Workbench Agent Updater
Genesys_Workbench_Metricbeat.service                 loaded active running Genesys Workbench Metricbeat
```

The above Linux Services can be located in **/etc/systemd/system**

> ### Warning
>
> - For each Workbench Agent Remote installation, the Heartbeat component is restarted, this will affect the status displayed of ALL Workbench components - therefore, post Workbench Agent Remote installation, please wait several minutes for the Workbench Heartbeat component to restart and status to recover.

Example of a new Workbench Agent Remote object in Workbench post installation



Workbench Agent Remote Configuration File

The **install_config.json** contains settings required to successfully install Workbench Agent Remote on a remote Host, these settings are automatically generated during the installation of the Workbench Primary Node/Host.

See **#** comments inline regarding modifications that may be required to the **install_config.json** file.

Example **install_config.json**:

```
{
"updater" : {
"name" : "WB_Agent_Updater_9.x.xxx.xx",
"executable" : "/opt/Genesys/Workbench_9.x.xxx.xx/updater",
#change the above if a different installation path is required
"displayName" : "Genesys Workbench Agent Updater 9.x.xxx.xx",
"description" : "Genesys Workbench Agent updater service for PureEngage environments",
"arguments" : [ "-rootPath=/opt/Genesys/Workbench_9.x.xxx.xx", "-logPath=/opt/Genesys/
Workbench_9.x.xxx.xx/logs" ],
#change the above if a different installation path is required
"yamlFile" : null
},
"root_folder" : "/opt/Genesys/Workbench_9.x.xxx.xx",
#change the above if a different installation path is required
"wb_io_ip" : "GEN-WB-1",
"wb_io_port" : "8181",
# change if the Workbench IO is changed from the default 8181
"wb_io_https_port" : "8181",
#change the above if the Workbench IO is changed from the default 8181
```

```
"logstash_host" : "GEN-WB-1",
"logstash_port" : "5048",
#change the above if the Workbench Logstash is changed from the default 5048
"datacenter_name" : "APAC",
# change if the respective Data-Center is changed
"datacenter_id" : "2e048957-b9f1-463b-84bd-116cdf494de2",
"update_hour" : "02:00",
#the property above should not be modified manually in the file. If needed, you can modify it
in Workbench UI, in the configuration properties of the WAR application
"zookeeper_hosts" : [ "GEN-WB-1:2181" ],
"local_http_port" : "9091",
#change the above if the Workbench Kibana is changed from the default 9091
"local_https_port" : "8443",
#change the above if the Workbench Kibana is changed from the default 8443
#the properties below should not be modified manually, doing this will cause Workbench Agent
Remote (WAR) to behave unexpectedly
"tls_server_cert_file" : "na",
"tls_server_key_file" : "na",
"tls_ca_cert_file" : "na",
"enable_tls" : false,
"enable_mutual_tls" : false,
"update_file_name" : "wbagent_9.x.xxx.xx.tar.gz",
"update_file_checksum" : "166ca35224bff0194c1d94c40e216a6ac249eca3284f92bbad39811528c95678",
"download_endpoint" : "wb/upgrade/upgrade-download",
"notify_endpoint" : "wb/upgrade/notify"
}
```

Post Installation

Validate Installation

Ensure the Workbench Agent Remote Services below are running:

- Genesys Workbench Agent Remote
- Genesys Workbench Metricbeat
- Genesys Workbench Agent Updater

If the above Services are not present, check the agent_install.log file for the highlighted terms below:

time="2020-MM-DDT13:48:34Z" level=info msg="**Available disk space meets requirements** for the agent installer" available_MB=145032 min_MB_needed=100
time="2020-MM-DDT13:48:34Z" level=info msg="**Found installation configuration file**"
time="2020-MM-DDT13:48:34Z" level=info msg="**Configuration loaded**"
time="2020-MM-DDT13:48:34Z" level=info msg="Downloading file from: http://WB-1:8181/wb/upgrade/upgrade-download?file=wbagent_9.x.xxx.xx.zip"
time="2020-MM-DDT13:48:34Z" level=info msg="Downloading file to path: C:/Program Files/Workbench_9.x.xxx.xx\\wbagent_9.x.xxx.xx.zip"
time="2020-MM-DDT13:48:34Z" level=info msg="**Downloaded compressed file successfully**"
time="2020-MM-DDT13:48:37Z" level=info msg="**Files successfully extracted**, compressed file:C:/Program Files/Workbench_9.1.000.00\\wbagent_9.x.xxx.xx.zip"
time="2020-MM-DDT13:48:37Z" level=info msg="**Creating updater service**..."
time="2020-MM-DDT13:48:37Z" level=info msg="**Done creating updater service**"

time="2020-MM-DDT13:48:37Z" level=info msg="**Installing updater service** named: Genesys Workbench Agent Updater 9.1.000.00"
time="2020-MM-DDT13:48:37Z" level=info msg="**Starting updater service**..."
time="2020-MM-DDT13:48:37Z" level=info msg="Updater service status: **RUNNING**"

Metric Data Transmission

Post installation, Workbench Agent Remote will send Metric (Host/Application CPU/RAM/DISK/NETWORK) data to the respective local Data-Center Workbench instance/Cluster

- Host Metric Data
  - Host CPU and RAM Metrics - enabled by default - cannot be disabled
  - Host Disk, Network and Uptime Metrics can be enabled/disabled
  - The default Host Metric transmit frequency to the respective Workbench instance/Cluster is 60 seconds
- Application/Process Metric Data
  - Application/Process can be transmitted based on Top 10 or Specific Process Names (i.e. "metricbeat.exe")
  - The Top 10 (CPU/RAM) Application/Process Metrics
  - Application/Process Metrics are summarised by default
  - The default Application/Process transmit frequency to the respective Workbench instance/Cluster is 60 seconds

> **Important**
>
> - Any changes to Sections **5 Host Metrics** and **6 Application Metrics** of the Workbench Agent Remote configuration does NOT required a restart of Services; the changes are dynamic

Auto Upgrade

Workbench Agent Remote has an auto-upgrade capability, therefore installing Workbench Agent Remote is a one time exercise; when new Workbench or Workbench Agent Remote versions are released, the respective Workbench Agent Remote components can be automatically upgraded based on receiving an upgrade notification from the Workbench IO application.

Each Workbench Agent Remote application installed on a remote, non Workbench host:

- will receive a notification from the Workbench IO application if/when a new Workbench Agent Remote component is available for upgrade
- has Auto Upgrade enabled by default
- checks the hash of the downloaded file to validate it matches the original upgrade notification received from Workbench IO
  - if it matches the upgrade if initiated based on the Upgrade Time value
- the upgrade on the remote Host by default will occur at **02:00** - change via **Section 3. Auto Upgrade - Upgrade Time** value if required
- the **Section 3. Auto Upgrade - Upgrade Time** value can be changed for each Workbench Agent Remote application
  - providing flexibility as to when the auto upgrade check/action will be initiated.

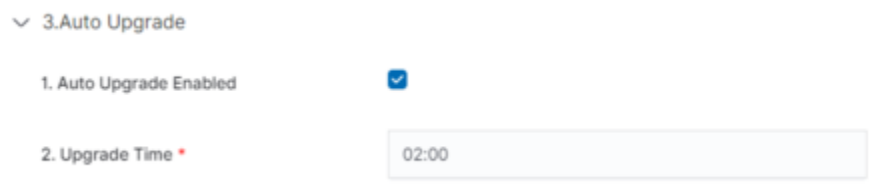
Auto Upgrade - Example Steps to upgrade the Workbench Agent Remote (WAR) Application

- In Workbench Configuration > Applications, for each of the Workbench Agent Remote (WAR) applications, set the desired upgrade time (default is 02:00).
  - The upgrade time is relative to the destination machine where WAR is installed
    - e.g. if the WB time is Eastern time-zone and WAR machine is in Pacific time-zone, the time must be in Pacific time-zone.
- Delete (archive to a different folder) any previous/existing Workbench Agent Remote (WAR) package (wgagent_9.x.xxx.xx.zip or wbagent_9.x.xxx.xx.tar.gz) files within
  - **<WB_HOME_FOLDER>/Karaf/resources/windows/data** for Windows
  - **<WB_HOME_FOLDER>/Karaf/resources/linux/data** for Linux
- Copy the new WAR package (.zip or .gz) file to
  - **<WB_HOME_FOLDER>/Karaf/resources/windows/data** for Windows
  - **<WB_HOME_FOLDER>/Karaf/resources/linux/data** for Linux
- The checksum for the new package will be calculated (this will take a few minutes)
- After the checksum is calculated, an upgrade notification is sent to Workbench Agent Remote (WAR)
- Once Workbench Agent Remote (WAR) receives the notification, it will schedule the upgrade
- The Workbench Agent Remote (WAR) upgrade will automatically occur based on the upgrade time
- The Workbench Agent Remote (WAR) Application will be automatically restarted
- The Workbench Agent Remote (WAR) will now be running the updated package

> ### Warning

- Please note that if the Upgrade Time is updated after the new WAR package is copied, the time change will take effect based on the **old** time value and not the new updated time
- Workbench upgrades starting from version 9.1 will automatically trigger the upgrade of any WAR components that existed prior to the Workbench upgrade.
- The respective Workbench Agent Remote (WAR) components, installed on hosts such as SIP, URS, GVP etc, will be upgraded based on the WAR **Upgrade Time** (default 02:00)
- For WB 9.3 the WAR [General] section **Log File Location**, **Segment** and **Expire** fields will be blank post an upgrade until the WAR **Upgrade Time** (default 02:00) is triggered and the WAR upgrade is completed

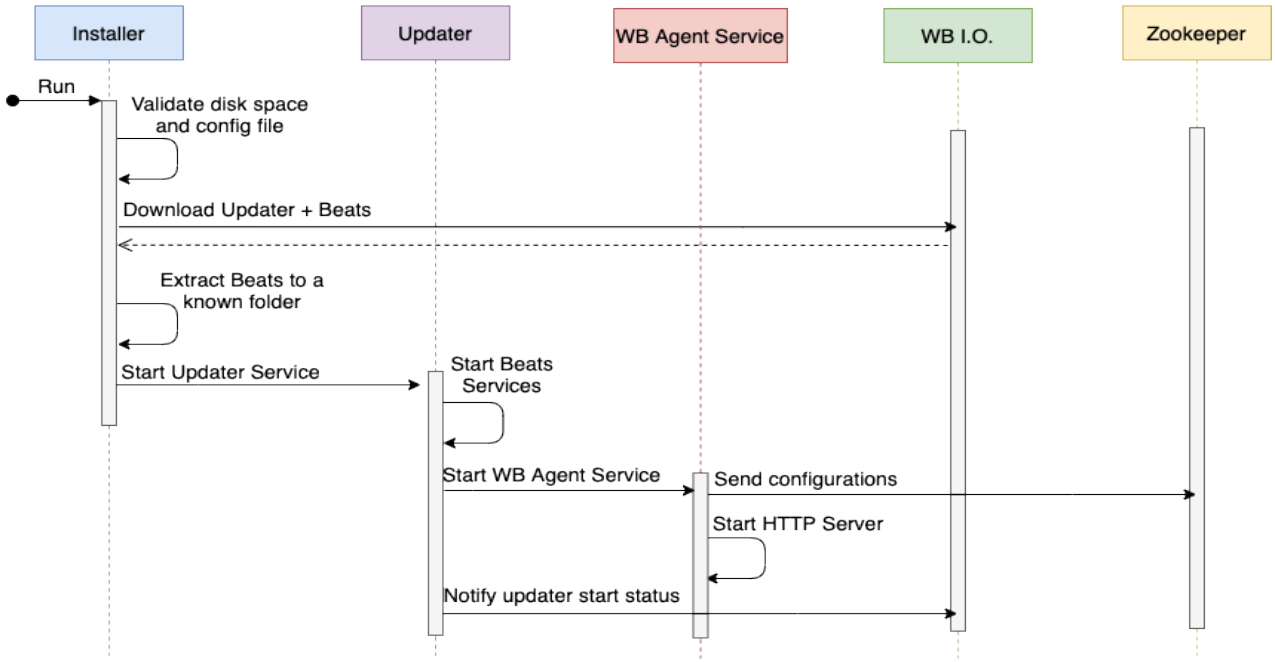
Auto Upgrade - Upgrade Time



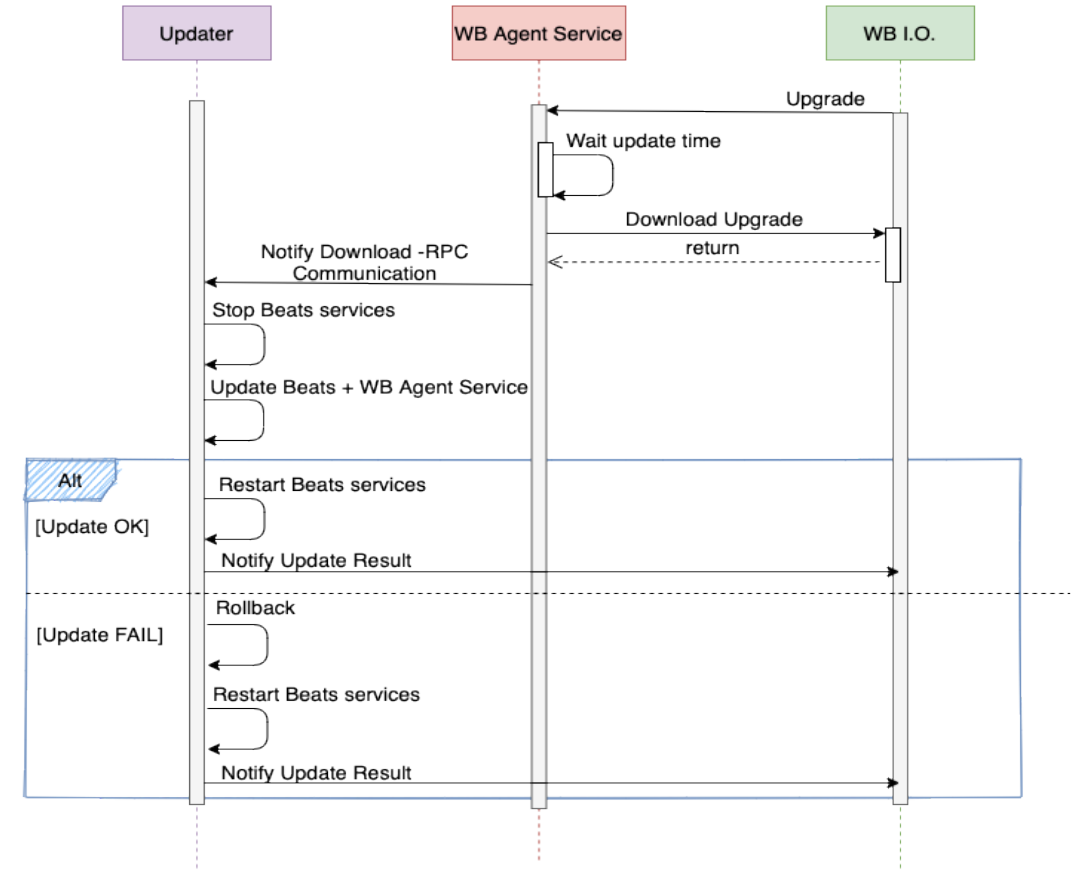
Auto Upgrade Sequence Diagrams

The diagram below details the Workbench agent Remote installation and upgrade functions:

Installation



New Update



Uninstallation - Windows Hosts

- On the respective Remote Host(s) - i.e. **UK-SIP-1**
- **cd** to **C:\Program Files\Workbench_9.x.xxx.xx** (or equivalent) directory
- Run **uninstall.exe** (cmd) or **.\uninstall.exe** (PS) as Administrator

The above action will remove the 3 x Windows Services:

- Genesys Workbench Agent Remote
- Genesys Workbench Metricbeat
- Genesys Workbench Agent Updater

An **uninstall.log** is also created detailing the uninstallation progress.

Important

- Workbench Agent Remote will no longer send Host and Application Metrics to the Workbench instance/Cluster, therefore Dashboard visualizations will not present any data for the respective host(s) that have had Workbench Agent Remote uninstalled.

Warning

- Post Workbench Agent Remote uninstall, the **uninstall.exe** and **uninstall.log** files will need manual deletion

Uninstallation - Linux Hosts

- On the respective Remote Host(s) - i.e. **UK-SIP-1**
- **cd** to **/opt/Genesys/Workbench_9.x.xxx.xx/** (or equivalent) directory
- Run **sudo ./uninstall** (as a *sudo* privileged user)

Warning

- Run **sudo ./uninstall** (as a *sudo* privileged user)

The above action will remove the 3 x Linux Services:

- Genesys_Workbench_Agent_Remote
- Genesys_Workbench_Metricbeat
- Genesys_Workbench_Agent_Updater

An **uninstall.log** is also created detailing the uninstallation progress.

Important

- Workbench Agent Remote will no longer send Host and Application Metrics to the Workbench instance/Cluster, therefore Dashboard visualizations will not present any data for the respective host(s) that have had Workbench Agent Remote uninstalled.

Warning

- Post Workbench Agent Remote uninstall, the **uninstall** and **uninstall.log** files will need manual deletion

Post Installation Configuration

Genesys recommended post installation step:

> **Important**
>
> The Workbench installation uses the Ant Installer component, if during the Workbench installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.

Uninstalling Workbench

This section details the steps to uninstall the Workbench components.

Important

- If any Workbench data is required for archival purposes, please ensure it is saved at a separate location prior to running the Workbench uninstall script(s).
- The Workbench uninstall process **permanently** removes the Workbench Services associated with all the Workbench components and **all files, including data and logs** etc.
- The uninstall process will leave the original configuration file used to generate the Workbench installation; if needed, this can be provided to Genesys Customer Care if related to an installation issue.
- The Workbench uninstallation should be done in reverse Workbench installation order.
  - If permanently removing Workbench and you no longer wish to use Workbench
    - uninstall any Workbench Agents running on remote Genesys Application Servers (i.e. SIP, URS, FWK etc).
  - Uninstall any Workbench Additional nodes
  - Uninstall the Workbench Primary node.

Windows Operating System

The following steps will allow you to **uninstall** Workbench in **Windows**.

1. Browse to the Workbench home installation folder (i.e. "C:\Program Files\Workbench_9.x.xxx.xx")
2. Open a Command/Powershell Console as an **Administrator**
3. Run **uninstall.bat** file
4. Remove any remaining files/folders from and including the Workbench "Home" installation folder
5. This completes the Workbench Linux uninstall process.

Linux Operating System

The following steps will allow you to **uninstall** Workbench on **Linux**.

1. Via a Linux Terminal, **cd** (Change Directory) to where Workbench is installed (i.e. **/opt/Genesys/Workbench_9.x.xxx.xx**).
2. Run **./uninstall.sh** as a User with **Administrator** permissions - not as "root"
3. Remove any remaining files/folders from and including the Workbench "Home" installation folder
4. This completes the Workbench Linux uninstall process.

Configuring TLS

> **Important**
>
> - TLS connections to Workbench IO and Kibana (essentially the main Workbench UI) is currently NOT supported
> - TLS connections from Workbench IO Applications at different Data-Centers is supported
> - TLS connections to Elasticsearch has to be enabled when enabling Elasticsearch Authentication
> - TLS connections to ZooKeeper is NOT supported
> - TLS connection from Workbench to Engage Configuration Server is supported
> - TLS connection from Workbench to Engage Solution Control Server is supported
> - TLS connection from Workbench to Engage Message Server is supported

Workbench TLS

Currently Workbench supports TLS connections/communication between its Workbench IO Application(s).

For example a Workbench IO Application in APAC can communicate with a Workbench IO Application in EMEA, providing secure messaging of Alarm, Changes, Channel Monitoring and Auditing events across the WAN, to enable this Workbench IO "APAC" to Workbench IO "EMEA" connection/ communication, the respective Workbench Host Objects must first be TLS Enabled.

Enable Workbench Host TLS

This section details the enablement of the Workbench Host TLS via the "2. Workbench TLS Communication" Section:

Only enable the Workbench Host TLS setting if/when:

- Workbench IO Application TLS connection/communication is preferred between Workbench IO Applications at different Data-Centers (i.e. "APAC" and "EMEA") for improved security; complete this Workbench Host TLS enablement before enabling Workbench IO Application TLS
- Workbench ElasticSearch Authentication is planned to be enabled; complete this Workbench Host TLS enablement before enabling ElasticSearch Authentication

Please follow these steps to enable the Workbench Host TLS settings:

1. Certificates need to be in a Java Key Store (.jks file) and accessible on the host by the user account running Workbench
2. Within Workbench, browse to the Configuration > Hosts section and select the host that TLS will be enabled on
3. Within the host object settings, navigate to the "2. Workbench TLS Communication" section
4. Populate the following options:
    - Keystore Path: path of the Java Key store on the host
    - Keystore Password: password for the key store
    - Truststore Path: path to the Java trust store
    - Truststore Password: password for the Java trust store
    - Protocol (default: TLSv1.2): TLS protocol that will be used
    - Algorithms: comma-delimited list of cipher suites that the host will use for TLS negotiation/ communication with other nodes
        - See the "JSSE Cipher Suite Names" section of the following doc for a valid list of cipher suites supported by Java https://docs.oracle.com/javase/10/docs/specs/security/standard-names.html
    - Mutual-TLS: check to enable mutual TLS
5. Click the save button to commit the changes

Enable Workbench IO Application TLS

This section details the enablement TLS for the Workbench IO Application

Only enable the Workbench IO Application TLS setting if/when:

- TLS connection/communication is preferred between Workbench IO Applications at different Data-Centers for improved security

Please follow these steps to enable the Workbench IO Application TLS settings:

1. Ensure that the TLS properties have been first configured for the host object that the Workbench_IO application is running on (See the above "Enable Workbench Host TLS" section)
2. Within Workbench, browse to the Configuration > Applications section and select the Workbench_IO application in the list that TLS will be enabled on
3. With the Workbench_IO application object, navigate to the "9. Workbench Distributed Mode" section
4. Check the "TLS Enabled" property
5. Click "Save" to commit the changes
6. Restart the Workbench_IO service for changes to take effect

Enable ElasticSearch Application TLS (only if enabling Elastic Authentication)

This section details the enablement of TLS for the ElasticSearch node when using Elastic authentication

Only enable the ElasticSearch Application TLS setting if/when:

- Workbench ElasticSearch Authentication is planned to be enabled
  Note: It is important to complete this ElasticSearch TLS enablement before enabling ElasticSearch Authentication

Please follow these steps to enable the Workbench IO Application TLS settings:

1. Ensure that the TLS properties have been first configured for the host object that the ElasticSearch node is running on (see the above "Enable Workbench Host TLS" section)
2. On the host in which the ElasticSearch node is running, place a copy of the key store and trust store in the following directory:
   - {WBInstallDirectory}/ElasticSearch/config
3. Within Workbench, browse to the Configuration > Applications section and select the ElasticSearch application in the list that TLS will be enabled on
4. With the ElasticSearch application object, navigate to the "8.Workbench Elasticsearch Authentication" section
5. Enable the authentication and specify the desired username and password
6. Click "Save" to commit the changes

Workbench to Engage TLS

Workbench supports TLS connections to the following Genesys Framework components:

- Configuration Server
- Message Server
- Solution Control Server

To setup/enable TLS for each of these components, please follow the Genesys Security guide at the following location to configure TLS:

Documentation/System/8.5.x/SDG/Welcome

Ensure that the certificates are installed on the Workbench Server host/VM to enable connectivity to the Framework components.

Note: For Windows VMs/Hosts ensure that the certificates are installed for both the user running the

Workbench installation as well as the LOCAL_SYSTEM account that will be running the Workbench Services.

Once the framework components and the respective hosts/VMs have been configured to use TLS, the provisioned Workbench Server application in Configuration Server will also need to be configured with the TLS properties to connect to each of the Framework components.

Instructions for setting up TLS from Workbench to the Framework:

Configuration Server

During Workbench installation, when prompted to specify the Configuration Server details, make sure to specify the auto-upgrade port that is defined for the Configuration Server instance.

Note: If Workbench was originally installed using a non-secure port of Configuration Server, the following file can be updated within the Workbench installation directory to change the port to an auto-upgrade port:

{WbInstallDir}/karaf/etc/ConfigServerInstances.cfg

Within this file, update the port for the primary Configuration Server. After the file is updated, restart the Workbench_IO to use the new Configuration Server settings.

Solution Control Server (SCS)

1) During Workbench installation you will be prompted to select the Solution Control Server instance the Workbench will connect to subscribe to framework events.

2) From within Genesys Administrator or Genesys Administrator Extension (GAX), ensure that the provisioned Workbench Server application object has a connection to both the primary and backup (if applicable) Solution Control Server and that the secure port is selected when adding these connections. Workbench will use this port when connecting to Solution Control Server.

Message Server

1) During Workbench installation you will be prompted to select the Message Server instance that Workbench will connect to subscribe to framework events.

2) From within Genesys Administrator or Genesys Administrator Extension (GAX), ensure that the provisioned Workbench Server application object has a connection to the primary and backup (if applicable) Message Servers and that the secure port is selected when configuring these connections. Workbench will use this secure port when connecting to Message Server.

Workbench Authentication

This section provides details on Workbench Authentication, specifically the back-end ZooKeeper and Elasticsearch storage to enhance security.

Workbench ZooKeeper Authentication

ZooKeeper authentication provides improved security for the back-end Workbench storage, essentially requiring a username and password to access the ZooKeeper data.

ZooKeeper authentication is not enabled by default and can be enabled through the Workbench UI post installation.

ZooKeeper handles authentication / authorization by using ACLs to specify permissions on each ZooKeeper node. Once authentication is enabled, the nodes that already exist in Zookeeper will be associated with the new user. After that, any new configuration data that is saved in ZooKeeper will be associated with the new user. In this way, only the owner can access data saved in Zookeeper and no other user can view or edit it. Disabling authentication again will disassociate the Zookeeper user from all existing data nodes and allow any user to view or edit data saved in Zookeeper.

In case a cluster of ZooKeeper nodes is desired for fault tolerance and high availability, additional nodes can be installed. If authentication has been enabled in ZooKeeper prior to installing the additional nodes, this must be first disabled. After disabling authentication, proceed with installing the additional nodes. Once the additional nodes have been installed, ZooKeeper authentication can be reenabled.

Limitations/Considerations

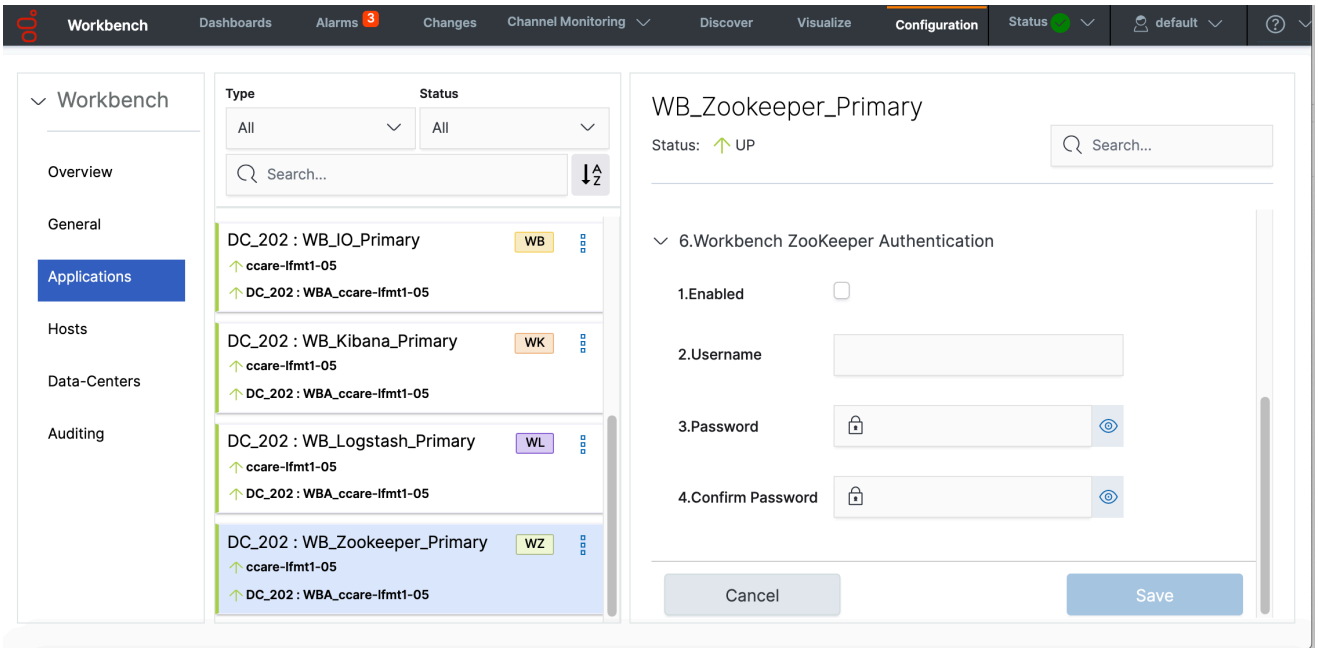
Warning

- Installing ZooKeeper "Additional" Nodes after enabling ZooKeeper Authentication is possible, but ZooKeeper Authentication should be disabled first.
  - After disabling authentication, the additional ZooKeeper nodes can be installed
  - Once the additional ZooKeeper nodes have been installed, ZooKeeper Authentication can be re-enabled
- While the Zookeeper Authentication enable/disable process is running, some data may appear inconsistent if you navigate to other pages in the application; to avoid this, please wait until the notification "Updating ZooKeeper Data is completed" appears at the bottom of the page.
- While the ZooKeeper Authentication enablement is in progress, it is recommended to **not** make any other Workbench configuration changes until the "Updating ZooKeeper Data is completed" toast pop-up is presented, which will be ~5 minutes.
- For multi Workbench Data-Center (i.e. APAC and EMEA) deployments with Workbench Cluster (Primary, Node 2, Node 3), when enabling/changing Workbench ZooKeeper username and password, please ensure you're logged into the respective Workbench Data-Center before making the change

- i.e. if you have 2 x Workbench Data-Centers (i.e. APAC and EMEA) with Workbench Cluster (Primary, Node 2, Node 3) at each Data-Center, and you wish to change the EMEA Workbench ZooKeeper username and password, please ensure you're logged into the EMEA Workbench and not the APAC Workbench

Enabling ZooKeeper Authentication

Navigate to Configuration > Applications > WB Zookeeper > 6.Workbench Zookeeper Authentication



Configure the Fields below and click 'Save':

- Enabled: Click this checkbox to enable ZooKeeper Authentication.
- Username: Provide an ZooKeeper Username (i.e. "WB_ZK") which be be used for the Authentication Username Credential
- Password: Provide an ZooKeeper Password (i.e. "my_p@ssword123") which be be used for the Authentication Username Credential
- Confirm password: Provide the ZooKeeper Password (i.e. "my_p@ssword123") again to ensure accuracy
- Click 'Save'

Workbench ZooKeeper Authentication will now be enabled.

> **Tip**
> The password fields include an eye icon button that allows you to see the plain text when entering the password

Workbench Elasticsearch Authentication

Elasticsearch authentication provides improved security for the back-end Workbench storage, essentially requiring a username and password to access the Elasticsearch data.

Elasticsearch authentication is not enabled by default and can be enabled through the Workbench UI post installation.
Elasticsearch handles authentication/authorization by using File-based user authentication. All the data about the users for the file realm is stored in two files on each node in the cluster: "users" and "users_roles". Both files are located in Elasticsearch config directory and are read on startup.

The users and users_roles files are managed locally by the node and are not managed globally by the cluster. This means that with a typical multi-node cluster, the exact same changes need to be applied on each and every node in the Workbench cluster, as such, any change from the Workbench UI will be reflected automatically in all other nodes in the cluster.

Pre-Requisites

- The customer must generate the respective Host/Server Certificates.
- TLS settings should be configured on the Workbench Hosts Objects that are running the Elasticsearch component (i.e. WB_Elasticsearch_Primary, WB_Elasticsearch.2, WB_Elasticsearch.3).
  - please review the Configurating TLS section for details on Workbench Host TLS configuration
- A copy of Host TLS Certificate must be copied to the respective Elasticsearch configuration directory (i.e. /opt/Genesys/Workbench_9.x.xxx.xx/ElasticSearch/config) in all Workbench Elasticsearch nodes.

Limitations/Considerations

Warning

- All Workbench components will be restarted post enabling Elasticsearch Authentication, therefore Workbench Application statuses will be Red/Down for up to ~3 minutes.
- Elasticsearch Authentication can be enabled either pre of post Cluster formation; configurations are sync'd automatically to the Additional Elasticsearch nodes when enabled via the Primary Elasticsearch node

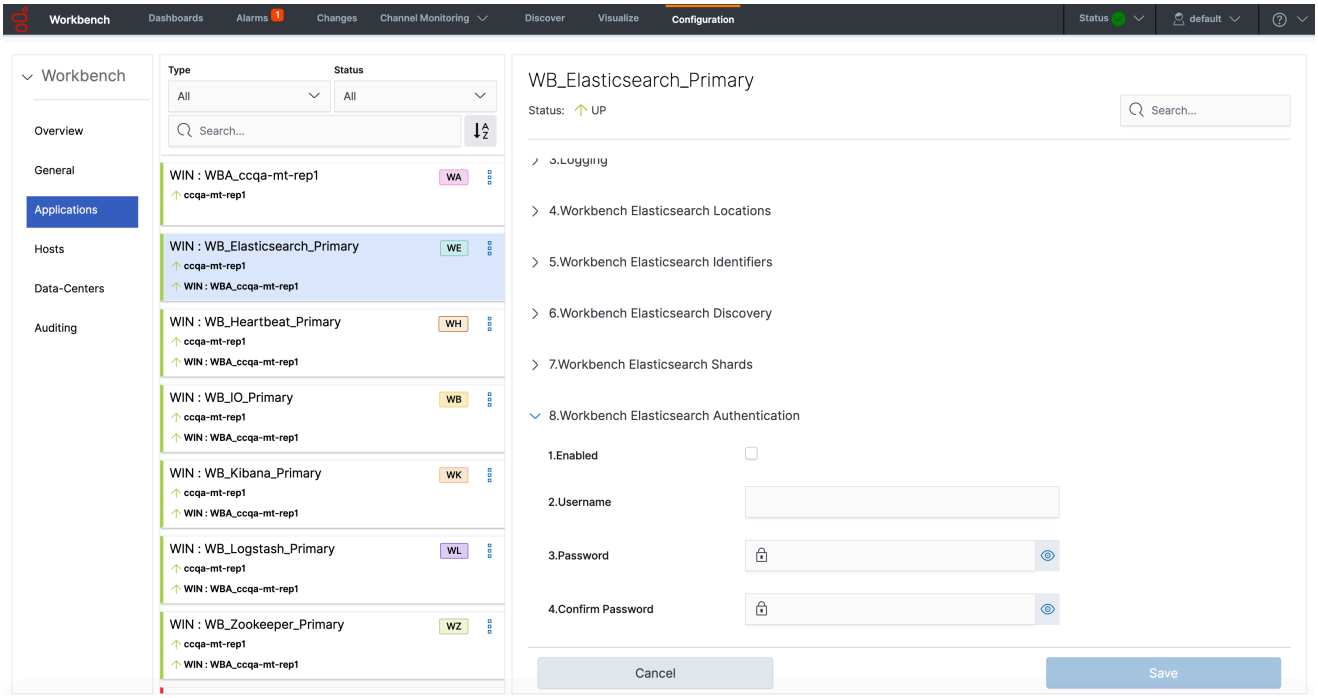
Recommended Procedure

Recommended procedure to enable Workbench Elasticsearch Authentication (Elasticsearch Cluster):

- Install all Workbench Elasticsearch nodes
- Enable TLS on each Workbench node
- Form Workbench Elasticsearch Cluster
- Enable Elasticsearch Authentication

Enabling Elasticsearch Authentication

Navigate to Configuration > Applications > WB Elasticsearch > 8.Workbench Elasticsearch Authentication



Configure the Fields below and click 'Save':

- Enabled: Click this checkbox to enable Elasticsearch Authentication.
- Username: Provide an Elasticsearch Username (i.e. "WB_ES") which be be used for the Authentication Username Credential
- Password: Provide an Elasticsearch Password (i.e. "my_p@ssword123") which be be used for the Authentication Username Credential
- Confirm password: Provide the Elasticsearch Password (i.e. "my_p@ssword123") again to ensure

accuracy

- Click 'Save'

Workbench Elasticsearch Authentication will now be enabled.
Workbench components will be restarted.
Workbench components will connect to the respective Elasticsearch component(s) using the provided credentials.
Workbench Elasticsearch Authentication can be disabled by un-checking the Enabled checkbox and clicking 'Save'.

> **Tip**
>
> The password fields include an eye icon button that allows you to see the plain text when entering the password.

Workbench Data-Center Synchronization

Overview

A Workbench **Data-Center(s)** is a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes, whereby:

- Each Workbench host, and the respective applications within that host, are assigned to a Data-Center, this is mandatory
- The Data-Center name is entered during Workbench Primary Node installation
- The Data-Center name is case-sensitive and a max of 10 characters

Post Workbench Data-Center Sync Benefits

Workbench Data-Center **synchronization** forms a **distributed** Workbench architecture whereby:

- Engage Alarms can be cleared holistically from any Workbench at any Data-Center
- Metric data (i.e. CPU/RAM/DISK/NETWORK) from remote Workbench Agents (i.e. deployed on Genesys Application hosts such as SIP, URS, FWK etc) can be ingested into the local Workbench Data-Center instance/Cluster
  - i.e. provides network traffic optimization
- WB Configuration can be edited/view holistically
  - WB Configuration is based on the Workbench Master – the Workbench Master being the **initiator** of the WB to WB Data-Center Sync
    - For simplicity, Genesys recommends your Workbench Master is the Workbench deployed at the same Data-Center as the Master Configuration Server
    - Use this Workbench Master as the initiator when synching Workbench Data-Centers
- Channel Monitoring (CM) Call Flows, Media Files and Reports can be viewed holistically
- CM Call Flows and Media Files can be added/edited/deleted holistically

Post Workbench Data-Center Sync Limitations

Important

- Dashboards and Visualizations from either Data-Center do NOT sync to the other
  - i.e. Post Data-Center Sync, the "APAC" Dashobards will NOT be synched to the "EMEA" Data-Center, and vice-versa
- Users can ONLY view Metric data from the Data-Center they are logged into
  - i.e. Users cannot log into the APAC Data-Center and view Metrics from the "EMEA" and "LATAM" Data-Centers
- Only Active Workbench Alarms will be sync’d during the Data-Center to Data-Center syncing process
- Only Workbench Changes will be sync’d during the Data-Center to Data-Center syncing process based on the Retention Period configured on the WB Master
- Channel Monitoring Call Flows metadata is sync – not the actual CM Call Flow Object - this enables holistic managment of a Call Flow, irrespective of its Data-Center
  - This is by design, a Channel Monitoring Call Flow is associated with a WB IO application at only 1 x Data-Center

Data-Center Synchronization - Planning

Pre Data-Center Sync Workbench Architecture

The previous Workbench Installation sections in this document result in a Workbench instance/Cluster deployed at a given Data-Center.

For example:

- You have deployed a single node Workbench in APAC
  - The Engage Master Configuration Server is deployed in APAC
  - An Engage Distributed Solution Control Server (SCS) is deployed
  - Engage Alarms and Changes from both Data-Centers are being ingested into the APAC Workbench

- You have deployed a single node Workbench in EMEA
  - An Engage Configuration Server Proxy is deployed in EMEA
  - An Engage Distributed Solution Control Server (SCS) is deployed
  - Alarms and Changes from both Data-Centers are being ingested into the EMEA Workbench

- From a Genesys Engage perspective the APAC and EMEA Data-Centers are integrated via **CS Proxy** and **Distributed SCS** architecture

- At this stage, the 2 x Workbench deployments are separate from each other, albeit they're integrated to the same Engage platform and you wish to form an holistic, metric data ingestion optimised, distributed Workbench architecture

Check Workbench Component Status at each Data-Center

Prior to commencing a Workbench Data-Center Synchronization, please ensure the following components, at each Data-Center, have a Up/Green status:

- Workbench IO

- Workbench Elasticsearch
- Workbench ZooKeeper
- Workbench Agent (running on the respectice Workbench Hosts that are going to be synched)

Warning

- Please double-check the Workbench components above, at each Data-Center, have a Up/Green status before initiating a Workbench Data-Center Sync
- Do not change the Elasticsearch Port (i.e. 9200) post Data-Center synchronization - if the default requires change, change before Data-Center Sync
- Do not change the ZooKeeper Port (i.e. 2181) post Data-Center synchronization - if the default requires change, change before Data-Center Sync

Important

- Workbench Versions on ALL Nodes and at ALL Data-Centers should be running the same release - i.e. do NOT mix 9.0.000.00 with 9.1.000.00.

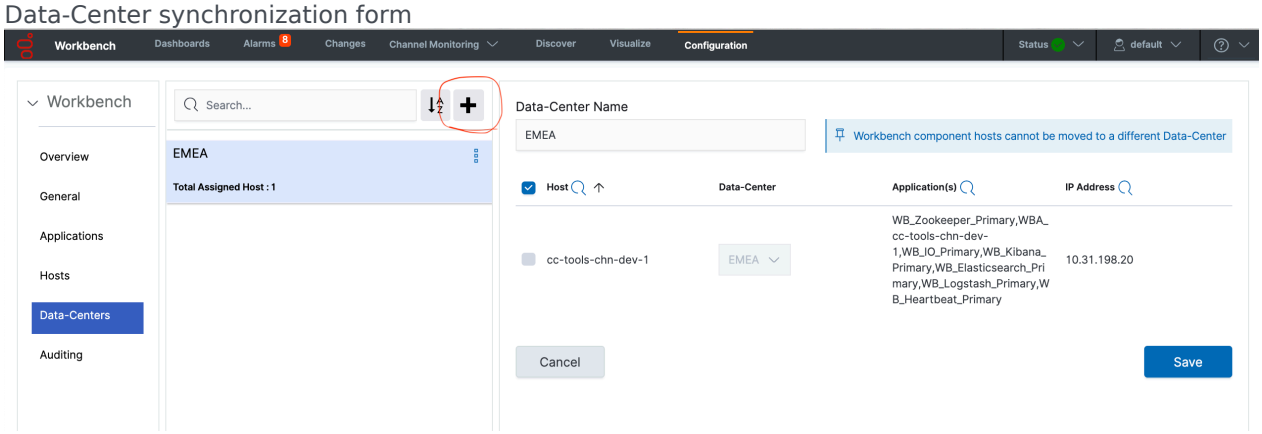
Important

- With the above planning considered, please progress to the next **Data-Center Syncronization - Configuration** section to begin the Data-Center Syncronization process.

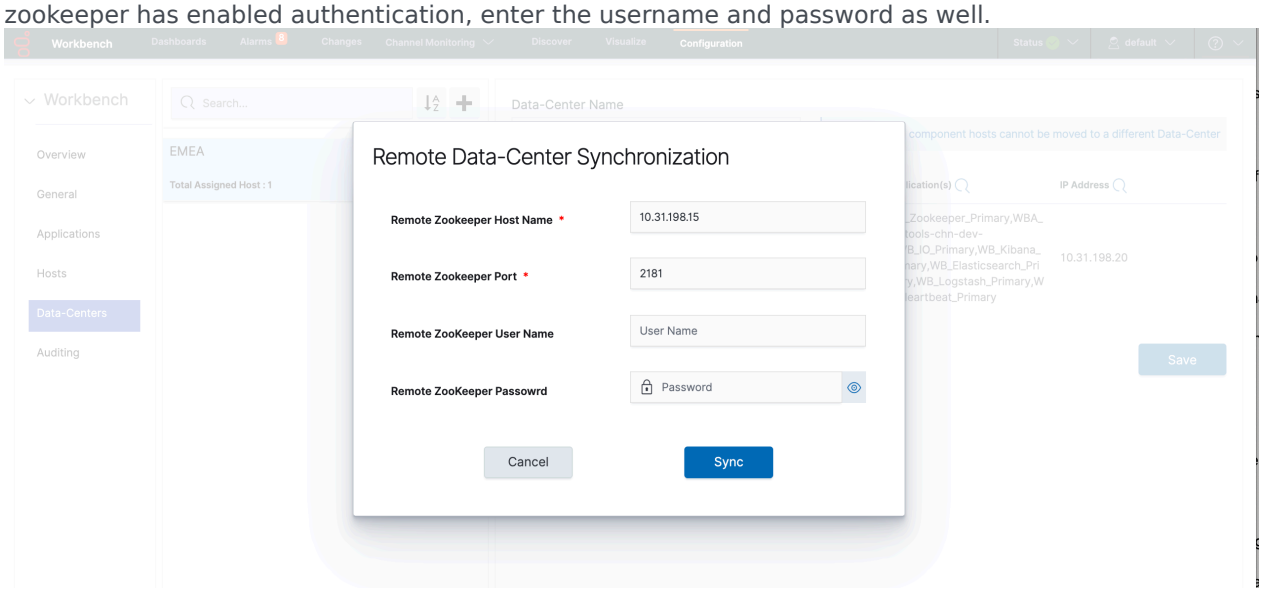
Data-Center Synchronization - Configuration

This section details the steps necessary to perform a Workbench Data-Center Synchronization:

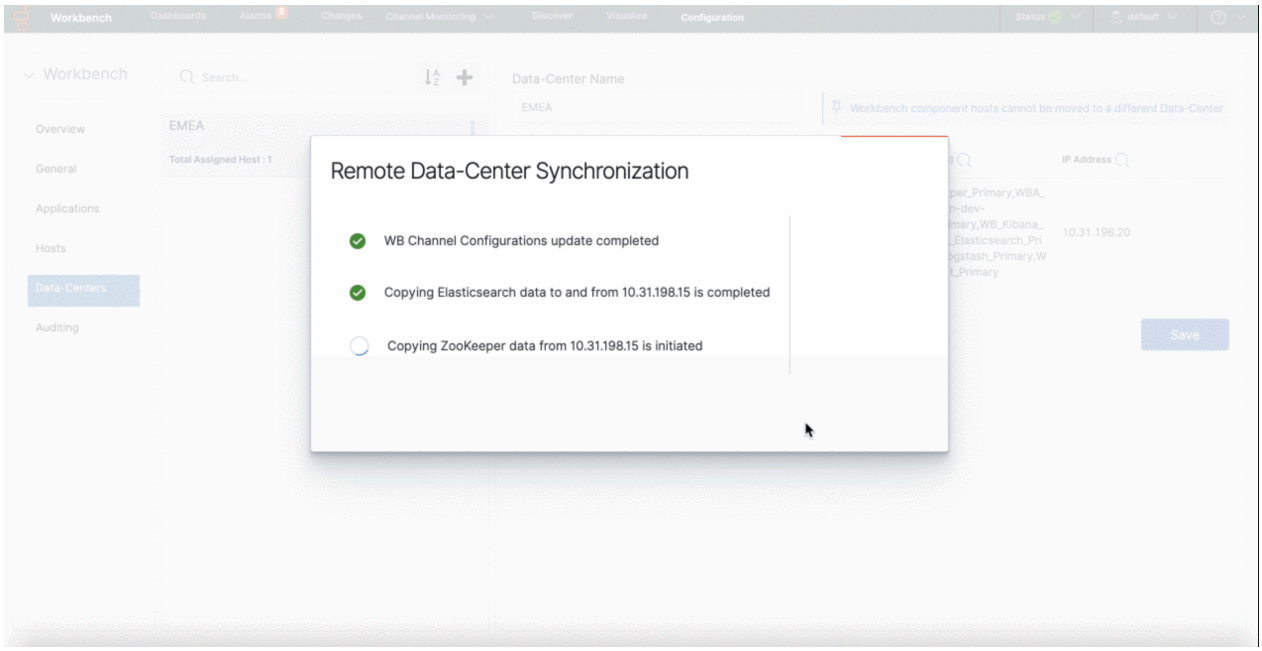
1. Go to the configuration page -> Data-Center section and click the below button to display the remote Data-Center synchronization form



2. In the displayed form, please fill the mandatory fields, remote zookeeper hostname and port. If remote zookeeper has enabled authentication, enter the username and password as well.

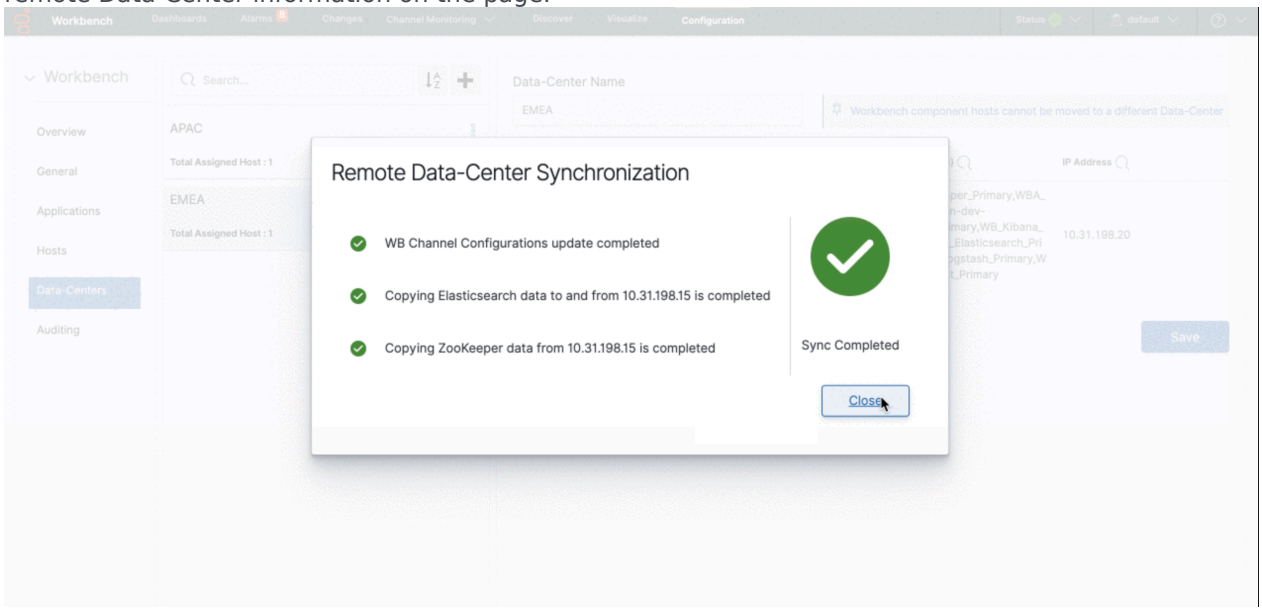


3. After filling the form click the sync button and wait, If your remote Zookeeper address is valid and able to connect, it will start progress synchronization and display the progress status on the screen



> **Warning**
>
> Please wait for the Workbench Data-Center synchronization to complete; do not perform any Workbench Configuration Changes during this time

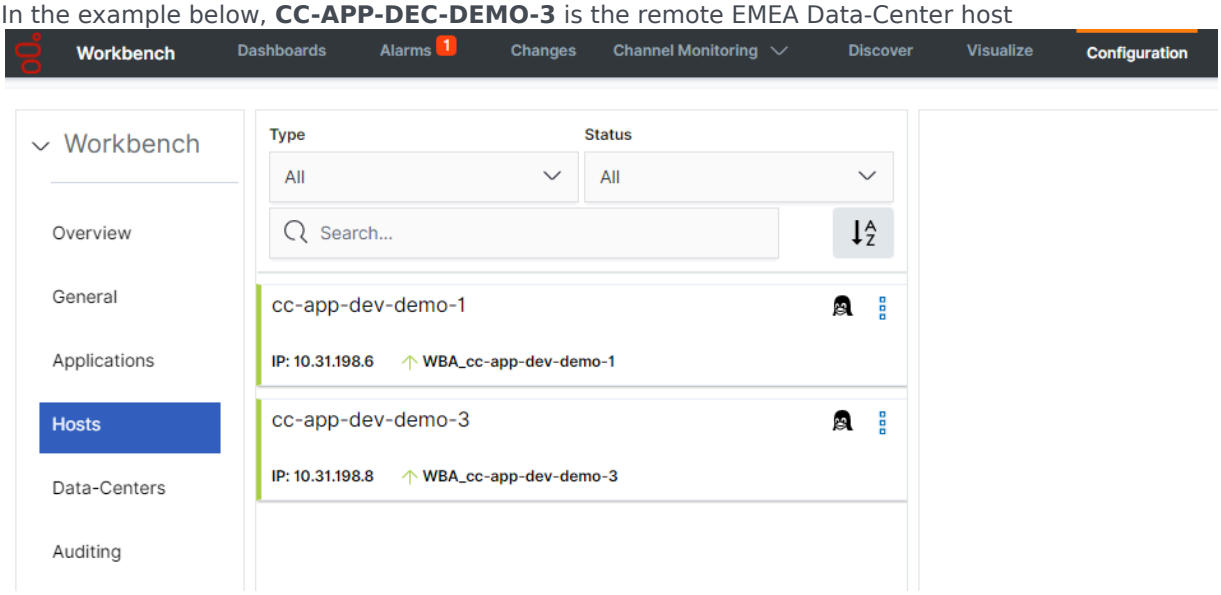
4. Once synchronization completed you can close the modal window and able to see the synchronized remote Data-Center information on the page.



5. Check the new/additional remote Workbench Data-Center Host(s) are present in Workbench\

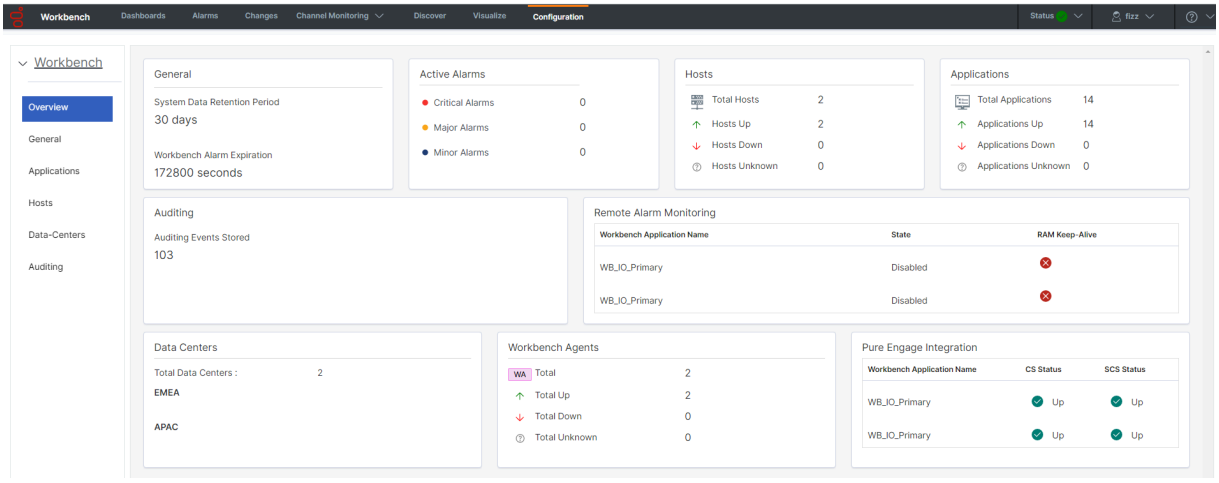
Configuration\Hosts

1. In the example below, **CC-APP-DEC-DEMO-3** is the remote EMEA Data-Center host



6. Check the number of Data-Centers and their names are present in Workbench\Configuration\Overview

1. In the example below, we have 2 x Data-Centers - **APAC** (the initiator) and the remote **EMEA** Data-Center



7. Repeat the above steps for any other Workbench Data-Center deployments that you wish to form in a Workbench distrbuted architecture

Workbench Data-Center - Post Formation

Warning

1. The folders '<WB_HOME_FOLDER>\Karaf\resources\windows\ wbagent_9.x.xxx.xx_installscripts' directory (Windows) and '<WB_HOME_FOLDER>/Karaf/resources/linux/wbagent_9.x.xxx.xx_installscripts' directory (Linux) WILL NEED to be *DELETED* first as new folders will be created with the updated details
2. When forming a Workbench Cluster, for example adding a Workbench Node 2 or Node 3, or Node N, on completion of forming the Workbench Cluster, the Workbench IO (i.e. WB_IO_Primary) Application now needs to be restarted to regenerate the correct Workbench Agent Remote JSON configuration file"

Workbench Data-Center - Renaming

Warning

1. The folders '<WB_HOME_FOLDER>\Karaf\resources\windows\ wbagent_9.x.xxx.xx_installscripts' directory (Windows) and '<WB_HOME_FOLDER>/Karaf/resources/linux/wbagent_9.x.xxx.xx_installscripts' directory (Linux) WILL NEED to be deleted first as new folders will be created with the updated details
2. If/when a Workbench Data-Center is renamed, the Workbench IO (i.e. WB_IO_Primary) Application needs to be restarted to regenerate the correct Workbench Agent Remote JSON configuration file"

Workbench Data-Center - Renaming - Workbench Agent Remote

Warning

1. Post the renaming of a Workbench Data-Center, if an existing host requires a Workbench Agent Remote re-installation, the newly generated binaries in the folders '<WB_HOME_FOLDER>\Karaf\resources\windows\wbagent_9.x.xxx.xx_installscripts' directory (Windows) and '<WB_HOME_FOLDER>/Karaf/resources/linux/

wbagent_9.x.xxx.xx_installscripts’ directory (Linux), will first need to be copied to the host before running the “installer.exe” (Windows) or “installer” (Linux) executable”

Planning and Deployment - Upgrade

This chapter provides details on the deployment of Genesys Workbench - Upgrade.

It contains the following sections:

- Workbench Upgrade – Windows - Pre – Upgrade Steps
- Workbench Upgrade – Windows - Primary Node Upgrade
- Workbench Upgrade – Windows - Additional Node Upgrade
- Workbench Upgrade – Windows – Rollback to Workbench 9.0
- Workbench Upgrade – Windows – Removing old version
- Workbench Upgrade – Linux - Pre – Upgrade Steps
- Workbench Upgrade – Linux - Primary Node Upgrade
- Workbench Upgrade – Linux - Additional Node Upgrade
- Workbench Upgrade – Linux – Rollback to Workbench 9.0
- Workbench Upgrade – Linux – Removing old version

> ### Warning
>
> - **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Workbench N-1 Upgrade

> ### Warning
>
> - Workbench only supports an N-1 upgrade path

Warning

- Please ensure your on the immediate previous Workbench release before upgrading

Warning

- i.e. Do not upgrade directly from 9.0.000.00 to 9.1.100.00 - instead from 9.0.000.00 upgrade to 9.1.000.00, then upgrade to 9.1.100.00

Workbench Version Alignment

Important

- Workbench Versions on ALL Nodes and at ALL Data-Centers should be running the same release - i.e. do NOT mix 9.0.000.00 with 9.1.000.00.

Workbench 9.2 to 9.3 Visualizations cannot be deleted

Important

- When upgrading from Workbench 9.2 to 9.3, the migrated Visualizations cannot be deleted; this will be addressed in a future Workbench 9.x release

Pre-Upgrade Steps - Windows

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Important

- Before proceeding with a Workbench upgrade:
  - Ensure **ALL** of the **current/old** Workbench version Services are **Started/Running** for a successful upgrade - on ALL Workbench Nodes (i.e. Primary and Additional)
  - At the end of a successful upgrade, ALL the old Workbench version Services will be **Stopped** set to **Manual**
- The Workbench Agent Service in the Primary Workbench Node should be up and running without any interruptions until all the associated Additional Nodes are upgraded from 9.2 to 9.3.000.00

Important

- For Workbench 9.2 to 9.3 upgrades:
  - During the upgrade to 9.3, Workbench component statuses may be inaccurate until all Workbench Cluster Nodes are fully upgraded/completed
  - The Workbench Primary Services should be up/running before commencing any Workbench 9.3 Node2, Node3, NodeN upgrades
  - Existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
  - The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
  - As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/message will be displayed
  - Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

- When upgrading from Workbench 9.2 to 9.3, the migrated Visualizations cannot be deleted; this will be addressed in a future Workbench 9.x release

Workbench N-1 Upgrade

Important

- **Workbench only supports an N-1 upgrade path**
- Please ensure your on the immediate previous Workbench release before upgrading
- i.e. Do not upgrade directly from 9.0.000.00 to 9.1.100.00 - instead from 9.0.000.00 upgrade to 9.1.000.00, then upgrade to 9.1.100.00
  - Follow this approach for each and every Workbench release upgrade

Workbench 9.1.100.00 to 9.2.xxx.xx upgrade - DataSync Utility

Important

- If/when your Workbench deployment has **multi Data-Center's that are synchronized**, please follow these steps below to avoid Workbench multi Data-Center data discrepancies

1. On the Workbench Primary Node/Host (i.e. APAC)
2. Extract the new downloaded "*Workbench_9.2.xxx.xx_WINDOWS.zip*" file to a working {WORK_DIR} directory (i.e. C:\tmp)
3. Navigate into the "*{WORK_DIR}\Workbench_9.2.xxx.xx_WINDOWS\ip\windows*" directory
4. Extract the "*{WORK_DIR}\Workbench_9.2.xxx.xx_Installer_Windows.zip*" file
5. Navigate into the "*{WORK_DIR}\Workbench_9.2.xxx.xx_Installer_Windows*" directory
6. Open a Command/Powershell Console **As Administrator** in the **{WORK_DIR}\Workbench_9.2.000.00_Installer_Windows\ip\windows** directory

7. Run "wb_patch.bat"
8. Enter the Workbench **Primary ZooKeeper IP_ADDRESS:PORT** of the Workbench Primary Node/Host (i.e. 10.20.30.40:2181)
   *If the Workbench Zookeeper has authentication enabled, provide the respective Primary Zookeeper username and password
9. The DataSync Utility will execute and provide progress information in the console.
10. It is a one time process and we don't require the steps while upgrading other Data centers.

> ## Warning
>
> - Only now commence the 9.1.100.00 to 9.2.xxx.xx Workbench upgrade

Workbench Upgrade - Windows - Primary Node

The Workbench installation files will be contained in the Genesys My Portal obtained downloaded compressed file.

Important

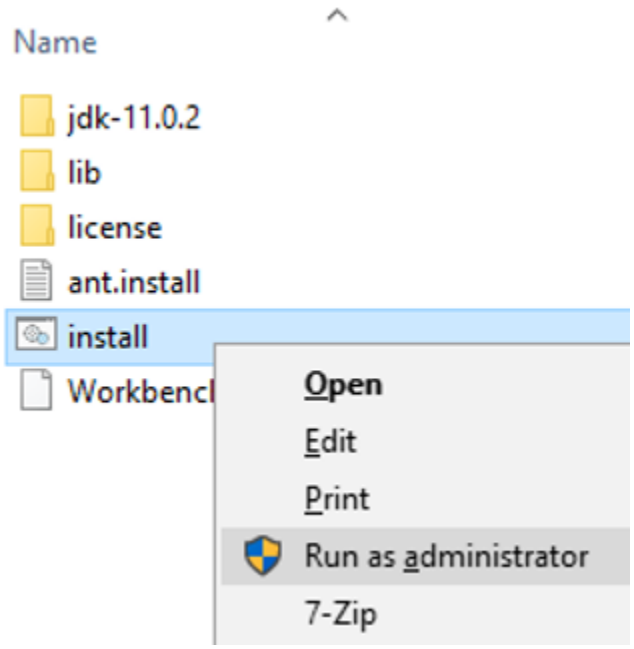
1. All Workbench deployments require a Primary Node. In any WB Cluster deployments, the WB Primary Node must be upgraded prior to upgrading WB Additional nodes/ applications. Ensure WB Additional nodes are up and running until the WB Primary node upgrade is completed. Once the WB Primary node upgrade is completed and its "Services" are "Started", proceed with the WB Additional nodes upgrade process in section “Workbench Upgrade – Windows - Additional Node”.
2. The Workbench installation uses the Ant Installer component. If during the Workbench upgrade a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, after upgrade, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.
3. Use an **Administrator** level account when running the Workbench *install.bat* file.
4. Genesys does not recommend installation of its components via Microsoft Remote Desktop.
5. If the Workbench installation is cancelled mid completion, please ensure the Workbench install directory is cleaned/purged prior to attempting another install.
6. For Workbench 9.0 to 9.2 Kibana uses port 8181 and Workbench IO uses port 8182
7. For Workbench 9.3 Kibana uses port 8182 (localhost access only) and Workbench IO uses port 8181

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

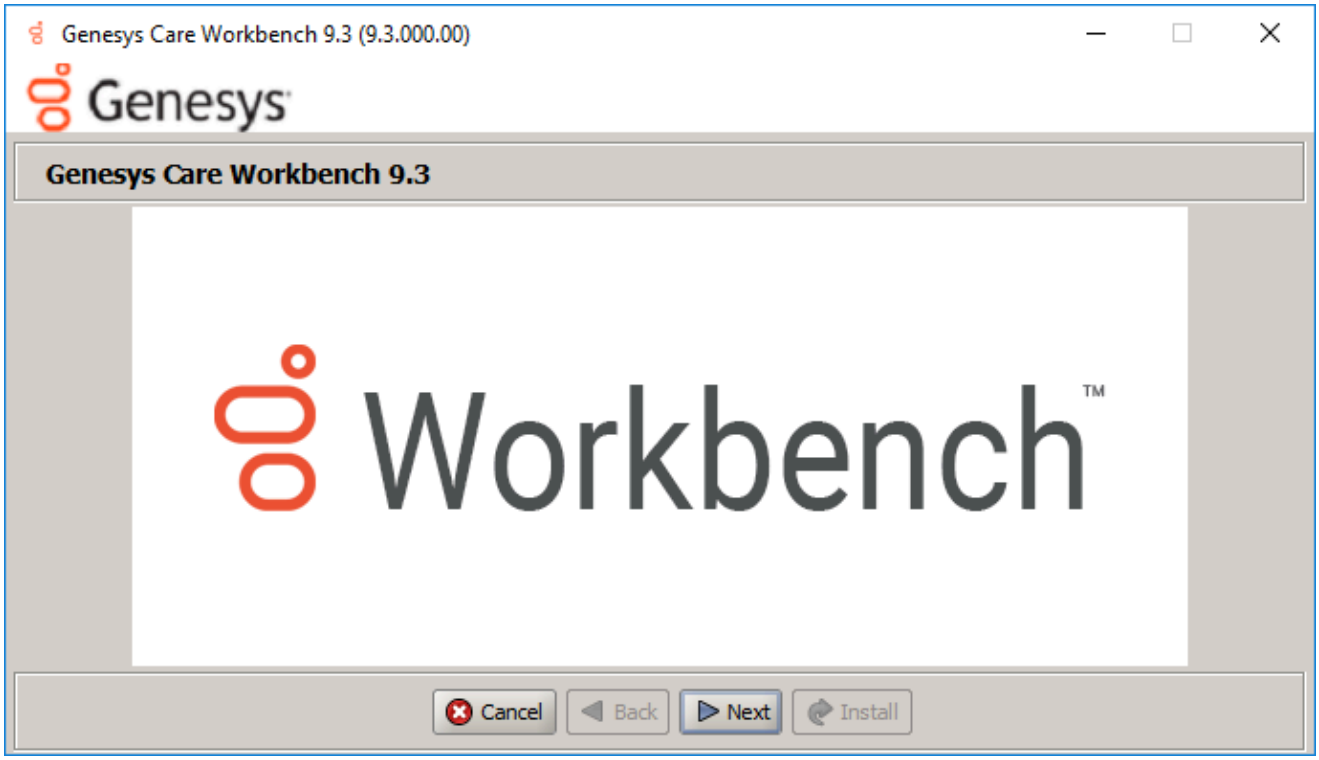
Please use the following steps to upgrade Workbench 9:

1. Extract the downloaded **Workbench_9.x.xxx.xx_Pkg.zip** compressed zip file.
2. Navigate into the **Workbench_9.x.xxx.xx_Pkg\ip\Windows** folder.
3. Extract the **Workbench_9.x.xxx.xx_Installer_Windows.zip** compressed zip file.
4. Navigate into the **Workbench_9.x.xxx.xx_Installer_Windows** folder
6. Right Click on the **install.bat** file and select **Run as Administrator**; alternatively, open a command prompt **As Administrator** and run **install.bat**.

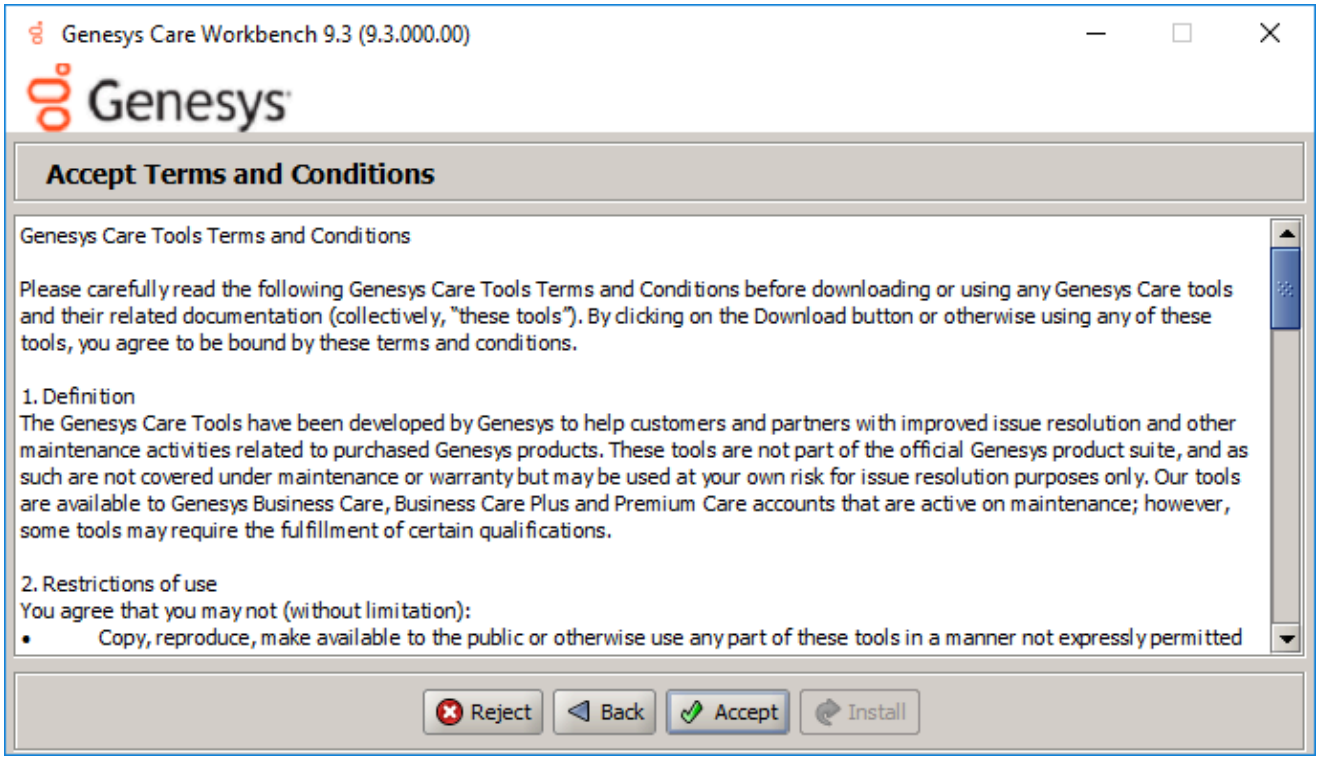


7. On the **Genesys Care Workbench 9.x** screen

- To start the Workbench upgrade, click **Next**

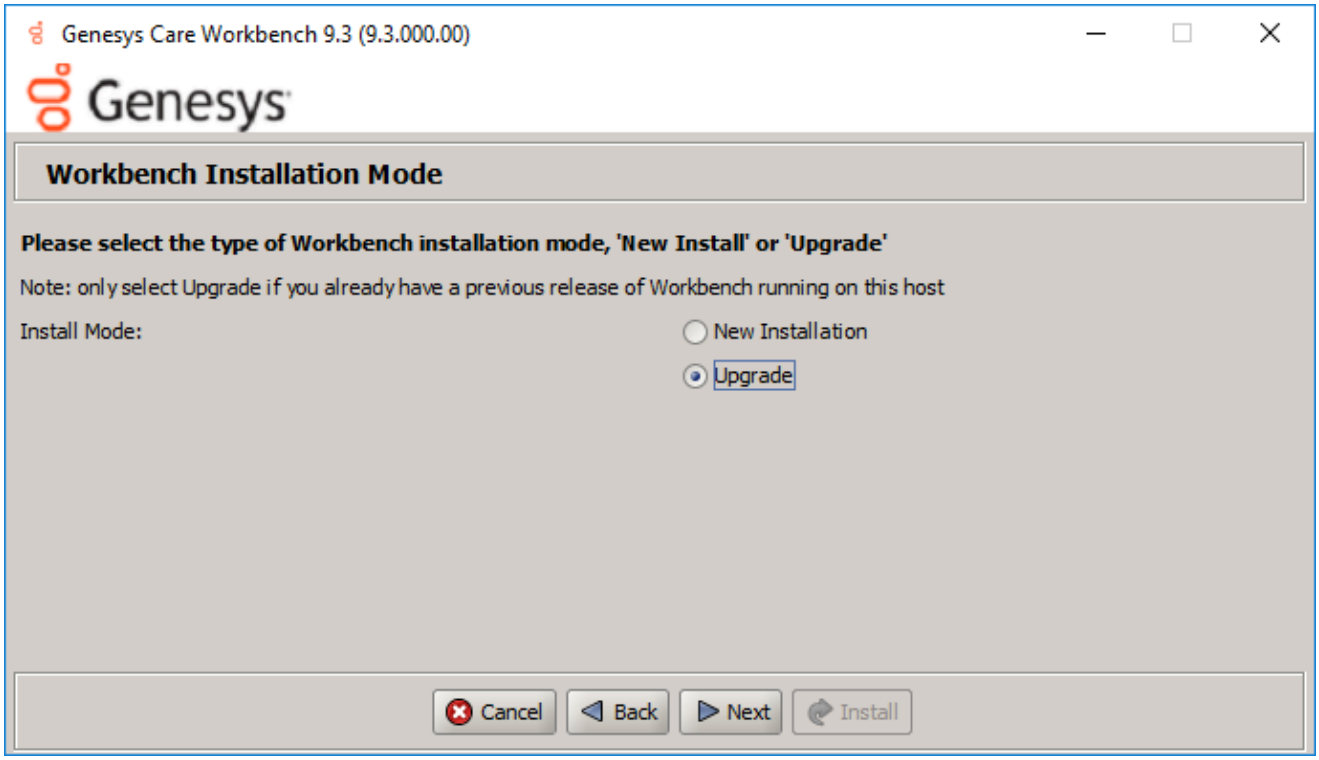


8. Review and if in agreement
   - Click **Accept** to the Genesys Terms and Conditions to continue.



9. On the Workbench **Installation Mode** screen

- Select **Upgrade** mode given there is already a previous release of Workbench running on this host/ node.



Important

- All the Workbench components, on this host, where the upgrade installer has been initiated, will be upgraded.

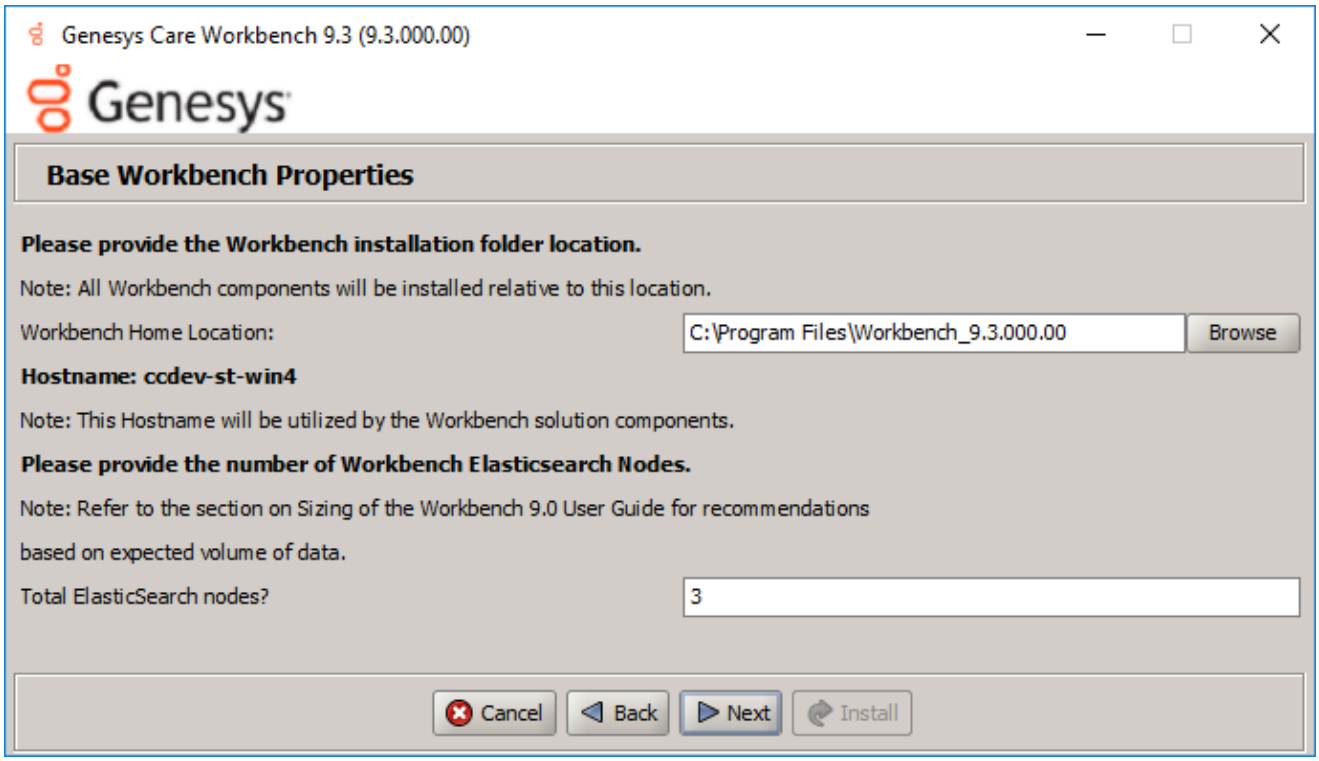
10. On the **Workbench Home Location** folder

- Provide the path where the new Workbench components will be installed (i.e. "C:\Program Files\Workbench_9.x.xxx.xx")
  - Select **default** to accept the default options
  - Select **Custom** to change the default options

Important

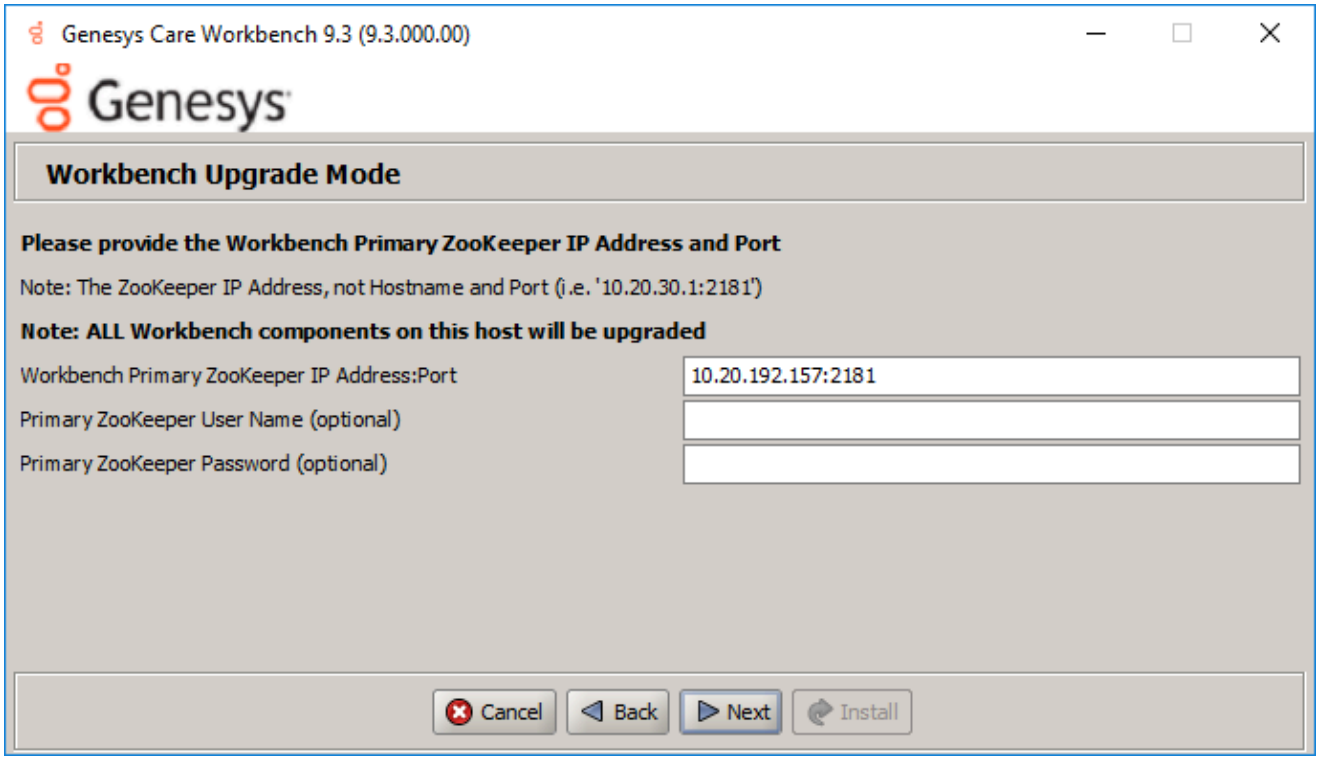
- This **new** version directory has to be different than the **current/old** Workbench version

installation location.



11. On the Workbench **Primary Zookeeper IP Address and Port**.

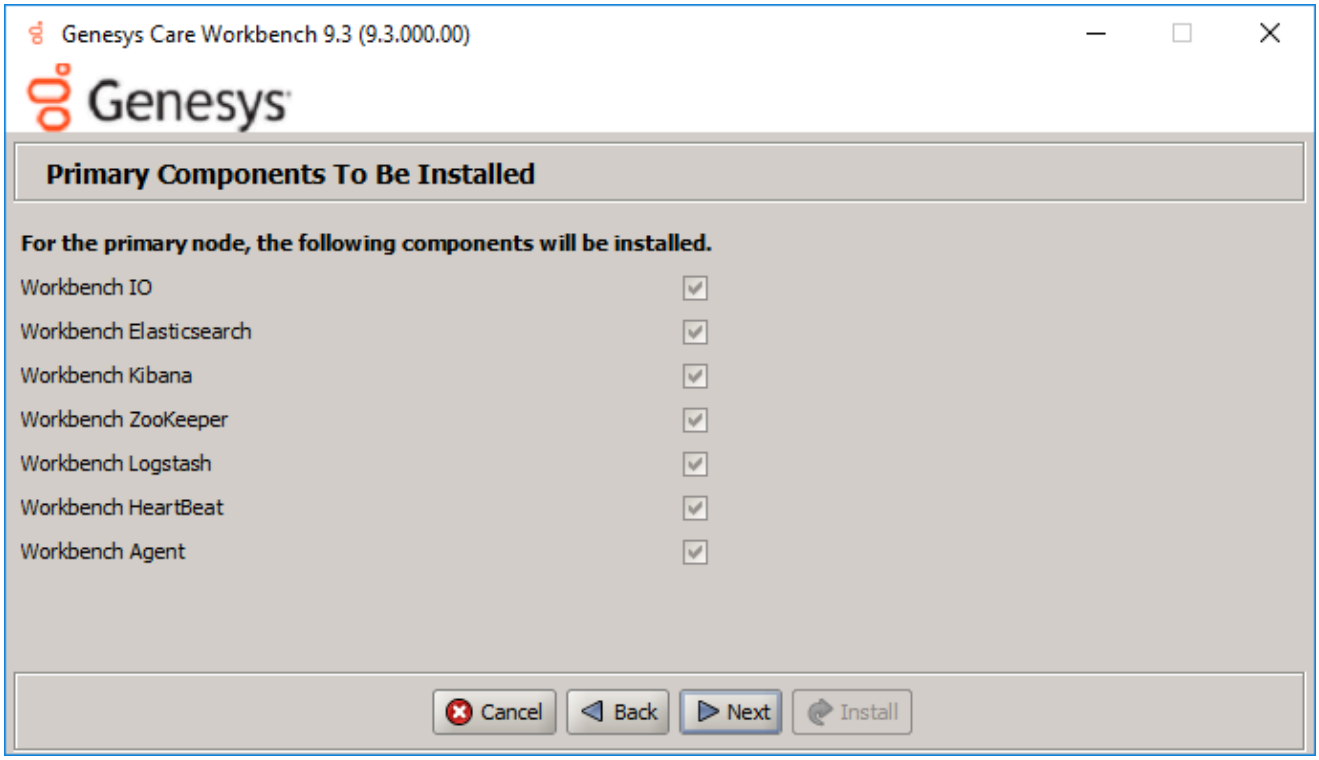
- Enter the Primary ZooKeeper IP:Port and click **Next**



> **Important**
> Provide Primary Zookeeper **IP Address:Port** (i.e. do **not** enter the hostname:port)

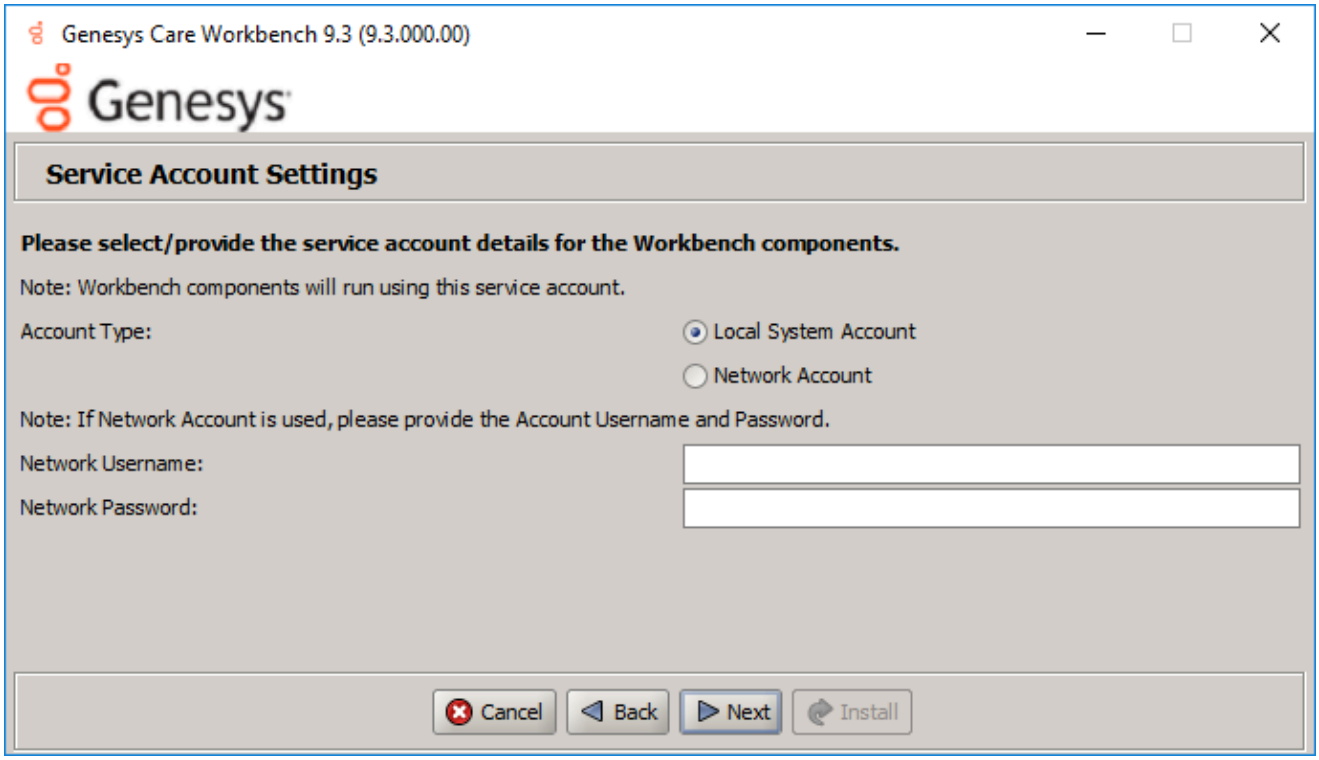
12. On the Workbench **Components to be Upgraded** screen.

- Which provides context on which Workbench components will be upgraded
- Click **Next**



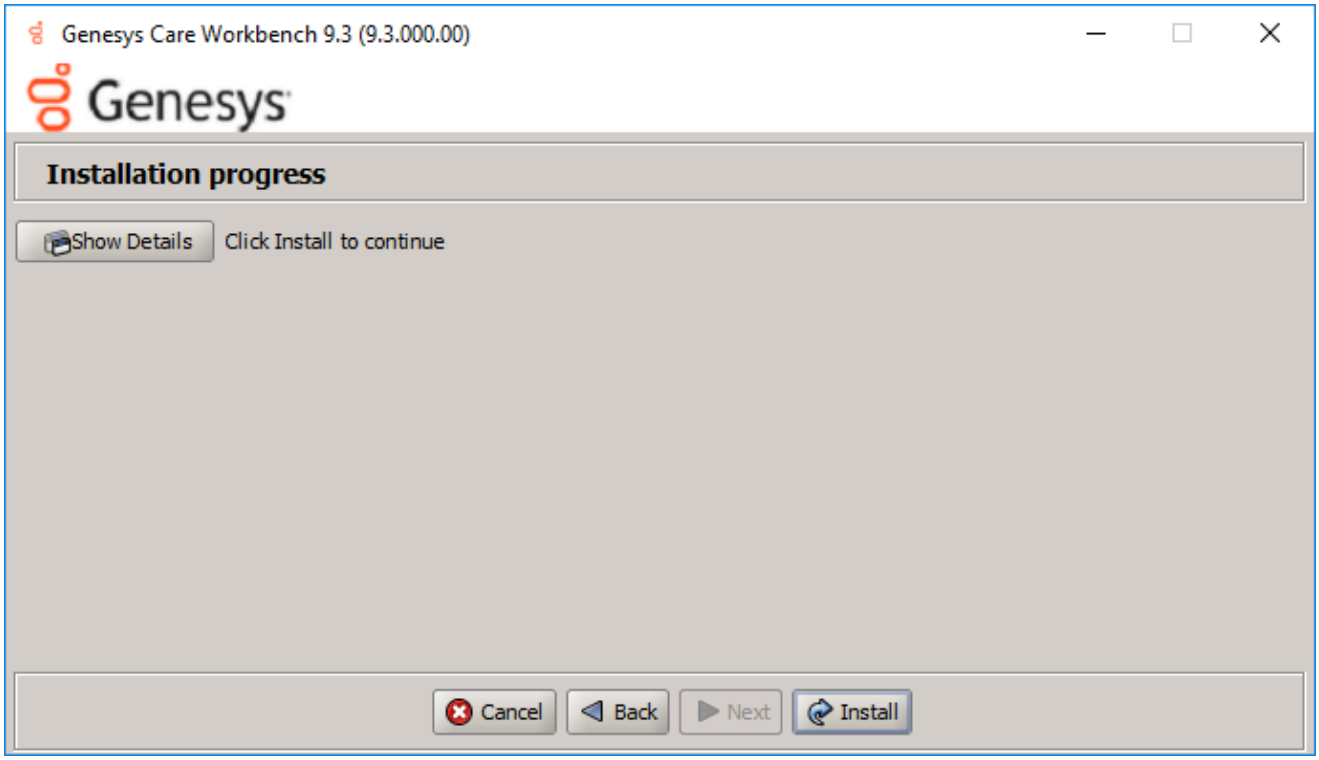
13. On the **Service Account** Settings screen

- The Workbench components are installed and executed as Services and the appropriate permissions are required to install them.
- Select either Local System Account or a Network Account
  - if Network Account is selected, provide the Username and Password to be used.
- Once complete, click **Next**.



14. On the **Installation Progress** screen

- Click **Install**

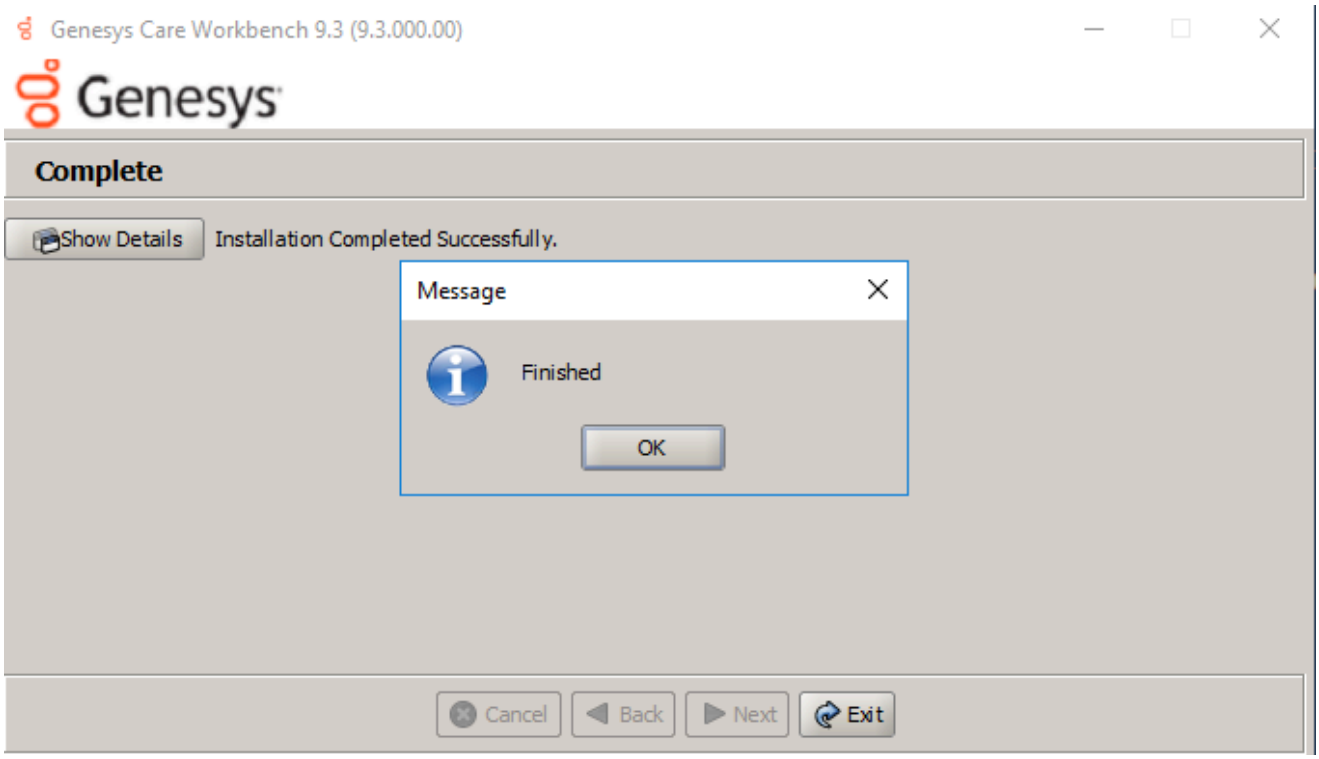


Tip

- The *Show Details* button allows you to review the steps the installer is taking to install the Workbench component(s).
- This is also a good source for any errors that may be observed during the upgrade process.

15. On the **Installation Complete** screen

- Click **OK** and **Exit** when presented with the **Finished** dialog



Important

- Once the new Workbench version is installed, new Workbench 9.x.xxx.xx Services will be registered in the Service registry
- The previous Workbench version Services will be automatically **Stopped** and set to **Manual**.
- The Workbench port configuration of upgraded components will be same as the Workbench **old** components.
- The Workbench data and log folders will be automatically created in the new Workbench installed location.
- At the end of the upgrade process, Workbench 9.y.yyy.yy Cluster, data and configuration will be restored as per the prior Workbench 9.x.xxx.xx installation.

16. **Next Steps**

Important

- The Workbench Primary Node has been upgraded
- If there are Additional Workbench Nodes at this Data-center, please continue to upgrade those using the **Workbench Upgrade – Windows - Additional Node** section as a reference

Warning

- The respective Workbench Agent Remote (WAR) components, installed on hosts such as SIP, URS, GVP etc, will be upgraded based on the WAR **Upgrade Time** (default 02:00)
- For WB 9.3 the WAR [General] **Log File Location**, **Segment** and **Expire** fields will be blank post an upgrade until the WAR **Upgrade Time** (default 02:00) is triggered and the WAR upgrade is completed

Workbench Upgrade – Windows - Additional Node

Warning

1. Ensure the Workbench Primary host/node has been successfully upgraded prior to commencing the upgrade of Workbench Additional Hosts/Nodes.
2. For Workbench Primary Node upgrade, please see instructions in section “Workbench Upgrade - Windows - Primary Node”
3. Ensure the Workbench Additional Hosts/Nodes are up and running until the Workbench Primary node has completed the upgrade process.
4. Once the Workbench Primary node upgrade is completed and its new Services are started, proceed with the Workbench Additional Nodes upgrade process.
5. The Workbench data and log folders will be automatically created in the new Workbench installed location.
6. **ALL** the Workbench components on this particular host where the Workbench upgrade installer is run will be upgraded.
7. You cannot upgrade specific Workbench components on a host/node - it's ALL Workbench components

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Following these instructions when upgrading a Workbench Additional Node:

1. Extract the downloaded **Workbench_9.x.xxx.xx_Pkg.zip** compressed zip file.
2. Navigate into the **Workbench_9.x.xxx.xx_Pkg\ip\Windows** folder.
3. Extract the **Workbench_9.x.xxx.xx_Installer_Windows.zip** compressed zip file.
4. Navigate into the **Workbench_9.x.xxx.xx_Installer_Windows** folder

5. Right Click on the **install.bat** file and select Run as Administrator; alternatively, open a command prompt As Administrator and run **install.bat**.

6. On the Genesys Care Workbench 9.x screen.

- Click **Next**

7. On the Genesys Terms and Conditions screen.

- Review and if in agreement, click **Accept** to continue

8. On the next Workbench **Installation Mode** screen

- Select **Upgrade** mode given you already have a previous release of Workbench running on this host/node.
- Click **Next**

9. On the **Base Workbench Properties - Installation Folder** screen

- Provide the **Workbench Home Location** folder where Workbench components will be installed (i.e. "C:\Program Files\Workbench_9.x.xxx.xx")
- For **Settings Type** select either **Default** or **Custom**
  - Choose **Default** for the default paths, ports etc
  - Choose **Custom** to provide specific custom paths, ports etc
- Click **Next**

10. On the Workbench Primary Zookeeper **IP Address** and **Port** screen

- Enter the Workbench Primary Zookeeper **IP Address** and **Port**
- Click **Next**

11. On the Workbench **Components to be Upgraded** screen

- All the Workbench components that are installed on this host/node will be automatically checked
- Click **Next**

12. On the **Service Account** Settings screen

- Choose **System Account** or **Network Account**
  - if Network Account is selected, provide the Username and Password to be used.
- Once complete, click **Next**.

13. On the **Installation Progress** screen

- Click **Next** to start the upgrade

14. On the **Installation Complete** screen

- Click **OK** on the **Finished** dialog
- Click **Exit**

15. At the end of the upgrade process, the previous Workbench versions data and configuration will be restored to the new Workbench version.

16. **Repeat** the above for **ALL** Workbench Additional Nodes.

Workbench Upgrade – Windows – Rollback to Workbench 9.0

If you encounter issues with your Workbench upgrade, we recommend opening a Genesys Support Case to progress and resolve the problem.

Please review the Troubleshooting section of this document for log collection recommendations.

However, if there is a need to rollback the version of Workbench to the previous version,, the following steps should be followed.

Single Node deployment - Rollback/Downgrade

1. Uninstall Workbench_9.1.000.00
    a. Browse to Workbench installation folder (C:\Program Files\Workbench_9.1.000.00) and locate file **uninstall.bat**
    b. Run **uninstall.bat** file as **Administrator**
    c. Post running **uninstall.bat** delete the old version folders
2. Start the previous Workbench Services manually from the Service menu
    a. Genesys Workbench Agent
    b. Genesys Workbench Elasticsearch
    c. Genesys Workbench Kibana
    d. Genesys Workbench ZooKeeper
    e. Genesys Workbench.IO
3. Right click each Service name as listed above, select **Properties**
4. Change start type to **Automatic** and select **OK**

> ### Important
> Once the previous WB Services are started, navigate to **http://<WORKBENCH_HOST>:8181** to login and use Workbench

Cluster Node deployment - Rollback/Downgrade

> **Important**
>
> For Cluster deployments, once you Rollback/Downgrade Workbench, you will lose all Elasticsearch data (Alarms, Changes, Call Flow and Auditing).

1. Open all nodes where ElasticSearch 9.0 is installed, navigate to data folder. Delete all files and folders present inside data folder.
2. Uninstall Workbench_9.1.000.00 in primary node.
    a. Browse to Worbench installation folder (C:\Program Files\Workbench_9.1.000.00) and locate file **uninstall.bat**
    b. Run **uninstall.bat** file as **Administrator**
    c. Post running **uninstall.bat** and delete the old version folders
3. Uninstall Workbench_9.1.000.00 in all additional nodes using the above steps.
4. Open all Workbench nodes where ElasticSearch 9.1 is installed, navigate to **data** folder. Delete all files and folders present inside data folder.
5. In all Workbench Additional Nodes where ZooKeeper is installed, navigate to **data** folder. Except **myid** (file) delete all folders and files present inside data folder.

> **Important**
>
> 1. If the **myid** file is deleted, the ZooKeeper Cluster formation will not be successful.
> 2. Please make sure to **uninstall** Workbench 9.0.100.00 of all nodes of the cluster, before starting Services of Workbench 9.0.000.00; partial uninstall can cause data corruption.

6. Start Service manually from the previous version of Workbench from the Services in primary node
    a. Genesys Workbench Agent
    b. Genesys Workbench Elasticsearch
    c. Genesys Workbench Kibana
    d. Genesys Workbench ZooKeeper
    e. Genesys Workbench.IO
7. Now **Start** Workbench Services of other Workbench Additional Nodes.

8. Right click each Service name, select **Properties**.
9. Change *Start Type* to **Automatic** and select **OK** .

> ## Important
>
> Once the WB Services are started, navigate to **http://<WORKBENCH_HOST>:8181** to login and use Workbench.

Workbench Upgrade – Windows – Removing old version

Uninstalling older releases of Workbench

Windows Operating System

> **Important**
>
> 1. Only follow these instructions when Workbench has been successfully upgraded (i.e. to 9.1.000.00) and you are ready to uninstall the previous release of Workbench (i.e. 9.0.100.00) to free up space/resources.
> 2. Ensure and double check the previous Workbench version Workbench Services are ALL stopped prior to running the **unistall.bat** script.
> 3. The Workbench uninstall process **permanently** removes the previous Workbench Services associated with all the previous Workbench components and all files including data and logs etc.
> 4. If any previous Workbench data is required for archival purposes, please ensure it is saved at a separate location prior to running the uninstall script.
> 5. The uninstall process will leave the original configuration file used to generate the Workbench installation; this can be provided to Genesys Care if related to an installation issue.

The following steps provide instructions on uninstalling an older release of Workbench after a successful Workbench upgrade (i.e. from 9.0.100.00 to 9.1.000.00):

1. Browse to the Workbench installation folder of the version to be removed (i.e. "C:\Program Files\Workbench_9.0.100.00") and locate the file **uninstall.bat**.
2. Execute the **uninstall.bat** file as an Administrator.
3. Post running **uninstall.bat**, also delete traces of files/folders (i.e. delete the **uninstall.bat** and **ConfigFileBackup** folder).

Linux Pre-Upgrade Steps

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Important

- Before proceeding with a Workbench upgrade:
  - Ensure **ALL** of the **current/old** Workbench version Services are **Started/Running** for a successful upgrade - on ALL Workbench Nodes (i.e. Primary and Additional)
  - At the end of a successful upgrade, ALL the old Workbench version Services will be **Stopped** set to **Manual**
- The Workbench Agent Service in the Primary Workbench Node should be up and running without any interruptions until all the associated Additional Nodes are upgraded from 9.2 to 9.3.000.00

Important

- For Workbench 9.2 to 9.3 upgrades:
  - During the upgrade to 9.3, Workbench component statuses may be inaccurate until all Workbench Cluster Nodes are fully upgraded/completed
  - The Workbench Primary Services should be up/running before commencing any Workbench 9.3 Node2, Node3, NodeN upgrades
  - Existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
  - The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
  - As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/message will be displayed
  - Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

- When upgrading from Workbench 9.2 to 9.3, the migrated Visualizations cannot be deleted; this will be addressed in a future Workbench 9.x release

Workbench N-1 Upgrade

Important

- **Workbench only supports an N-1 upgrade path**
- Please ensure your on the immediate previous Workbench release before upgrading
- i.e. Do not upgrade directly from 9.0.000.00 to 9.1.100.00 - instead from 9.0.000.00 upgrade to 9.1.000.00, then upgrade to 9.1.100.00
  - Follow this approach for each and every Workbench release upgrade

Workbench 9.1.100.00 to 9.2.xxx.xx upgrade - DataSync Utility

Important

- If/when your Workbench deployment has **multi Data-Center's that are synchronized**, please follow these steps below to avoid Workbench multi Data-Center data discrepancies

1. On the Workbench Primary Node/Host (i.e. APAC)
2. Extract the new downloaded "*Workbench_9.2.xxx.xx_LINUX.tar.gz*" file to a working {WORK_DIR} directory (i.e. ~/tmp)
3. Navigate into the "*{WORK_DIR}/Workbench_9.2.xxx.xx_LINUX/ip/linux*" directory
4. Extract the "*{WORK_DIR}/Workbench_9.2.xxx.xx_Installer_Linux.tar.gz*" file
5. Run **"wb_patch.sh"**
6. Enter the Workbench **Primary ZooKeeper IP_ADDRESS:PORT** of the Workbench Primary Node/Host (i.e. 10.20.30.40:2181)

*If the Workbench Zookeeper has authentication enabled, provide the respective Primary Zookeeper username and password

7. The DataSync Utility will run and provide progress information in the console
8. It is a one time process and we don't require the steps while upgrading other Data centers.

> ## Warning
>
> - Only now commence the 9.1.100.00 to 9.2.xxx.xx Workbench upgrade

Workbench Upgrade - Linux - Primary Node

The Workbench installation files will be contained in the Genesys My Portal obtained downloaded compressed file.

Important

1. Workbench requires the installation of a **Primary Node** at each and every Workbench Data-Center.
2. The Workbench Primary Node must be installed/upgraded prior to installing/upgrading Workbench Additional Nodes.
3. Workbench ships with its own pre-bundled Java distribution, OpenJDK11; all Workbench components will be configured through the installation to use this Java distribution and should not affect any other components that may be installed on the host.
4. The Workbench installation uses the Ant Installer component, if during the Workbench installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.
5. Use an **sudo** level account when running the Workbench *install.sh* file.
6. If the Workbench installation is cancelled mid completion, please ensure the Workbench install directory is cleaned/purged prior to attempting another install
7. For Workbench 9.0 to 9.2 Kibana uses port 8181 and Workbench IO uses port 8182
8. For Workbench 9.3 Kibana uses port 8182 (localhost access only) and Workbench IO uses port 8181

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Please use the following steps to upgrade Workbench 9 on Linux:

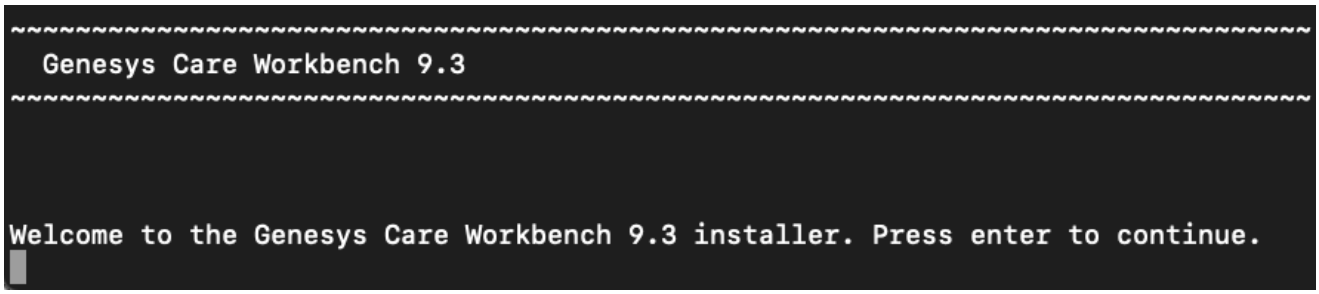
1. Run **tar zxf Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz** to extract the downloaded

Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz compressed file.

2. **cd** into the **ip\linux** folder.
3. Run **tar zxf Workbench_9.x.xxx.xx_Installer_Linux.tar.gz** - to extract the *Workbench_9.x.xxx.xx_linux.tar.gz* compressed tar file.
4. Run **./install.sh** (Do NOT prefix **./install.sh** with **sudo**)

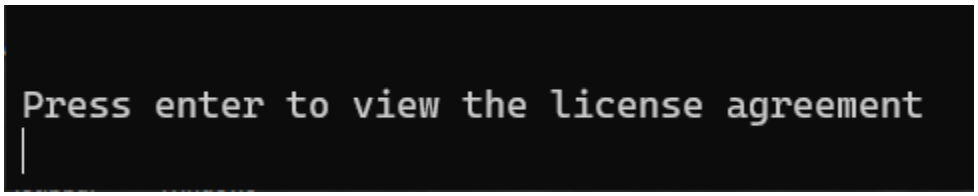
5. Genesys Care Workbench 9.x

- Press **Enter** to start the Workbench upgrade.



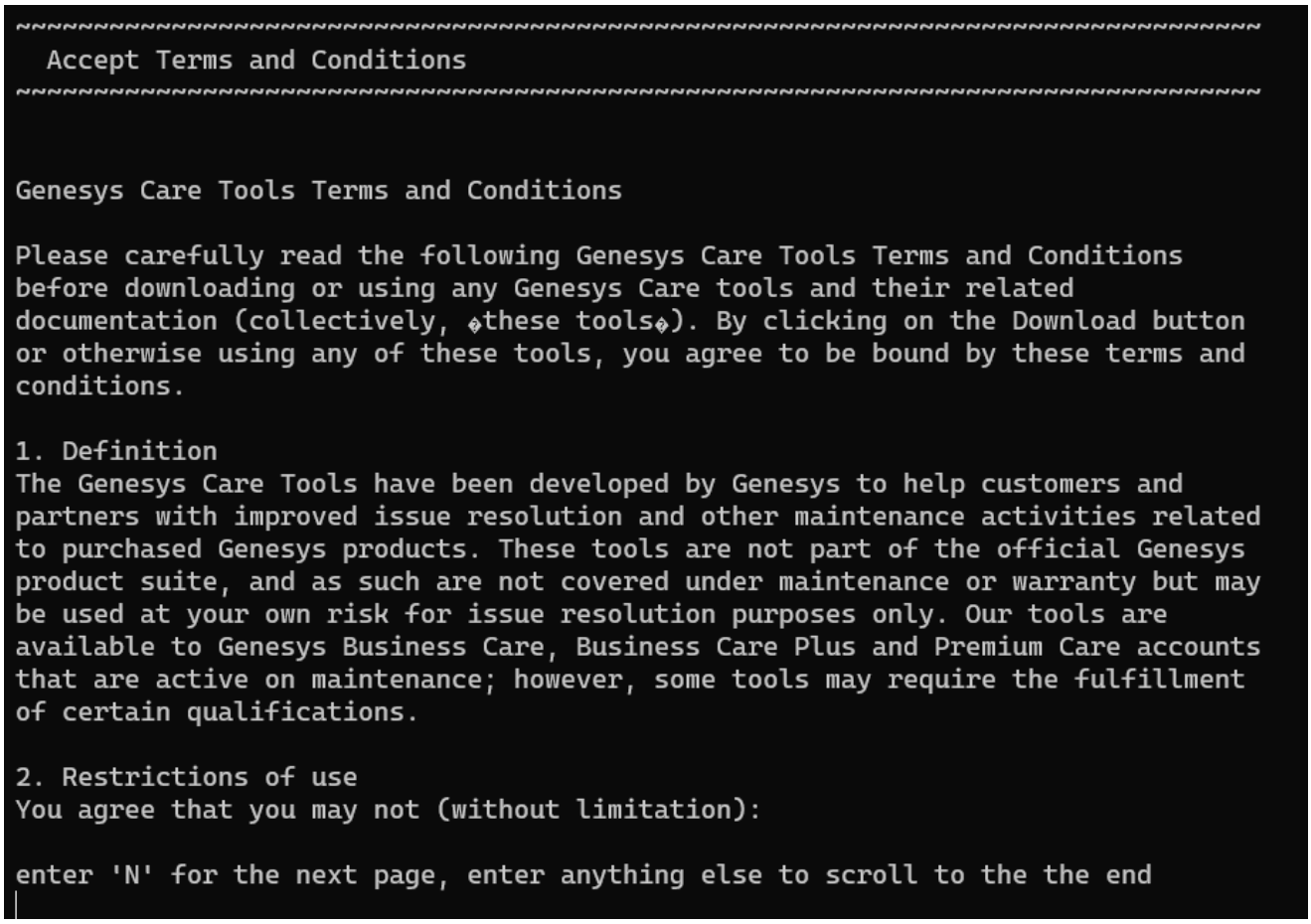
6. Genesys Workbench License Agreement

- Press **Enter** to view the Genesys Workbench license agreement



7. Review license agreement

- Enter **N** for the next page, or press **Enter** to scroll to the end of the Terms and Conditions



8. Genesys Workbench **Terms and Conditions**

- Press **Enter** to continue, if you agree to the Genesys Workbench Terms and Conditions

```
YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE GENESYS CARE TOOLS IS AT
YOUR SOLE RISK.  THE GENESYS CARE TOOLS ARE PROVIDED ◆AS IS◆ AND WITHOUT
WARRANTY OF ANY KIND.  GENESYS EXPRESSLY DISCLAIMS ALL WARRANTIES AND/OR
CONDITIONS EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY OR SATISFACTORY QUALITY AND
FITNESS FOR A PARTICULAR PURPOSE.  GENESYS DOES NOT WARRANT THAT THE USE OF THE
GENESYS CARE TOOLS WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ANY DEFECTS WILL
BE CORRECTED.  NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY GENESYS SHALL
CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY.  CUSTOMER
ASSUMES THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES,
SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.  THIS DISCLAIMER DOES NOT
LIMIT OR EXCLUDE ANY LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY GENESYS◆
NEGLIGENCE.
Limitation of Liability.
GENESYS SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY
CUSTOMER OR ANY USER OF THE GENESYS CARE TOOLS.  UNDER NO CIRCUMSTANCES,
INCLUDING NEGLIGENCE, SHALL GENESYS BE LIABLE FOR ANY INCIDENTAL, SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LIMITED
GRANT OF RIGHTS.  SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL
OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Do you accept the license? Y or N   [default:Y]
```

9. Workbench **Installation Mode**.

- Enter **2** for **Upgrade** - given there is already a previous release of Workbench running on this host/ node.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Workbench Installation Mode
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE SELECT THE TYPE OF WORKBENCH INSTALLATION MODE, 'NEW INSTALL' OR 'UPGRADE'
Note: only select Upgrade if you already have a previous release of Workbench running on this host
Install Mode:
  Enter a number
  1) New Installation [default]
  2) Upgrade
2
```

10. Workbench Base Properties - **Installation Path**.

- Press **Enter** to accept the default **/opt/Genesys/Workbench_9.x.xxx.xx** installation path

- Or provide a new installation path - i.e. */home/genesys/Workbench9.x.xxx.xx* and press **Enter**

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Base Workbench Properties
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE PROVIDE THE WORKBENCH INSTALLATION FOLDER LOCATION.
Note: All Workbench components will be installed relative to this location.
Workbench Home Location:   [default:/opt/Genesys/Workbench_9.3.000.00]
```

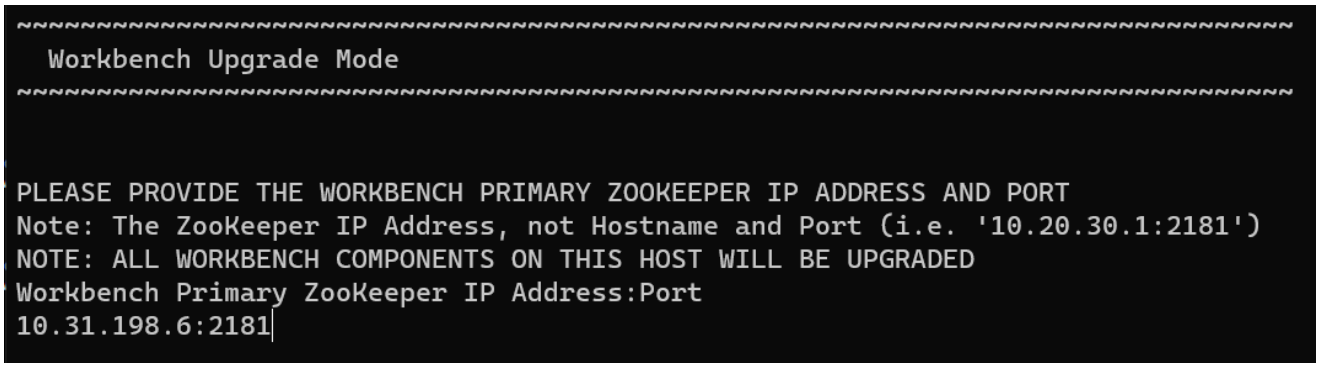
11. Workbench Base Properties - **Default** or **Custom**

- For Settings Type, either Default or Custom
  - Press **Enter** to accept the Default option - which enables provision of *Default* paths, ports etc
  - Type **2** and press **Enter** to choose the **Custom** option which enables provision of specific custom paths, ports etc

```
Settings Type:
  Enter a number
  1) Default [default]
  2) Custom
```

12. Workbench **Primary ZooKeeper IP Address:Port**.

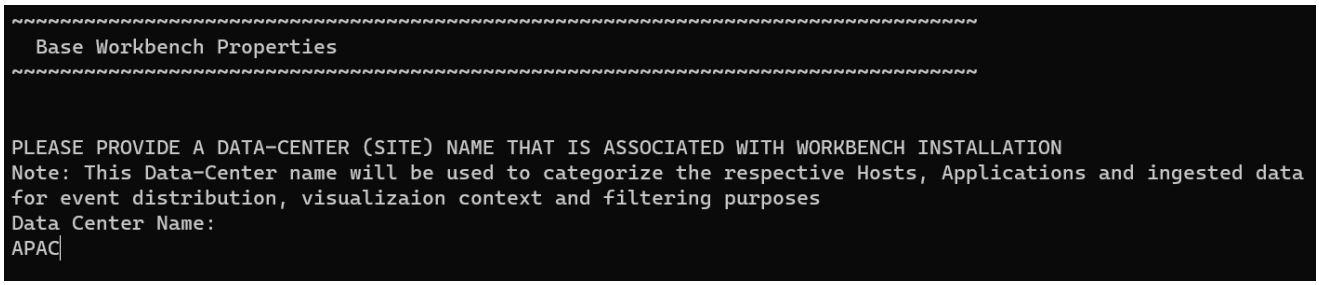
- Enter the Workbench Primary Zookeeper IP Address and Port
- Press **Enter**



13. Workbench **Data-Center**.

- Type the Data-Center name for this Workbench instance/Cluster (i.e. "APAC", "EMEA", "Chicago" - do NOT use "default")
- Press **Enter**

> **Important**
>
> - Workbench Data-Centers is a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes
> - Each Workbench host, and the respective applications within that host, are assigned to a Data-Center, this is mandatory
> - Note: The Data-Center name is **case-sensitive**, limited to a maximum of **10**, Alphanumeric and underscore characters only.

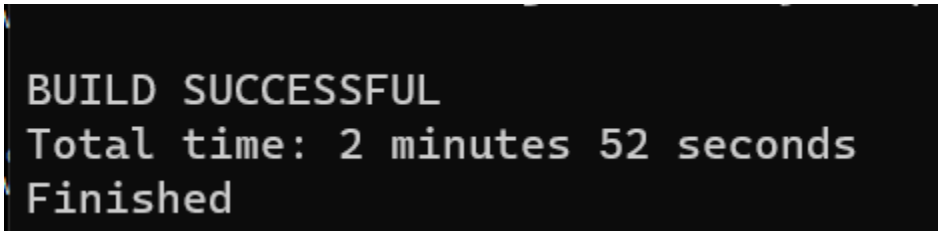


14. **Installation Progress**

- The Workbench installer will now upgrade the old Workbench version to the new Workbench version

15. **Installation Complete**

- The message message indicates the Workbench upgrade process is complete



> ## Important
>
> - Once the new Workbench version is installed, new Workbench 9.x.xxx.xx Services will be registered in the Service registry
> - The previous Workbench version Services will be automatically **Stopped** and set to **Manual**.
> - The Workbench port configuration of upgraded components will be same as the Workbench **old** components.
> - The Workbench data and log folders will be automatically created in the new Workbench installed location.
> - At the end of the upgrade process, Workbench 9.y.yyy.yy Cluster, data and configuration will be restored as per the prior Workbench 9.x.xxx.xx installation.

17. **Next Steps**

> ## Important
>
> - The Workbench Primary Node has been upgraded
> - If there are Additional Workbench Nodes at this Data-center, please continue to upgrade those using the **Workbench Upgrade – Linux - Additional Node** section as a reference

Warning

- The respective Workbench Agent Remote (WAR) components, installed on hosts such as SIP, URS, GVP etc, will be upgraded based on the WAR **Upgrade Time** (default 02:00)
- For WB 9.3 the WAR [General] **Log File Location**, **Segment** and **Expire** fields will be blank post an upgrade until the WAR **Upgrade Time** (default 02:00) is triggered and the WAR upgrade is completed

Workbench Upgrade – Linux - Additional Node

The Workbench installation files will be contained in the Genesys My Portal obtained downloaded compressed file.

Important

1. Workbench requires the installation of a **Primary Node** at each and every Workbench Data-Center.
2. The Workbench Primary Node must be installed/upgraded prior to installing/upgrading Workbench Additional Nodes.
3. Workbench ships with its own pre-bundled Java distribution, OpenJDK11; all Workbench components will be configured through the installation to use this Java distribution and should not affect any other components that may be installed on the host.
4. The Workbench installation uses the Ant Installer component, if during the Workbench installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.
5. Use an **sudo** level account when running the Workbench *install.sh* file (do NOT use the root account).
6. If the Workbench installation is cancelled mid completion, please ensure the Workbench install directory is cleaned/purged prior to attempting another install

Warning

- **Before commencing the Workbench upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and Workbench data integrity and operation will likely be compromised.**

Warning

- Only proceed if:
  - The Workbench Primary Node has been successfully upgraded.
- The Workbench Additional Node components you wish to upgrade are Up and Running with a Status of Green

Please use the following steps to upgrade Workbench 9 on Linux:

1. Run **tar zxf Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz** to extract the downloaded *Workbench_9.x.xxx.xx_LINUX_Pkg.tar.gz* compressed file.
2. **cd** into the **ip\linux** folder.
3. Run **tar zxf Workbench_9.x.xxx.xx_Installer_Linux.tar.gz** - to extract the *Workbench_9.x.xxx.xx_linux.tar.gz* compressed tar file.
4. Run **./install.sh** (Do NOT prefix **./install.sh** with **sudo**)

5. Genesys Care Workbench 9.x

- Press **Enter** to start the Workbench upgrade.

6. Genesys Workbench License Agreement

- Press **Enter** to view the Genesys Workbench license agreement

7. Review License Agreement

- Enter **N** for the next page, or press **Enter** to scroll to the end of the Terms and Conditions

8. Genesys Workbench **Terms and Conditions**

- Press **Enter** to continue, if you agree to the Genesys Workbench Terms and Conditions

9. Workbench **Installation Mode**.

- Enter **2** for **Upgrade** - given there is already a previous release of Workbench running on this host/node.

Important

- Select **2** for Upgrade given there is already a previous release of Workbench running on this host/node.
- All the Workbench components on this particular host will be upgraded.
- All *old version* Workbench Services will be automatically stopped at end of this upgrade process.

10. Workbench Base Properties - **Installation Path**.

- Press **Enter** to accept the default **/opt/Genesys/Workbench_9.x.xxx.xx** installation path
- Or provide a new installation path - i.e. **/home/genesys/WB9** and press **Enter**

Important

- This *Installation Path* directory should be different than the current Workbench 9.x installation location.
- Choose between the **Default** or **Custom** installation type.

11. Workbench Base Properties - **Default** or **Custom**

- For Settings Type, either Default or Custom
  - Press **Enter** to accept the Default option - which enables provision of **Default paths, ports** etc
  - Type **2** and press **Enter** to choose the **Custom** option which enables provision of specific custom paths, ports etc

> **Important**
>
> - Choose between the **Default** or **Custom** installation type.
> - For the *Default* type, the respective Workbench component **Default** (including binaries, paths, config, ports etc) options will be used.
> - Or, if required, you can change these *Default* options (paths, config, ports etc) by selecting a **Custom** install.

12. Workbench **Primary ZooKeeper IP Address:Port**.

- Enter the Workbench Primary Zookeeper IP Address and Port
- Press **Enter**

> **Important**
>
> - The Primary ZooKeeper IP Address not the Hostname

13. **Installation Progress**

- The Workbench installer will now upgrade the old Workbench version to the new Workbench version

14. **Installation Complete**

- Await the **BUILD SUCCESSFUL** message which indicates the Workbench upgrade process is complete

> **Important**
>
> - Once the new Workbench version is installed, new Workbench 9.x.xxx.xx Services will be registered in the Service registry
> - The previous Workbench version Services will be automatically **Stopped** and set to **Manual**.

- The Workbench port configuration of upgraded components will be same as the Workbench **old** components.
- The Workbench data and log folders will be automatically created in the new Workbench installed location.
- At the end of the upgrade process, Workbench 9.y.yyy.yy Cluster, data and configuration will be restored as per the prior Workbench 9.x.xxx.xx installation.
- Workbench Agent *Metricbeat* will be also installed during the upgrade process; this will send Metric data from the Workbench Hosts and Processes into the Workbench Elasticsearch storage for observability via Dashboards and Visualizations

16. **Next Steps**

Important

- The Workbench Additional Node has been upgraded
- Repeat the above if there are more Workbench Additional Nodes at this Data-Center

Workbench Upgrade – Linux – Rollback to Workbench 9.0

If you encounter issues with your Workbench upgrade, we recommend opening a Genesys Support Case to progress and resolve the problem.

Please review the Troubleshooting section of this document for log collection recommendations.

However, if there is a need to rollback the version of Workbench to the previous version,, the following steps should be followed.

Workbench Single Node Deployment - Rollback/Downgrade

> ### Warning
>
> - **Use a non root account** with sudo permissions for all the commands below - DO NOT USE THE <ROOT> ACCOUNT.

Uninstall the New Workbench Version

1. Uninstall Workbench_9.1.000.00
    a. Browse to Workbench installation folder (i.e /opt/Genesys/Workbench_9.1.000.00)
    b. Locate the **uninstall.sh** file
    c. Run **uninstall.sh** (DO NOT prefix ./install.sh with sudo).
    d. Post running **uninstall.sh**, delete the Workbench */opt/Genesys/Workbench_9.1.000.00* folders

Start the previous Workbench version Services

2. Start the previous (i.e.9.0.100.00) Workbench Services manually from the Service menu
    a. service WB_ZooKeeper_9.0.100.00 start
    b. service WB_Elasticsearch_9.0.100.00 start
    c. service WB_Kibana_9.0.100.00 start
    d. service WB_IO_9.0.100.00 start
    e. service WB_Agent_9.0.100.00 start

Auto-Start the previous Workbench version Services

3. Ensure the previous (i.e. 9.0.100.00) Workbench Services start on host restart
    a. sudo chkconfig WB_ZooKeeper_9.0.100.00 on
    b. sudo chkconfig WB_Elasticsearch_9.0.100.00 on
    c. sudo chkconfig WB_Kibana_9.0.100.00 on
    d. sudo chkconfig WB_IO_9.0.100.00 on
    e. sudo chkconfig WB_Agent_9.0.100.00 on

Once the previous Workbench Services are started, navigate to **http://<WORKBENCH_HOST>:8181** to login and use the previous Workbench version.

Workbench Cluster Node Deployment - Rollback/Downgrade

> ### Warning
>
> - **Use a non root account** with sudo permissions for all the commands below - DO NOT USE THE <ROOT> ACCOUNT.

> ### Warning
>
> For Cluster deployments, once you Rollback/Downgrade Workbench, you will lose all Elasticsearch data (Alarms, Changes, Call Flow and Auditing).

Uninstall the New Workbench Version on the Primary Node

1. Uninstall the Workbench Primary Node using the above steps.
    a. Run **./uninstall.sh** in the */opt/Genesys/Workbench_9.1.000.00* folder

Uninstall the New Workbench Version on the Additional Nodes

2. Uninstall the Workbench Additional Nodes using the above steps.
    a. Run **./uninstall.sh** in the */opt/Genesys/Workbench_9.1.000.00* folder

Cleanup previous Elasticsearch

4. On ALL **previous version** Workbench nodes where ElasticSearch 9.0.100.00 is installed
    a. Navigate to **data** folder.
    b. Run **cd /opt/Genesys/Workbench_9.0.100.00/Elasticsearch/data/nodes/** - to change directory to the Eslaticsearch *data* folder
    c. Run **sudo rm -R** - to delete all files and folders present inside the Elasticsearch **data** folder.

Cleanup previous ZooKeeper

5. On all **previous version** Workbench Additional Nodes where ZooKeeper 9.0.100.00 is installed.
    a. Navigate to **data** folder.
    b. Run **cd /opt/Genesys/Workbench_9.0.100.00/ZooKeeper/data/** - to change directory to the ZooKeeper *data* folder
    c. Except the **my.id** file - delete all files and folders present inside the ZooKeeper **data** folder.

Important

1. If the **myid** file is deleted, the ZooKeeper Cluster formation will not be successful.
2. Ensure to **uninstall** ALL components of Workbench 9.1.000.00 on all Workbench Nodes of the Cluster before starting Services of Workbench previous 9.0.100.00 release as partial uninstall of the new 9.1.000.00 release can cause data corruption.

Start the previous Workbench version Services on the Primary Node

6. Start the previous (i.e. 9.0.100.00) Workbench Services manually on the Workbench 9.0.100.00 Primary Node
    a. service WB_ZooKeeper_9.0.100.00 start
    b. service WB_Elasticsearch_9.0.100.00 start
    c. service WB_Kibana_9.0.100.00 start
    d. service WB_IO_9.0.100.00 start
    e. service WB_Agent_9.0.100.00 start

Auto-Start the previous Workbench version Services on the Additional Nodes

7. Start the previous (i.e. 9.0.100.00) Workbench Services manually on the Workbench 9.0.100.00 Additional Nodes

a. service WB_ZooKeeper_9.0.100.00 start
b. service WB_Elasticsearch_9.0.100.00 start
c. service WB_Kibana_9.0.100.00 start
d. service WB_IO_9.0.100.00 start
e. service WB_Agent_9.0.100.00 start

Auto-Start the previous Workbench version Services on the Primary Node

8. Ensure the previous (i.e. 9.0.100.00) Workbench Services start on host restart on the Workbench Primary Host
    a. sudo chkconfig WB_ZooKeeper_9.0.100.00 on
    b. sudo chkconfig WB_Elasticsearch_9.0.100.00 on
    c. sudo chkconfig WB_Kibana_9.0.100.00 on
    d. sudo chkconfig WB_IO_9.0.100.00 on
    e. sudo chkconfig WB_Agent_9.0.100.00 on

Auto-Start the previous Workbench version Services on the Additional Nodes

9. Ensure the previous (i.e. 9.0.100.00) Workbench Services start on host restart on the Workbench Additional Hosts
    a. sudo chkconfig WB_ZooKeeper_9.0.100.00 on
    b. sudo chkconfig WB_Elasticsearch_9.0.100.00 on
    c. sudo chkconfig WB_Kibana_9.0.100.00 on
    d. sudo chkconfig WB_IO_9.0.100.00 on
    e. sudo chkconfig WB_Agent_9.0.100.00 on

Once the previous Workbench Services are started, navigate to **http://<WORKBENCH_HOST>:8181** to login and use the previous Workbench version.

Workbench Upgrade – Linux – Removing old version

Important

1. Only follow these instructions when Workbench has been successfully upgraded (i.e. to 9.1.000.00) and you are ready to uninstall the previous release of Workbench (i.e. 9.0.100.00) to free up space/resources.
2. Ensure and double check the previous Workbench version Workbench Services are ALL **Stopped** prior to running the **uninstall.sh** script.
3. The Workbench uninstall process permanently removes the previous Workbench Services associated with all the previous Workbench components and all files including data and logs etc.
4. If any previous Workbench data is required for archival purposes, please ensure it is saved at a separate location prior to running the uninstall script.
5. The uninstall process will leave the original configuration file used to generate the Workbench installation; this can be provided to Genesys Care if related to an installation issue.

The following steps provide instructions on uninstalling an older release of Workbench after a successful Workbench upgrade (i.e. from 9.0.100.00 to 9.1.000.00):

1. **cd** to the Workbench installation folder of the version to be removed (i.e. "/opt/Genesys/Workbench_9.0.100.00")
2. Run **./uninstall.sh** (with a sudo privileged account and not root)
3. Post running **uninstall.sh**, also delete traces of files/folders (i.e. delete the **uninstall.sh** and **ConfigFileBackup** folder).

Using Workbench

This Using Workbench section contains information on the use and configuration of Workbench and its features thereof.

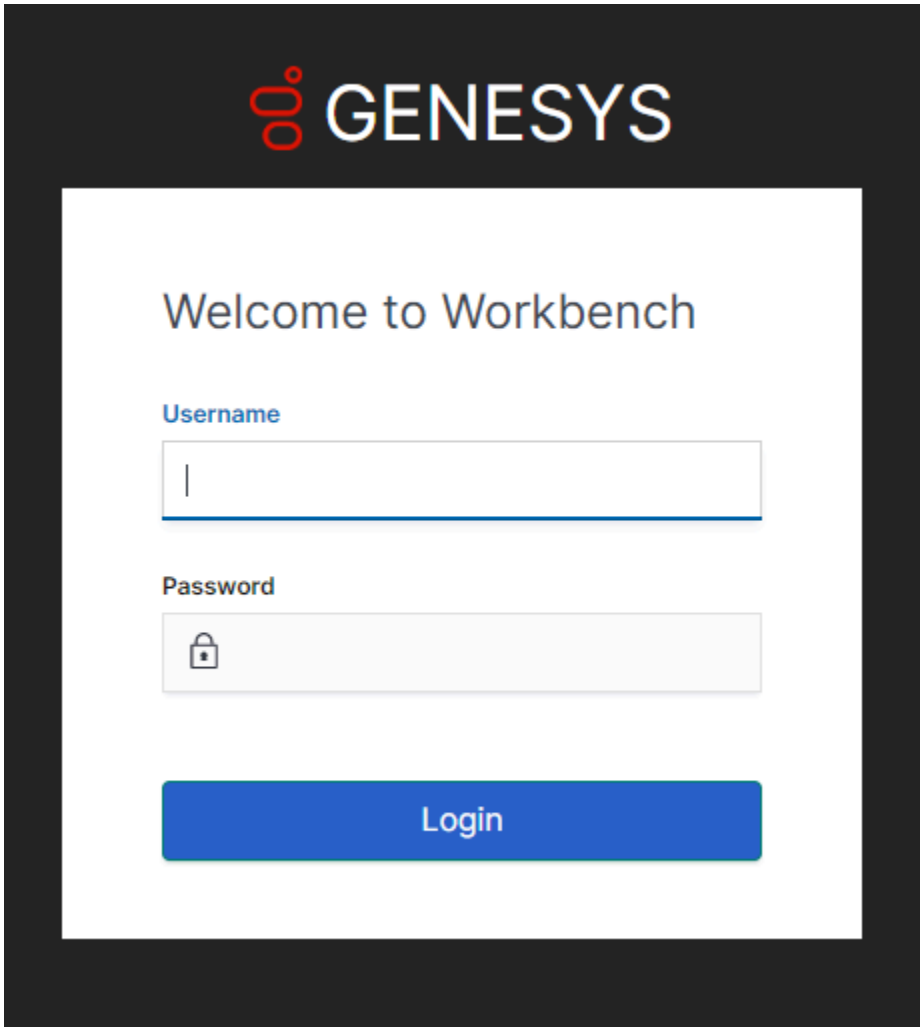
This section provides the following information:

- Logging In
- Navigation Bar
- Common Navigation Funcitonalities
- Alarm Console
- Changes Console
- Channel Monitoring
- Workbench Dashboards
- Workbench Visualizations
- Notification Channels
- Alerts
- Workbench Discover Console
- Workbench Configuration
- Workbench User Preferences

Logging In

Once Workbench has been successfully installed, please navigate to http://<WB_HOST>:8181 to login

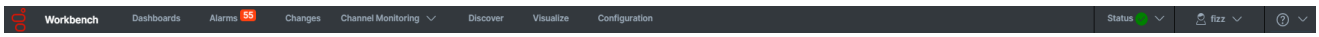
You will be presented with the Workbench login screen below:



Please use your Genesys Engage Configuration Server (CME) login credentials to authenticate and login to Workbench.

Once logged-in you will be presented with the Workbench Home Dashboard ("_Genesys Home") by default, this 'Start-up' page can be changed via User Preferences.

Navigation Bar



The Workbench navigation bar is located at the top of the browser, it provides the following navigation options:

- Dashboards
- Alarms
- Changes
- Channel Monitoring
  - Call Flows
  - Media
  - Reports
- Discover
- Visualize
- Configuration
  - Overview
  - General
  - Applications
  - Hosts
  - Data-Centers
  - Auditing
- Status
- User
  - User Preferences
  - Logout
- Help
  - Help
  - About

Alarm Console

The Workbench Alarm is a dedicated console that displays a real-time statistics summary of active alarms, as well as a real-time data-table of active and historic alarms.

The statistics summary displays Total, Critical, Major and Minor metrics for:
All Source Active Alarms, from Workbench and Genesys Engage
Workbench Active Alarms, from only Workbench
Genesys Engage Active Alarms, from only Genesys Engage

The real time data-table displays the below listed details of all alarms, be those active or closed. Every column is provided with a sorting/searching option based on its data type, which makes the alarm identification much easier.

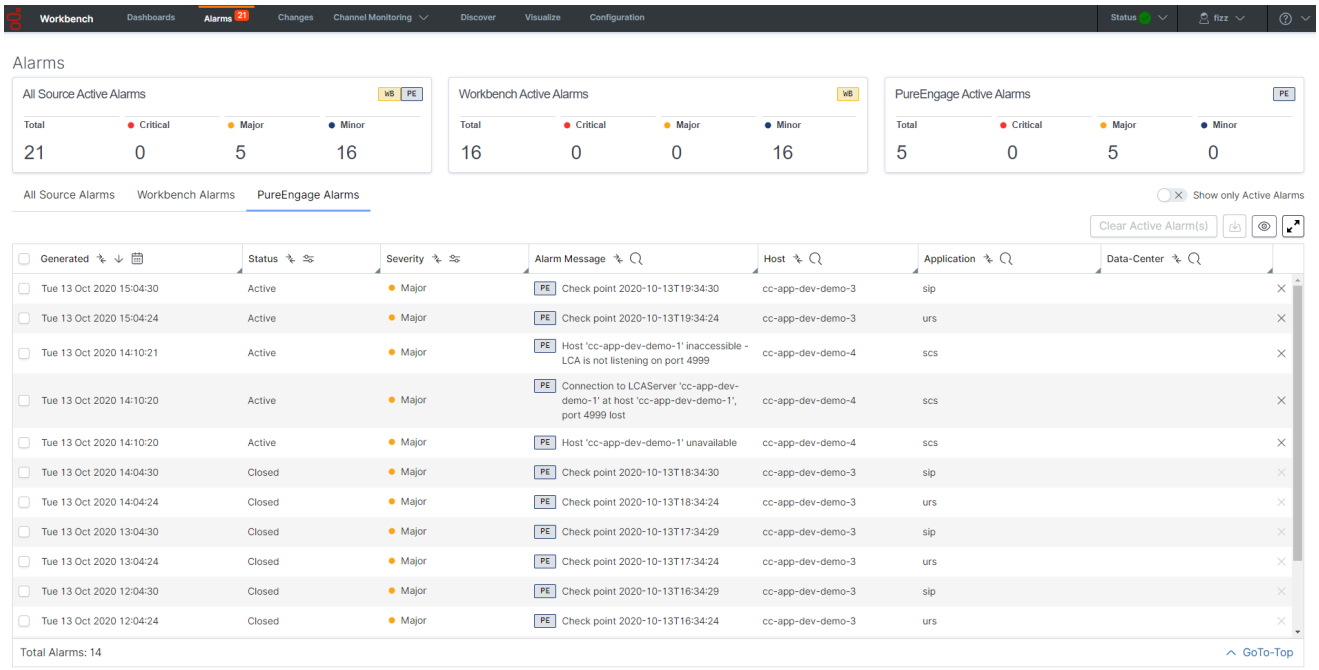
- The different data information of an alarm is segregated as columns in the data-table.
  - **Generated** - The date and time of an alarm generation.
    - Note: Timestamps are stored in UTC and translated to local time based on the Users Browser Time-Zone
  - **Status** - Indicates if the alarm event status is Active/Closed.
  - **Severity** - Denotes the severity of the alarm event. It can be Critical, Major or Minor.
  - **Alarm Message** - The message about the alarm event in text format.
  - **Host** - The name of the Host/Server associated to the alarm event.
  - **Application** - The name of the application associated to the alarm event.
  - **Data-Center** - The name of the Data-Center associated to the alarm (Workbench only not Engage) event.
  - **Sent to RAM Service** - The date and time by when the alarm event was sent to the Genesys Remote Alarm Monitoring (RAM) Service.
  - **Expiration** - The time (in seconds) by when the alarm event will automatically expire/clear.
  - **Cleared** - The date and time at when the alarm event was cleared.
  - **ID** - The internal ID of the alarm event.

The real time data-table is also equipped with the following buttons for easy sort, filter and export options.

- Show only Active Alarms - A filter to show only the active alarms available
- Clear Active Alarm: a DataTable row icon to Close/Clear a single Alarm
- Clear Active Alarm(s): a button to Close/Clear multiple/selected (max 200 at a time) active Alarm
- Export - Gives the option to export the data-table in either PDF or Excel format
- Column Visibility - Gives the option to show/hide the columns that you prefer.
- Normal/Full-Screen - To toggle between the normal and full screen mode.

- Column Reordering - Allows to move columns left or right within the data-table.
- Column Search/Filter - Filter data-table events based on Date & Time, drop-down filter or text searches
- Column Sort
  - 'Generated' and 'Sent to RAM Service'

An example Workbench **Alarm Console** shown below:



Alarm Console and Workbench Data-Center Synching

Important

- Post a Workbench Data-Center sync, **only Active Alarms** will be synced; Engage Alarms are not synched because each Workbench Data-Center IO component has it's own integration to the Engage Solution Control Server (SCS) component and therefore synching is not required.

Alarm Console Counters

Important

- If/when bulk Alarms are cleared via GA/GAX/SCI there may be a slight delay in the Workbench Alarm Counter updates

Changes Console

The Workbench Configuration **Changes** Console is a dedicated console that displays a real-time statistics summary as well as a data-table of historic Workbench and Genesys Engage Configuration Changes.

> ### Important
>
> - Currently Workbench is limited to tracking/displaying Genesys Engage CME **Host**, **Application** and **Solution** objects only; all other CME objects are not monitored by Workbench

The statistics summary being Configuration Changes that occured Today, Yesterday, This Week, Last Week, This Month, Last Month for:

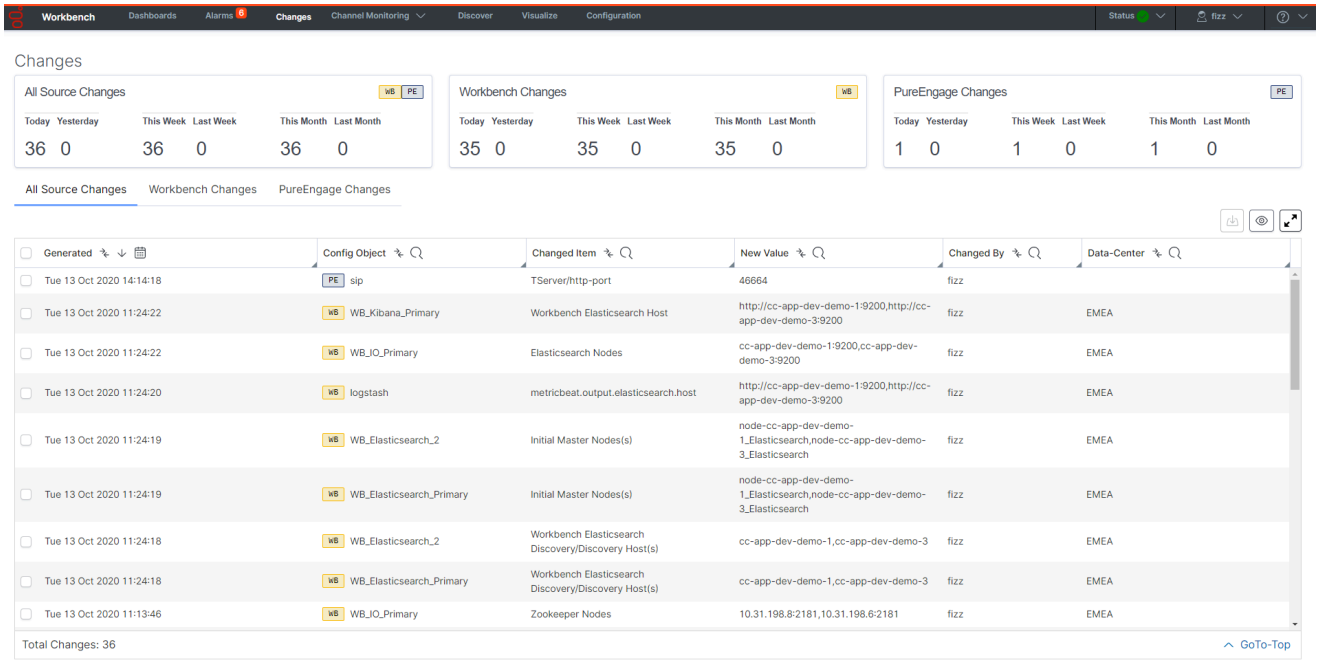
- All Source Changes; Changes from Workbench and Genesys Engage
- Workbench Changes; Changes only from Workbench
- Genesys Engage Changes; Changes only from Genesys Engage

The Changes Console also provides a real time data-table of historic Changes, from either Workbench and Genesys Engage (All Source Changes), Workbench only Changes or Genesys Engage only Changes; the Changes data-table provides the following functionality:

- Columns
  - **Generated** - the generation DateTime of this Change event
    - Note: Timestamps are stored in UTC and translated to local time based on the Users Browser Time-Zone
  - **Config Object** - the particular Object of this Change event
  - **Changed Item** - the Item of this Change event
  - **New Value** - the new value of this Change event
  - **ChangedBy** - the User who actioned the change
  - **Data-Center** - the associated Data-Center
  - **ID** - the internal ID of this Change event
  - **DB ID** - the internal DB ID of this Change event
- Export
  - PDF or XLS
- Column Visibility

    - Show/Hide columns
- Normal/Full-Screen
- Column Reordering
    - move columns left or right within the data-table
- Column Search/Filter
    - Filter data-table events based on DateTime, drop-down or text searches
- Column Sort
    - 'Generated' and 'Sent to RAM Service

An example Workbench **Changes Console** shown below:



Changes Console **ChangedBy** field for Genesys Engage Changes

For the Changes Console **ChangedBy** field to be accurate (not "N/A"), the following Genesys Engage configuration is required:

- A connection from the respective Genesys Engage Configuration Server or Configuration Server Proxy to

the Genesys Engage Message Server that Workbench is connected to.

- If not already, **standard=network** added to the **log** section of the Configuration Server or Configuration Server Proxy that Workbench is connected to.

Changes Console and Workbench Data-Center Synching

Important

- Post a Workbench Data-Center sync, existing Workbench Changes will be synced based on the Workbench Retention Period; Engage Changes will not be synched because each Workbench Data-Center IO component has it's own integration to the Engage Configuration/Message Server components and therefore synching is not required.

'

Channel Monitoring

With the Workbench ‘Channel Monitoring’ feature, create, schedule and manually initiate SIP **voice** test calls into you're Engage platform to proactively identify potential interaction and routing issues before your customers are impacted; this feature tests voice SIP/IVR/DTMF/PROMPT menu call flows, ensuring your service is functioning as designed and raising alarms within the Workbench Alarms Console when errors are encountered.

> ### Important
>
> - To utilise the Channel Monitoring feature of Workbench, your environment must have a Genesys SIP Server 8.1 or higher and DN’s configured for use as the "Destination" and "Caller User" DN's for Channel Monitoring initiated test calls.

With the Workbench Channel Monitoring feature you can:

- Create and run SIP/IVR contact center voice test calls
- Schedule recurring voice test calls to continuously monitor the health of the call processing environment
- Model Call Flows through IVR menus and routing to contact centre Agents
- Visualise Channel Monitoring Call Flow Statistics
- Control Call Flows with *Edit*, *Stop/Start*, *Schedule* and *Manual Test* capabilities
- Generate Channel Monitoring reports on Call Flow test results, call quality (jitter), and other call test metrics
  - Reports available:
    - Call Metrics
    - Call Stage Results
    - Call Results
    - Call Details
- Configure Channel Monitoring thresholds for various call test parameters and error conditions
  - Whenever a configured threshold is exceeded, a Workbench alarm will be generated - visible via the Workbench "Alarms" Console
  - These alarms can then be correlated with alarms, configuration changes to help diagnose problems that may have occurred

The following sections will guide you on:

- Creating Channel Monitoring Call Flows and Call Stages

- Call Flow Schedules
- Call Flow Alarms
- Statistic Summary
- Uploading Media Files
- Generating Reports

Channel Monitoring

Workbench Channel Monitoring; ensure call routing is functioning as designed and alert when issues are encountered

Key Features/Benefits

- A dedicated Workbench Channel Monitoring (CM) Console
- Workbench CM tests Engage SIP voice call routing to ensure call flows are functioning as designed
- Workbench CM raises Alarms if/when CM Call Flows encounter failures
- Schedule CM Call Flows for regular automated testing
- Manual CM Call Flow initiation for ad-hoc testing
- A CM Console data-table view of CM Call Flows etc with filtering and export
- CM Reporting to gain insights into call test results, failures and metrics

GENESYS

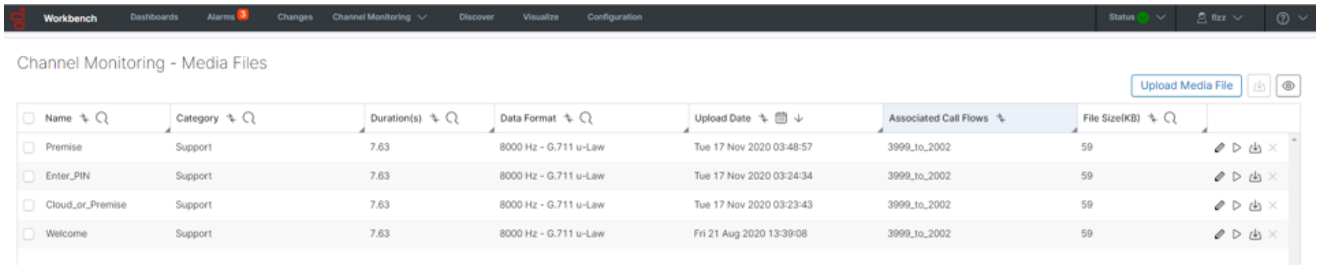
Example Call Flow

Scenario

- A customer calls 555-123-456 and hits Genesys SIP Server Routing Point 9999
- A “Welcome to Genesys Customer Care” prompt is played to the customer
- A “Is your call related to Cloud or Premise” prompt is played to the customer
- The customer speaks “Premise”
- A “Please enter your PIN number” prompt is played to the customer
- The customer enters “12345#” on their DTMF keypad
- The call is routed to a Contact Centre Agent

Workbench Channel Monitoring Requirements - for the above example scenario

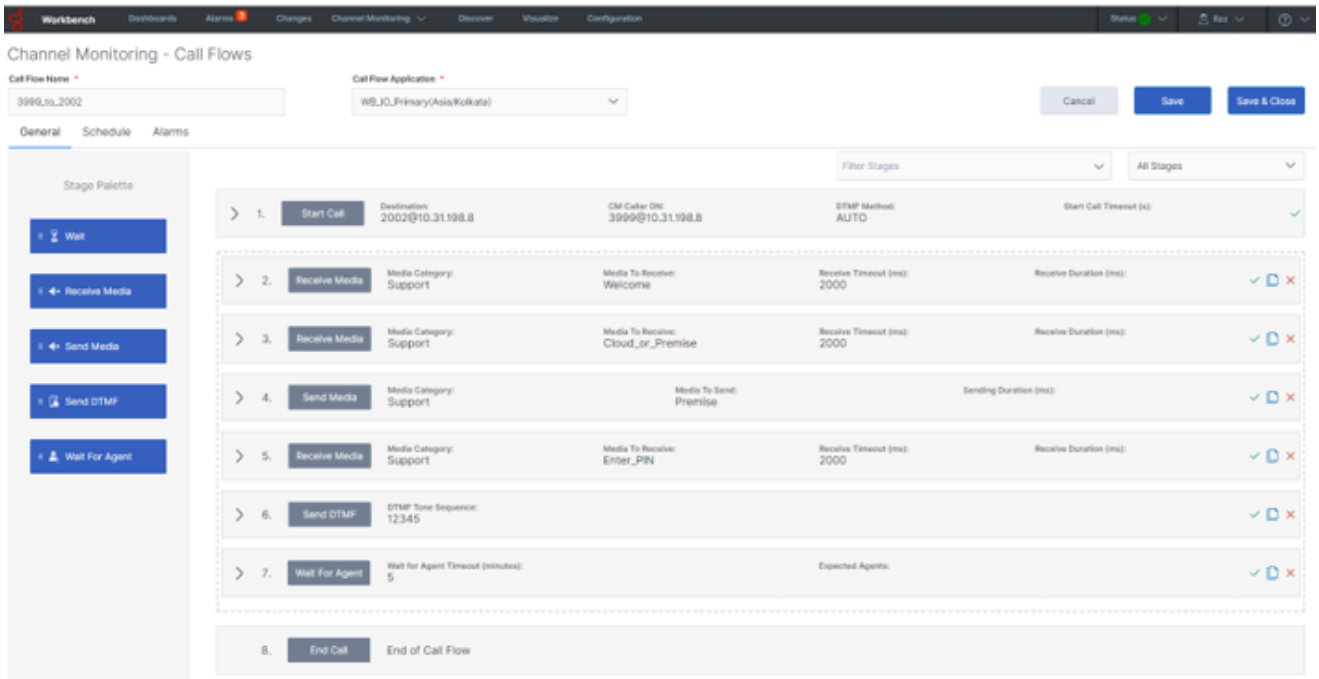
- A SIP Server DN to initiate the test call from Workbench to SIP Server
  - This is the "Destination" field of the Call Flow **Start Call** Stage - Workbench uses this DN to initiate the test call
- The exact “Welcome to Genesys Customer Care” prompt - uploaded to Workbench via the Channel Monitoring / Media Files menu
  - Channel Monitoring only accepts G.711 Mu Law - pcmu/8000 and G.711 A Law - pcma/8000 Media Files.
  - This will be used in the Call Flow **Receive Media** stage - Workbench will compare and progress/fail the Call Flow accordingly based on the received media
    - These files are used to compare what is expected to be received/sent; the comparison is duration [length of media file] based, not content.
- The exact “Is your call related to Cloud or Premise” prompt - uploaded to Workbench via the Channel Monitoring / Media Files menu
  - Channel Monitoring only accepts G.711 Mu Law - pcmu/8000 and G.711 A Law - pcma/8000 Media Files.
  - This will be used in the Call Flow **Receive Media** stage - Workbench will compare and progress/fail the Call Flow accordingly based on the received media
- A “Premise” prompt - uploaded to Workbench via the Channel Monitoring / Media Files menu
  - Channel Monitoring only accepts G.711 Mu Law - pcmu/8000 and G.711 A Law - pcma/8000 Media Files.
  - This will be used in the Call Flow **Send Media** Stage to inpersonate a human speaking "Premise"
- A “Please enter your PIN number” prompt uploaded to Workbench via the Channel Monitoring / Media Files menu
  - Channel Monitoring only accepts G.711 Mu Law - pcmu/8000 and G.711 A Law - pcma/8000 Media Files.
  - This will be used in the Call Flow **Receive Media** stage - Workbench will compare and progress/fail the Call Flow accordingly based on the received media



Workbench Channel Monitoring Call Flow “Stages”

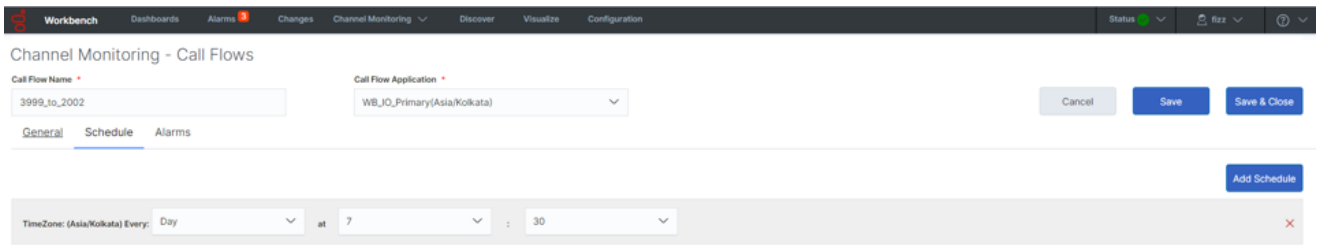
- Build the Workbench Call Flow to match the Customer Care Routing Point 9999 flow

- The Call Flow uses these Stages:
  - Start Call
  - Receive Media
  - Send Media
  - Send DTMF
  - Wait For Agent
  - End Call



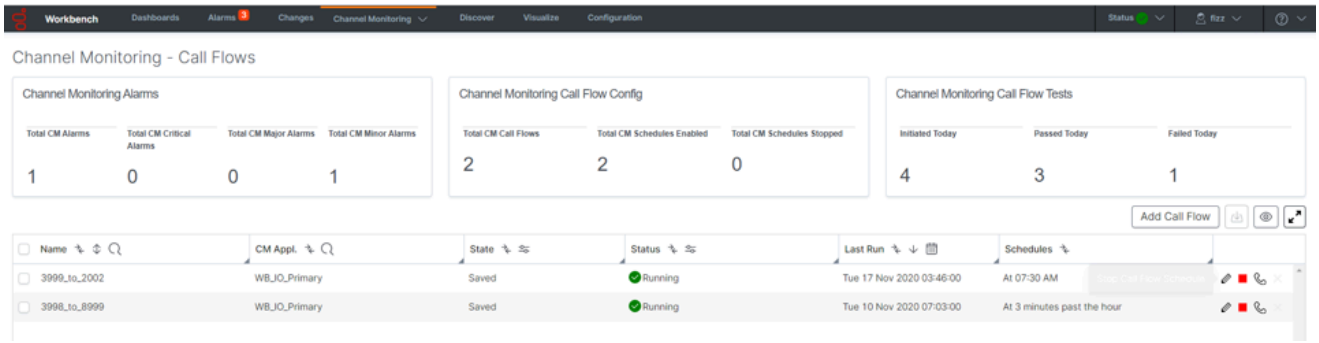
Workbench Channel Monitoring Call Flow “Schedule”

- The Call Flow will be tested, based on the Call Flow Schedules every day at 07:30 via the WB_IO_Primary application that’s deployed in Chennai, India



Workbench Channel Monitoring Call Flow “Started”

- The Call Flow 3999_to_2002 is “Started” and will initiate test calls based on the associated Schedule (i.e. 07:30)



CM - Call Flow Summary

The **Channel Monitoring Call Flow Summary** page enables real-time visibility of Call Flows, their respective statuses and also Call Flow Statistics:

- Post installation there will be no Call Flows displayed in the Call Flow Summary table.
- Follow the **CM - Add a New Call Flow** section to create your first Channel Monitoring Call Flow
- Once you've created a Call Flow it will appear in the Call Flow Summary table

The Channel Monitoring Console provides a real time data-table of Call Flows and their status; the CM Call Flow Summary table provides the following functionality:

- Columns
  - **Name** - the generation Date/Time of this Change event
    - Note: Timestamps are stored in UTC and translated to local time based on the Users Browser Time-Zone
  - **CM Appl.** - the particular Object of this Change event
  - **State** - the Item of this Change event
  - **Status** - the new value of this Change event
  - **Last Run** - the User who actioned the change
  - **Schedules** - the internal ID of this Change event
  - **Data-Center** - the Data-Center this Call Flow is associated with
- Export
  - PDF or XLS
- Column Visibility
  - Show/Hide columns
- Normal/Full-Screen
- Column Reordering
  - move columns left or right within the data-table
- Column Search/Filter
  - Filter data-table events based on DateTime, drop-down or text searches
- Column Sort
  - 'Name' and 'Last Run' columns

At the end of each Call Flow row there are options to:

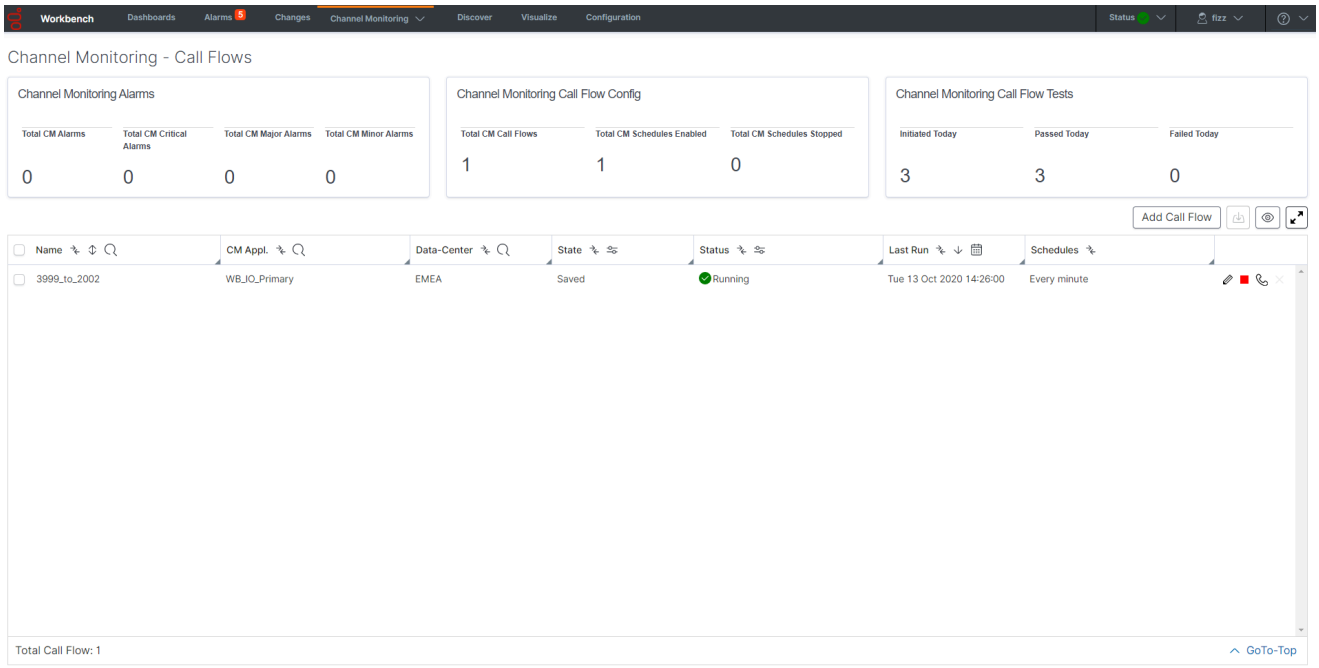
- **Edit** the Call Flow, select the **Pencil** button.
- **Start/Stop** the associated Call Flow Schedule, select either the **Play** or **Stop** button.
  - Note: the Call Flow needs to be in the **Ready** state, all config complete, to be able to Start the Call Flow Schedule
- **Initiate a Manual Call** for the respective Call Flow - the **Phone** button.
  - Note: the Call Flow needs to be in the **Ready** state, all config complete
- **Delete** the Call Flow, select the **Close** button.
  - Note: the Call Flow will be permanently deleted; no Media Files can be associated with a Call Flow to enable deletion

The Call Flow Summary page also provides:

- **Export** the Call Flow summary list to XLS or PDF the **Download** button.
- **Show/Hide** Call Flow table columns, select the **Eye** button.
- **Expand/Collapse** (full-Screen On/Off) the Call Flow table, select either the **Expand** or **Collapse** arrow button.

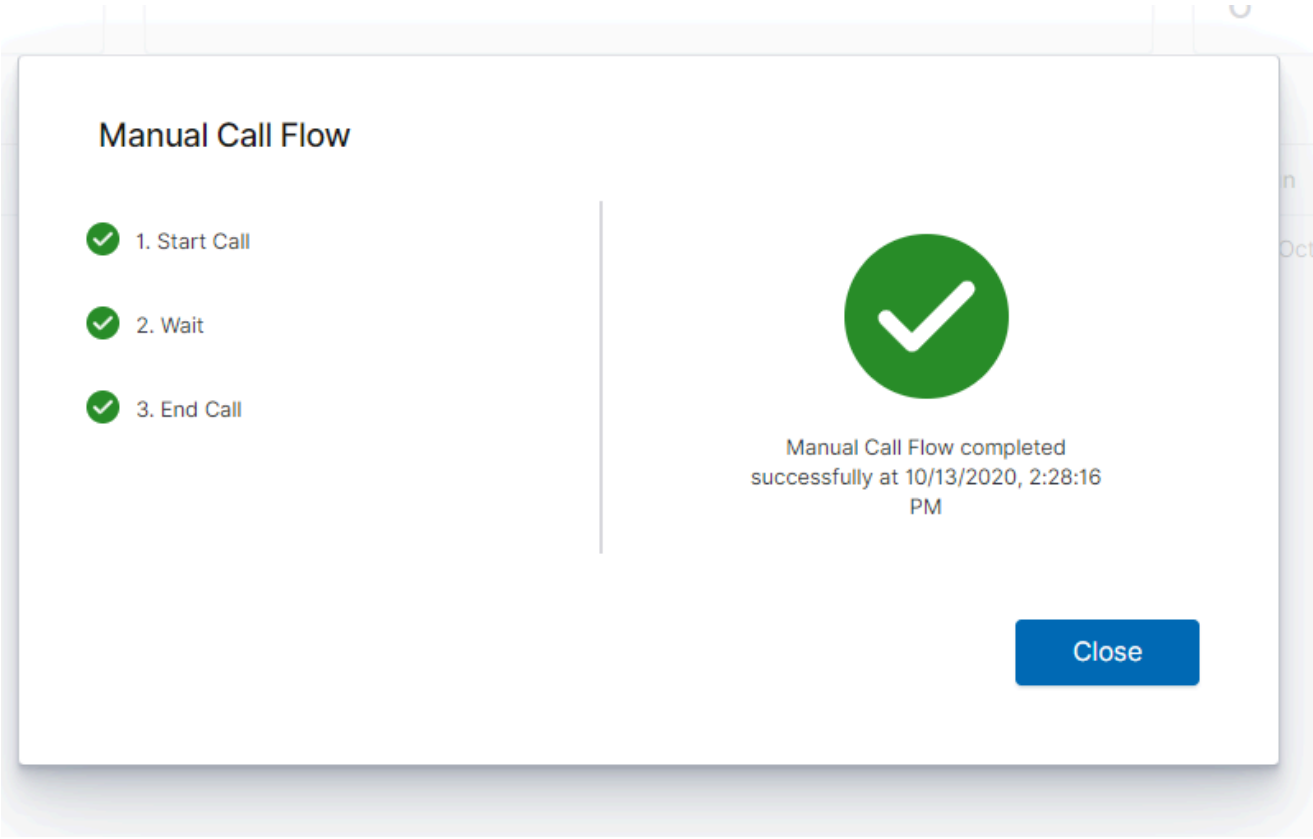
> **Important**
>
> - If/when Workbench Data-Center nodes/Clusters are synchronized, to form a **distributed Workbench deployment**, the Channel Monitoring feature is holistic, whereby, Channel Monitoring Call Flows, Media Files and Reports can be managed irrespective of the local Workbench Data-Center the user is logged into.

Call Flow Summary Example



Manual Call Flow Test

An example Call Flow **Manual** Call Flow test:

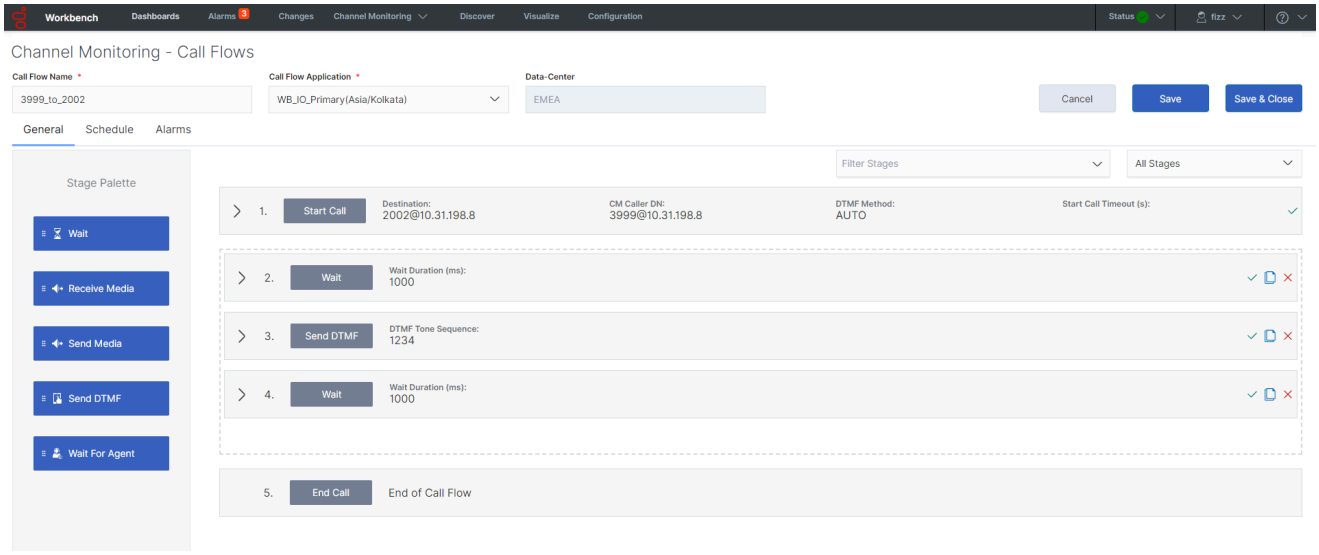

Manual Call Flow
1. Start Call
2. Wait
3. End Call
Manual Call Flow completed successfully at 10/13/2020, 2:28:16 PM
Close

CM - Add a New Call Flow

Channel Monitoring (CM) **Call Flows** are the primary templates for testing voice call routing, be that a simple call to a SIP DN or a call that navigates through an IVR with DFMT and speech recognition functionality and finaling connecting to a contact centre agent.

A Channel Monitoring Call Flow defines the different **Stages** in which a call will execute against the system that is being tested.

1. Select **Channel Monitoring > Call Flows** from the Workbench top navigation bar.
    1. The Call Flow Summary page is presented
2. Click the **Add Call Flow** button above the Call Flow data-table list to create a new Call Flow.
    1. The *Channel Monitoring - Call Flows* Edit page will be displayed; see example screen below
3. Enter a unique name in the **Call Flow Name** field - i.e. "TEST_2999_to_RP_8001" - to optimize sorting use either upper or lower case but avoid using both
4. Select the **Call Flow Application** from the dropdown list - i.e. "WB_IO_Primary"
    1. This is the Workbench IO application that will initiate the CM test calls
    2. The Data-Center field will be auto populated based on the Data-Center of the WB IO application
5. The mandatory **Start Call** and **End Call** Stages are pre-populated in the Call Flow Stages list



Building the Call Flow

- To build a Call Flow that will test your specific routing requirement, simply drag and drop a **Stage** from the **Stage Palette** on the left into the Call Flow Stages list window.
- From within the Call Flow Stages list, click on a specific Stage to expand, display and edit it's properties; see the **Send DTMF** Stage example above.
- Call Stages can be reordered within the list by dragging them up/down to the desired location.
- Please see **CM - Call Flow Stages** section for the description and usage of each call stage.
- Perform the necessary Call Flow modifications to match the desired test of your call routing.
- Click the **Save** or **Save & Close** button.

Call Flow Edit Functionality

- The **Cancel** button cancels Call Flow Edit mode and redirects back to the Channel Monitoring Call Flow Summary page
- The **Save** button saves the current configuration and the user remains in edit mode
- The **Save & Close** button saves the current configuration and redirects the user back to the Channel Monitoring Call Flow Summary page
- The Green **Tick** icon on the Stage row indicates this Stage has been fully configured
- The **Note with Pencil** icon on the Stage row indicates this Stage has NOT been fully configured
  - As such this Call Flow will have a **Draft** State as opposed to a **Ready** State
- The **Copy** icon on the Stage row copies (below) this Stage
- The Red **Delete** icon on the Stage row deletes this Stage

Important

- Every Call Flow requires it's own dedicated SIP Server DN.
- For example if you plan to test 5 x Genesys SIP/GVP call flows then you will need 5 x SIP Server DN's for the Channel Monitoring **Start Call** Stage and it's associated **Caller User** property.

CM - Call Stages

Call Flows are built with various Stages.

The Call Flow **Stages** within Channel Monitoring being:

- Start Call
- Receive Media
- Send DTMF Tone
- Send Media
- Wait for Agent
- Wait
- End Call

> **Important**
> Every Call Flow will/must begin with a Start Call stage and end with an End Call stage. All other Stages are optional, and can be added to the Call Flow in any order to build the Call Flow required for testing a specific call routing journey. The Call Stages and their properties are detailed in the sections below.

Start Call Stage

Registers the Workbench **Caller User** SIP account and initializes the call; this is the first stage of every Call Flow.

Properties:

- Destination (required):
  - The destination DN and IP address (i.e. a Genesys SIP Server RP)
  - Required Format: "DN@IPaddress"
- Caller User (required).
  - The DN that will be used to place the call from Channel Monitoring (as configured in the Genesys SIP server)
  - Required Format: “DN@IPaddress”
- Caller Password (required)
  - The password for the calling DN (as configured in the Genesys SIP server; enter the DN if no

password assigned)

- DTMF Method (required)
  - The method that will be used for sending DTMF tones with this Call Flow
  - Possible Options:
    - RTP:As defined in RFC 4733
    - SIP INFO:Sends the tones using out-of-band SIP INFO messages
    - INBOUND: Audio tones are sent in the RTP stream
    - AUTO: Uses RTP DTMF, and if not available, uses INBAND DTMF
- Start Call Timeout
  - The timeout in seconds for the initialization of the call.
    - This value can be any positive integer; if no value is entered, or the specified value is not in the correct format, the default value of 30 seconds is used.

Receive Media Stage

Listens for media to be sent from the Call Flow under test; the media that will be selected for this stage must be uploaded through the Channel Monitoring **Media Files** upload page.
See the *CM - Upload Media Files* section for additional details.

> **Important**
> Note: the comparison is duration [length of media file] based, not content.

Properties:

- Media Category (required)
  - The user-defined category to filter the media; this is created when a Media file is uploaded to Workbench Channel Monitoring and is used for organizing (i.e. "Support", "Sales") the media files.
- Media To Receive (required)
  - The media that is expected to be sent by the Call Flow under test
- Receive Timeout (required)
  - The timeout is in milliseconds; if media is not received from the Call Flow under test before this time elapses, then the test call fails and, if configured, an alarm is raised.
- Receiving Duration (optional)
  - The duration in milliseconds of the length of the media to be received; if no value is specified, then

the length of the selected media file is used.

> **Important**
> Please read the *Stages and Media Files* section below for important information about ongoing maintenance.

Send DTMF Tone Stage

Sends a DTMF tone to the call routing system/flow under test.

Properties:

- DTMF Tone Sequence (required)
  - The sequence of digits/tones that will be sent to the System Under Test.
  - Required Format: at least one digit but a sequence of digits can be specified. For example: 112233

Send Media Stage

Sends media to the call routing system/flow under test; the media that will be selected for this stage must be uploaded through the media upload page. See the “Upload Media” section for additional details.

Properties:

- Media Category (required)
  - The user-defined category to filter the media; this is created when a Media file is uploaded to Workbench Channel Monitoring and is used for organizing (i.e. "Support", "Sales") the media files
- Media To Send (required)
  - The media that is to be sent by the test call
- Sending Duration (optional)
  - The duration in seconds of the media that will be sent to the call. If no value is specified, then the file is played in its entirety.

> **Important**
> Please read the *Stages and Media Files* section for important information about ongoing maintenance.

Wait for an Agent Stage

Waits for a response from an Agent and records the length of time before connecting with an Agent; the Stage can be configured to accept a connection from any Agent or from a *white-list* of appropriate contacts.

- Wait for Agent Timeout:
  - Maximum time in minutes to wait for connecting to an Agent; if this maximum time is exceeded, the call fails and, if configured, an alarm is raised.
  - This value must be an integer; if no value is entered, or the specified value is not in the correct format, the default value of 5 minutes is used.
- Expected Agents: (optional)
  - The list of Agent DN's that will determine the success of a transfer if a connection is made to any Agent in the list.
  - If the list is left blank, the success of the transfer is determined by a connection to *any* Agent in the environment.
  - Required Format:
    - If transfers from your routing strategy to the Agent are using a "Refer" message, the agents should be listed as:
      - **DN@agentIpAddress**
    - If transfers from your routing strategy to the Agent are completed via a "Re-Invite," the agents should be listed as:
      - **agentIpAddress**
  - If you are not sure which transfer method is used, you can include entries for both "Refer" and "Re-Invite" transfer formats, and Channel Monitoring will accept both formats.

Wait Stage

Waits for a specified period of time (milliseconds) before proceeding to the next stage of the Call Flow.

Properties:

- Wait Duration: (required)
  - The time in **milliseconds** for the Stage to wait

End Call Stage

Terminates/ends the call when the Call Flow reaches this stage; this Stage is required/fixed as the final stage for all Call Flows.

Properties: None

Stages and Media Files

Before executing a call, Channel Monitoring extracts the required audio files from the database and stores them on a directory located in the <Workbench Installation directory>/cm_cache path; these audio files are the items configured on the Send Media and Receive Media stages.

> ### Important
> In time, this directory can grow if there are a high number of different media files and Call Flows. Genesys recommends that users periodically check this directory and delete all of its contents if space is needed. This is a safe operation as long as no Call Flow that needs one of these audio files is executing at the same time as the deletion.

CM - Editing Call Flows

The following are the steps to be followed to edit a Call Flow:

1. Select **Channel Monitoring** > **Call Flows** from the Workbench navigation bar.
2. The existing Call Flows will be displayed in the Call Flow Summary table.
3. To edit a particular Call Flow, select the **Pencil** button on that specific Call Flow row.
4. The **Edit Call Flow** page is displayed. The properties of the selected Call Flow will be populated accordingly.
5. Click on any Stage or field to edit.
6. Perform the necessary modifications.
7. Click the **Save** or **Save & Close** button.

Deleting Call Flows

The following are the steps to be followed to **Delete** a Call Flow:

1. Select **Channel Monitoring > Call Flows** from the Workbench navigation bar.
    1. The existing Call Flows will be displayed in the Call Flow Summary table.
2. To delete a particular Call Flow, select the **Delete Call Flow** button on that specific Call Flow row.
    1. A Warning confirmation dialog is presented
        1. The deletion of the Call Flow and it's associated data is permanent
3. Either click **Cancel** to avoid deleting the Call Flow or...
4. Check the **Impact(s) Understood and Accepted** dialog and click the **Delete** button to continue

> ### Important
> A Call Flow with a **Status** of **Running** cannot be deleted; please stop the Call Flow Schedule first to commence deletion of the Call Flow.

CM - Call Flow Schedules

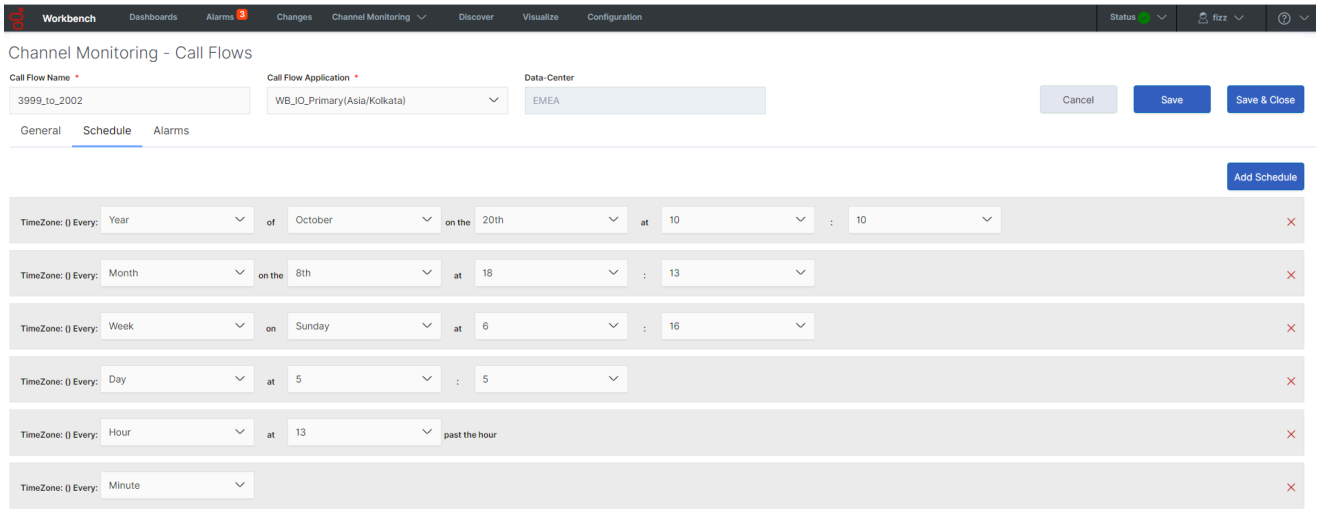
Schedules can be assigned to Call Flows to enable recurring automated tests.

The following are the steps to be followed to assign a Call Flow Schedule:

1. Select **Channel Monitoring > Call Flows** from the Workbench navigation bar.
    1. The existing Call Flows will be displayed in the Call Flow Summary table.
2. To edit a particular Call Flow, select the **Pencil** button on that specific Call Flow row.
    1. The Edit Call Flow page is displayed; the properties of the selected Call Flow will be populated accordingly.
3. Select the **Schedule** tab
    1. A "Currently there are no Schedules associated with the Call Flow" message is presented. i.e.: no Schedules are yet configured
4. Click **Add Schedule** to add a Schedule to the Call Flow
5. From the drop-down list select the Schedule frequency; Every Minute, Hour, Day, Week, Month, Year
    1. For the Every Hour, Day, Week, Month, Year frequencies further details are required such as Month, Day, Hour, Minute parameters
6. Configure your Schedule as per your requirements
7. Add more Schedules if needed
8. Once complete, click the **Save** or **Save & Close** button.

Call Flow Schedule Example

The example image below details the Schedule options for Call Flows:


Workbench
Dashboards
Alarms 3
Changes
Channel Monitoring
Discover
Visualize
Configuration
Status
fizz
Channel Monitoring - Call Flows
Call Flow Name *
3999_to_2002
Call Flow Application *
WB_IO_Primary(Asia/Kolkata)
Data-Center
EMEA
Cancel
Save
Save & Close
General
Schedule
Alarms
Add Schedule
TimeZone: () Every: Year of October on the 20th at 10 : 10
TimeZone: () Every: Month on the 8th at 18 : 13
TimeZone: () Every: Week on Sunday at 6 : 16
TimeZone: () Every: Day at 5 : 5
TimeZone: () Every: Hour at 13 past the hour
TimeZone: () Every: Minute

CM Call Flow Alarms

Workbench Alarms can and are assigned by default to each Call Flow

If/when a Call Flow encounters an issue, a Workbench Alarm will be raised accordingly.

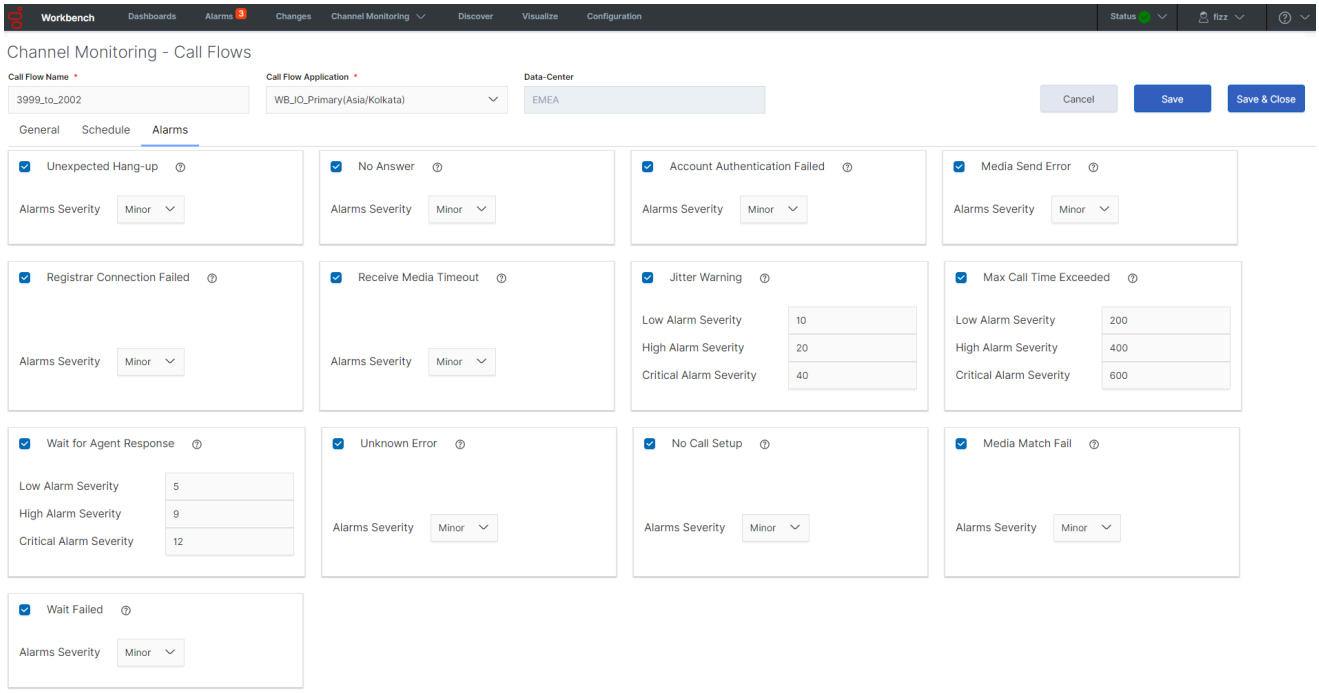
These Channel Monitoring Alarms can be viewed via the Alarms Console and/or via Channel Monitoring Reports.

Please use the following steps to assign/configure Call Flow Alarms:

1. Select **Channel Monitoring > Call Flows** from the Workbench navigation bar.
    1. The existing Call Flows will be displayed in the Call Flow Summary table.
2. To edit a particular Call Flow, select the **Pencil** button on that specific Call Flow row.
    1. The Edit Call Flow page is displayed; the properties of the selected Call Flow will be populated accordingly.
3. Select the **Alarms** tab
    1. The default settings are displayed; ALL Alarm types are enabled by default
4. The Alarm type modification parameters being:
    1. Enable
    2. Disable
    3. Severity
    4. Threshold (if applicable)
5. Once complete, click the **Save** or **Save & Close** button.

Call Flow Alarms Example

The example image below details the Alarms options for Call Flows:


Workbench
Dashboards
Alarms 3
Changes
Channel Monitoring
Discover
Visualize
Configuration
Status
fizz
Channel Monitoring - Call Flows
Call Flow Name *
3999_to_2002
Call Flow Application *
WB_IO_Primary(Asia/Kolkata)
Data-Center
EMEA
Cancel
Save
Save & Close
General
Schedule
Alarms
Unexpected Hang-up
Alarms Severity
Minor
No Answer
Alarms Severity
Minor
Account Authentication Failed
Alarms Severity
Minor
Media Send Error
Alarms Severity
Minor
Registrar Connection Failed
Alarms Severity
Minor
Receive Media Timeout
Alarms Severity
Minor
Jitter Warning
Low Alarm Severity
10
High Alarm Severity
20
Critical Alarm Severity
40
Max Call Time Exceeded
Low Alarm Severity
200
High Alarm Severity
400
Critical Alarm Severity
600
Wait for Agent Response
Low Alarm Severity
5
High Alarm Severity
9
Critical Alarm Severity
12
Unknown Error
Alarms Severity
Minor
No Call Setup
Alarms Severity
Minor
Media Match Fail
Alarms Severity
Minor
Wait Failed
Alarms Severity
Minor

CM - Uploading Media Files

Channel Monitoring Media Files are uploaded via the **Channel Monitoring - Media Files** page.

The uploaded media is used for the **Receive Media** and **Send Media** Call **Stages** of a Call Flow.

Please ensure you upload .WAV audio files with the following supported audio codecs:

- G.711 Mu Law - pcmu/8000
- G.711 A Law - pcma/8000

> **Important**
> Channel Monitoring only accepts **G.711 Mu Law - pcmu/8000** and **G.711 A Law - pcma/8000**.

> **Important**
> Channel Monitoring will automatically detect the codec negotiated between the peers of a call and execute the necessary transcoding while sending media so that the output audio matches the codec of the call.

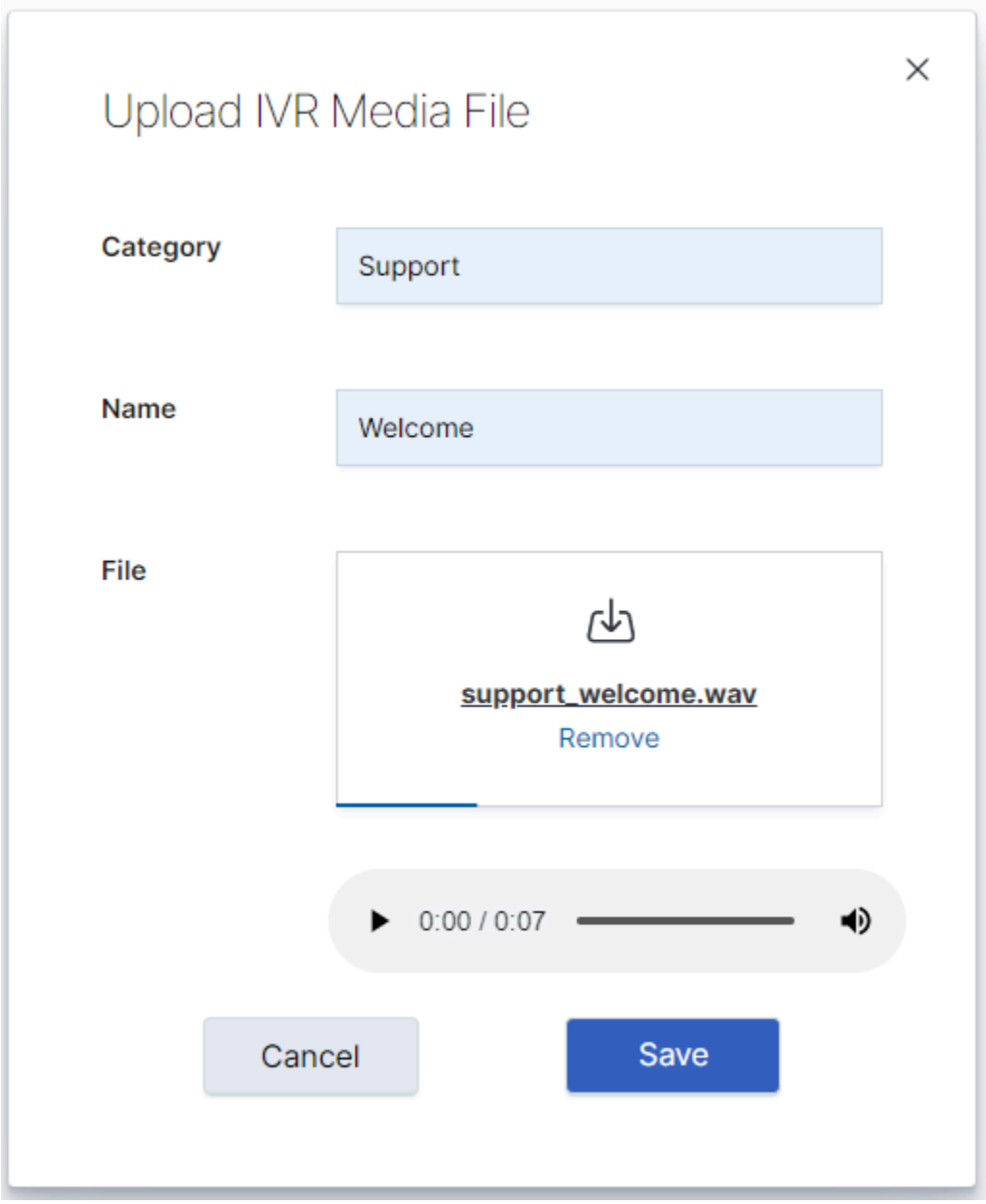
Adding New Media

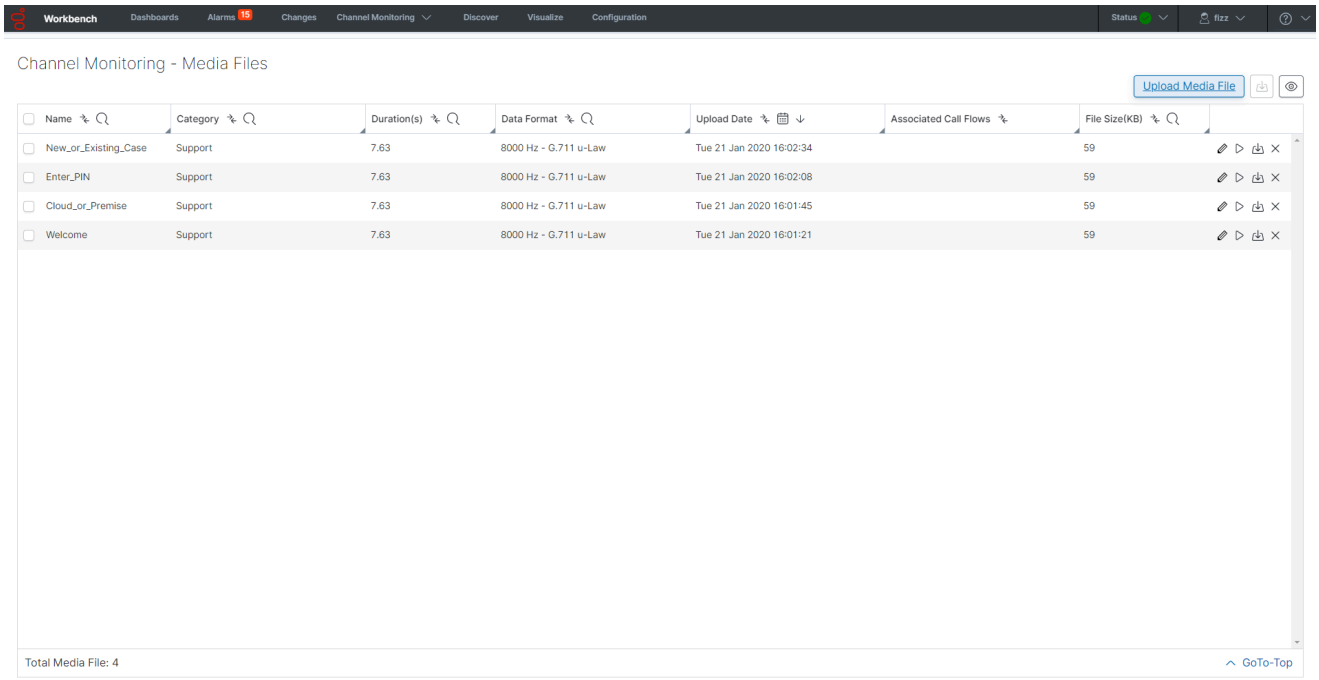
Please use the following steps to upload a new Media File:

1. Select **Channel Monitoring > Media Files** from the Workbench navigation bar.
    1. The *Channel Monitoring - Media Files* page is displayed.
    2. A "Currently there are no Media Files uploaded" message is presented if no Media Files are yet configured
2. Click the **Upload Media File** button
3. The *Upload IVR Media File* dialog is displayed.
4. In the **Category** field, provide a descriptive Category name (i.e. "Support") for the media being uploaded
    1. This category is used to logically group the files; if a Category already exists, it will display in the drop-down list; otherwise a new Category will be created
5. In the Name field, provide a descriptive **Name** (i.e. "Welcome")

6. For the File field, simply **drag and drop** the file on this field **or** click Select to **browse** to the file to be uploaded
    1. **Note**: Uploaded files must be in .wav format.
7. Click the **Save** button.

Example images for context below:





Existing Media

Once you have uploaded Media files, they are listed on the **Channel Monitoring - Media Files** page, as per the image above.

The Media File table provides the following details:

- **ID** - represents an unique *ID* for each Media file; it is an optionally displayed column.
- **Name** - represents the *Name* of the Media file; it is a default displayed column.
- **Category** - represents the *Category* group (i.e. Support, Sales) to which the Media File belongs to; it is a default displayed column.
- **Duration(s)** - represents the time *Duration* (seconds) of the Media file; it is an optionally displayed column.
- **Data Format** - represents the codec (uLaw/aLaw) details of the uploaded .WAV file; it is an optionally displayed column.
- **Upload Date** - represents the date/time which the Media file was uploaded to WB; it is a default displayed column.
- **Associated Call Flows** - represents the Call Flow Names which use this Media file within its Call Stages; it is a default displayed column.
- **File Size (kB)** - represents the size of the Media file in KB's; it is an optionally displayed column.

At the end of each row, there are options for the Media file:

- To **Edit** the Media File, select the **Pencil** button.
- To **Playback/Listen** to the Media File, select the **Play** button.
- To **Download** the Media File locally (for backup), select **Download** button.
- To **Delete** the Media File, select the **Delete** button.

Use the **Show/Hide Columns** button on top of the Media table to view/hide optionally displayed columns.

Warning

- Media Files should/can not be deleted if being used in an existing Call Flow within a **Receive Media** or **Send Media** Stage.
- To delete a Media File that is assigned to Call Flows, first **unassign** the Media File from the Call Flows, then delete the Media File.

CM - Reports

The Channel Monitoring Reports page provides historical insights into the Call Flow tests, their specific behavour and results.

Please use the following steps to use CM Reports:

1. Select **Channel Monitoring > Reports** from the Workbench top navigation bar.
    1. The CM Report page is presented
2. Select a **Call Flow** from the Call Flow Name drop-down list
    1. The CM Report is generated and data is displayed for a time-range of the current day (i.e. "Today")
3. If needed, from the Time Range drop-down, select a different timescale (i.e. "This Week" or "This Month" or "Last 15 Minutes")
    1. If/when the Time Range is changed, click the **Refresh** button to update the data

CM Reports Content

CM Reports contains 4 tabs:

- **Call Metrics**
- **Stage Results**
- **Call Results**
- **Call Details**

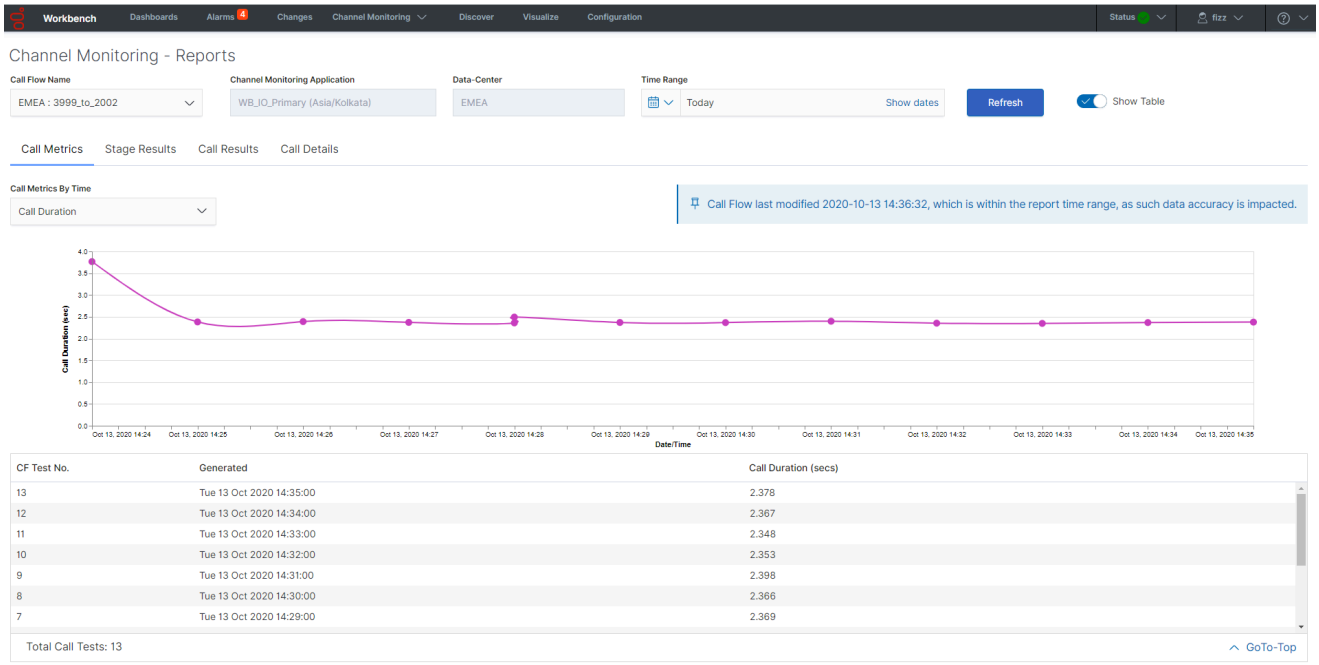
Each in the CM Reports section provides a different view of the available data on the selected Call Flow.

Call Metrics Report

The Call Metrics report uses a graph and table to describe the behavior of a Call Flow in time.

The horizontal axis shows the date/time in which individual calls were executed.

The vertical axis can be modified on the dropdown list to change the metric (Call Duration, Jitter, Time Wait for Agent) used to analyze the call.



The **Jitter** and **Time Wait for Agent** metrics have three thresholds that can be configured in the Alarms section of the Call Flow configuration (see CM - Call Flow Alarms); the threshold for each severity (Critical, Major, Minor) is shown in the graph as a different horizontal line.

The available Call Metric Report *Metrics* are:

Call Duration

The length of the call in seconds. The duration is measured from the moment Channel Monitoring starts the call (i.e., sends the first SIP invite message), until the call is finished because it either encounters an error or ends as expected.

Wait Time for Agent

The amount of time in minutes between the start of the transfer to an agent, and the moment when the agent answers the call.

Jitter

A measure of the quality of the call. In the context of Channel Monitoring, jitter is understood as “the variation of a signal with respect to some clock signal, where the arrival time of the signal is expected to coincide with the arrival of the clock signal.” In this case, the signal refers to the RTP packets downloaded to Channel Monitoring, and the clock signal is the RTP clock rate for the media stream. Jitter is measured in milliseconds.

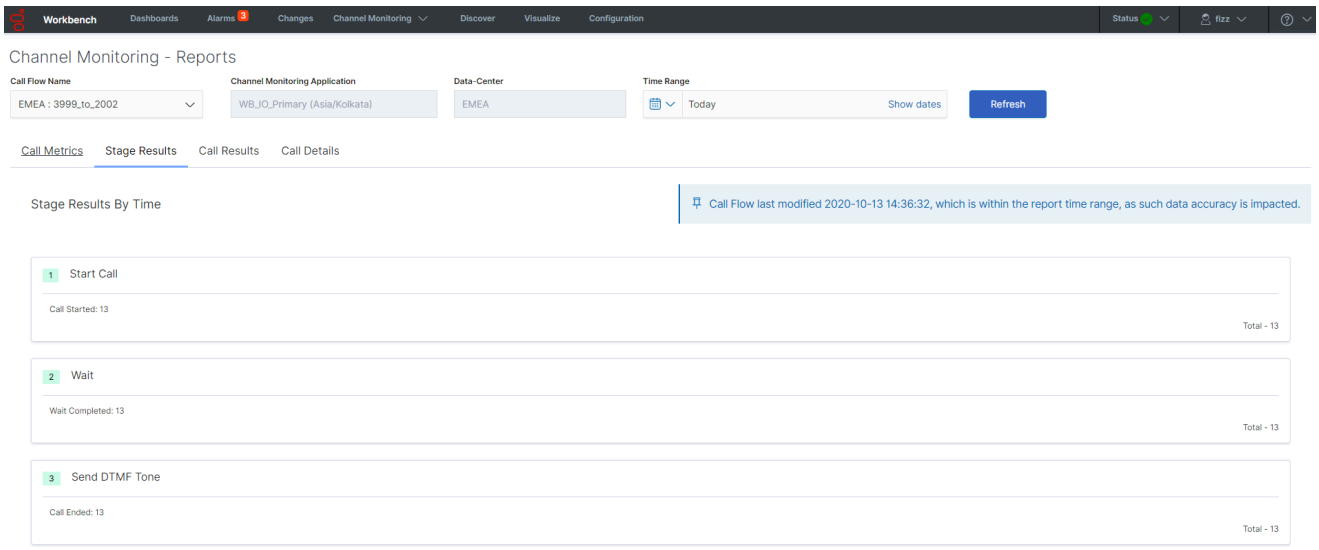
The quoted jitter definition above is from Internet Engineering Task Force (IETF) RFC 3393: IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), page 2, retrieved from https://tools.ietf.org/html/rfc3393.

Stage Results Report

This section shows the different outcomes per Stage of a Call Flow.

The report aggregates all the Stage results across the different calls for the given Call Flow.

For example, if a call fails while sending audio because of an unexpected hang-up, this will increase the count for **Unexpected Hang-Ups** during that specific send media stage.



The available *Stage Results* are:

Success

All stages were executed and their results were as expected.

Pending Result

The call has finished and is being analyzed to determine if it failed at some point of its execution or if it's a success. Even though most results are determined in real-time during the execution of the call, some could be delayed to the end of the call (such as media analysis).

Registrar Connection Failed

The SIP account used by Channel Monitoring to make calls could not connect to SIP Server. This would usually occur during the "Start Call" stage when Channel Monitoring tries to reach SIP Server. Possible causes include problems trying to resolve the domain name or IP address of SIP Server.

Account Authentication Failed

The SIP account used by Channel Monitoring to make calls could not authenticate against SIP Server using the provided credentials. This would usually occur during the “Start Call” stage when Channel Monitoring tries to register the account in SIP Server.

Unexpected Hang-up

The call was being executed and it stopped in an unexpected moment. Calls should end (hang-up) during the “End Call” stage and the “Wait for Agent” stage when the initial call is replaced because of the transfer to the agent. If the call ends at any other stage, it will be considered an unexpected hang-up.

No Answer

Channel Monitoring was not able to reach the target DN and complete the Start Call transaction after a given timeout. This could occur during the “Start Call” stage as Channel Monitoring tries to set up the call with the System Under Test.

Media Analysis Failed

Media received during the call did not match the expected media. A call could have various “Receive Media” stages where audio is received and then analyzed to determine if it matches the expected audio. This comparison produces a percentage error that, when high enough, will produce this error.

No Answer from Agent

A transfer to an agent was expected to occur but no provided DN answered the call before the given timeout. In this case, Channel Monitoring waits for the call to get transferred to one of the DNs provided during the call flow creation. The call might get transferred but it will only be successful if the target of the transfer is contained in the list of DNs set up by the user while configuring the “Wait for Agent” stage.

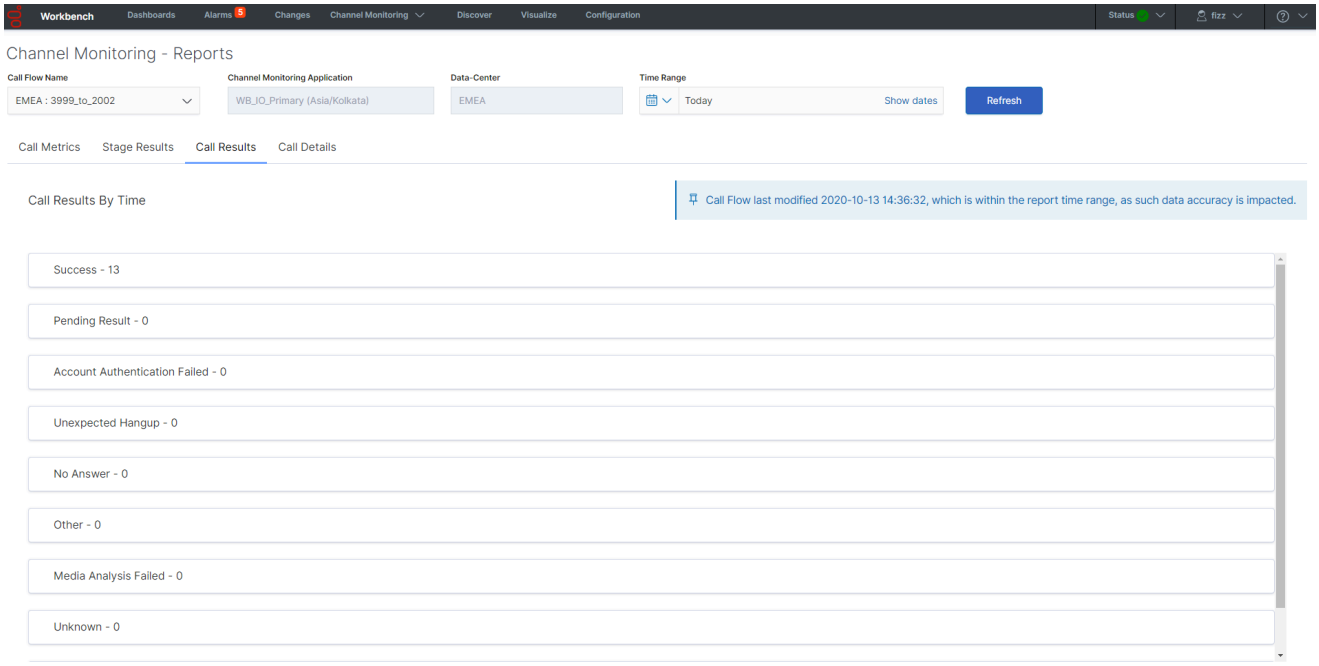
Call Results Report

The Call Results report presents the overall outcome for the calls placed against the Call Flow and the number of times each outcome has occurred.

The possible Call Results are:

- Success
- Pending Result
- Account Authentication Failed
- Unexpected Hangup
- No Answer
- Other

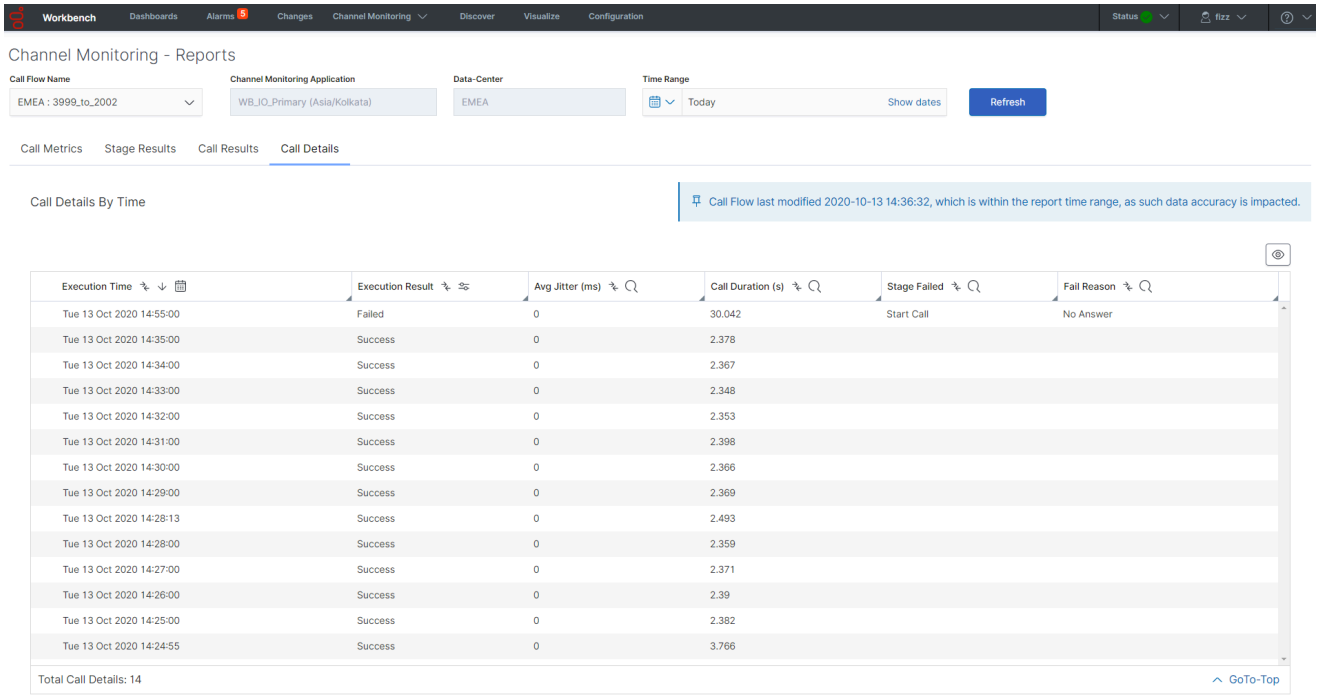
- Media Analysis Failed
- Unknown
- No Answer From Agent



Call Details Report

This report uses a tabular view to present various properties of the test calls. Each row represents the execution of a single call from the repsecitve Call Flow.

The possible execution results for a call are “Success” and “Fail”; if the call *Failed*, the table will show the Stage in which it failed and the reason for the error.

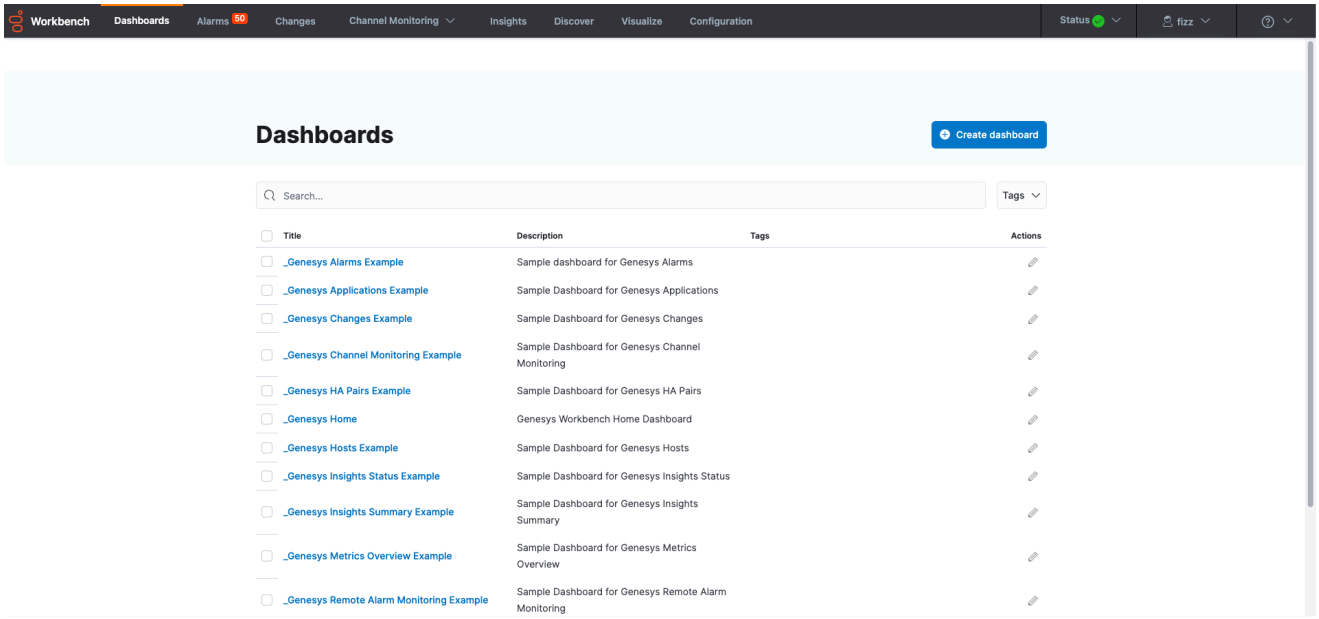

Workbench
Dashboards
Alarms 5
Changes
Channel Monitoring
Discover
Visualize
Configuration
Status
fizz
Channel Monitoring - Reports
Call Flow Name
EMEA : 3999_to_2002
Channel Monitoring Application
WB_IO_Primary (Asia/Kolkata)
Data-Center
EMEA
Time Range
Today
Show dates
Refresh
Call Metrics
Stage Results
Call Results
Call Details
Call Details By Time
Call Flow last modified 2020-10-13 14:36:32, which is within the report time range, as such data accuracy is impacted.
Execution Time
Execution Result
Avg Jitter (ms)
Call Duration (s)
Stage Failed
Fail Reason
Tue 13 Oct 2020 14:55:00 Failed 0 30.042 Start Call No Answer
Tue 13 Oct 2020 14:35:00 Success 0 2.378
Tue 13 Oct 2020 14:34:00 Success 0 2.367
Tue 13 Oct 2020 14:33:00 Success 0 2.348
Tue 13 Oct 2020 14:32:00 Success 0 2.353
Tue 13 Oct 2020 14:31:00 Success 0 2.398
Tue 13 Oct 2020 14:30:00 Success 0 2.366
Tue 13 Oct 2020 14:29:00 Success 0 2.369
Tue 13 Oct 2020 14:28:13 Success 0 2.493
Tue 13 Oct 2020 14:28:00 Success 0 2.359
Tue 13 Oct 2020 14:27:00 Success 0 2.371
Tue 13 Oct 2020 14:26:00 Success 0 2.39
Tue 13 Oct 2020 14:25:00 Success 0 2.382
Tue 13 Oct 2020 14:24:55 Success 0 3.766
Total Call Details: 14
GoTo-Top

Workbench Dashboards

Workbench Dashboards are a placeholder for a collection of "Visualizations" that display health, status and event data.

Workbench Dashboards provide at-a-glance insights into data that has been ingested from your Genesys Engage platform as well as Workbench related data/events.

To view and use Workbench Dashboards, click **Dashboards** on the Workbench top navigation bar; post installation Dashboards (13) contain shipped examples to view and use, detailed below:



Dashboard Functionality

With Workbench Dashboards you can:

- Create new Dashboards
- Search for Dashboards
- Share Dashboards
- Clone/Copy Dashboards
- Edit/Customize Dashboards
- Full-Screen Dashboards

- Arrange Visualizations within the Dashboards.
- Gain monitoring and troubleshooting insights from the shipped Dashboards and newly created Dashboards.
- Use and learn from shipped example Dashboards.
- View the shipped Visualizations within the shipped Dashboards.

Genesys Home Dashboard

Workbench ships with a "_Genesys Home" Dashboard concept.

In Workbench 9.3 the default home dashboard is the "_Genesys Metrics Overview Example" which provides details of:

- Number of Hosts
- Top Hosts by CPU
- Top Hosts by Memory
- Host(s) Uptime
- Host(s) CPU Usage
- Host(s) Memory Usage
- Host(s) # of Processes
- Host(s) Disk Usage
- Top Processes by CPU
- Top Processes by Memory
- Host(s) CPU and Memory Usage
- Top Host(s) Processes by CPU vs Time
- Host(s) Network Traffic Bytes

Important

- The "_Genesys Metrics Overview Example" will display Hosts that are ingestion Metric data into the Workbench solution; including the Workbench Hosts
- Workbench Agent Remote (WAR) components need to be installed on remote hosts such as sip, urs, gvp etc for Workbench to show their respective data

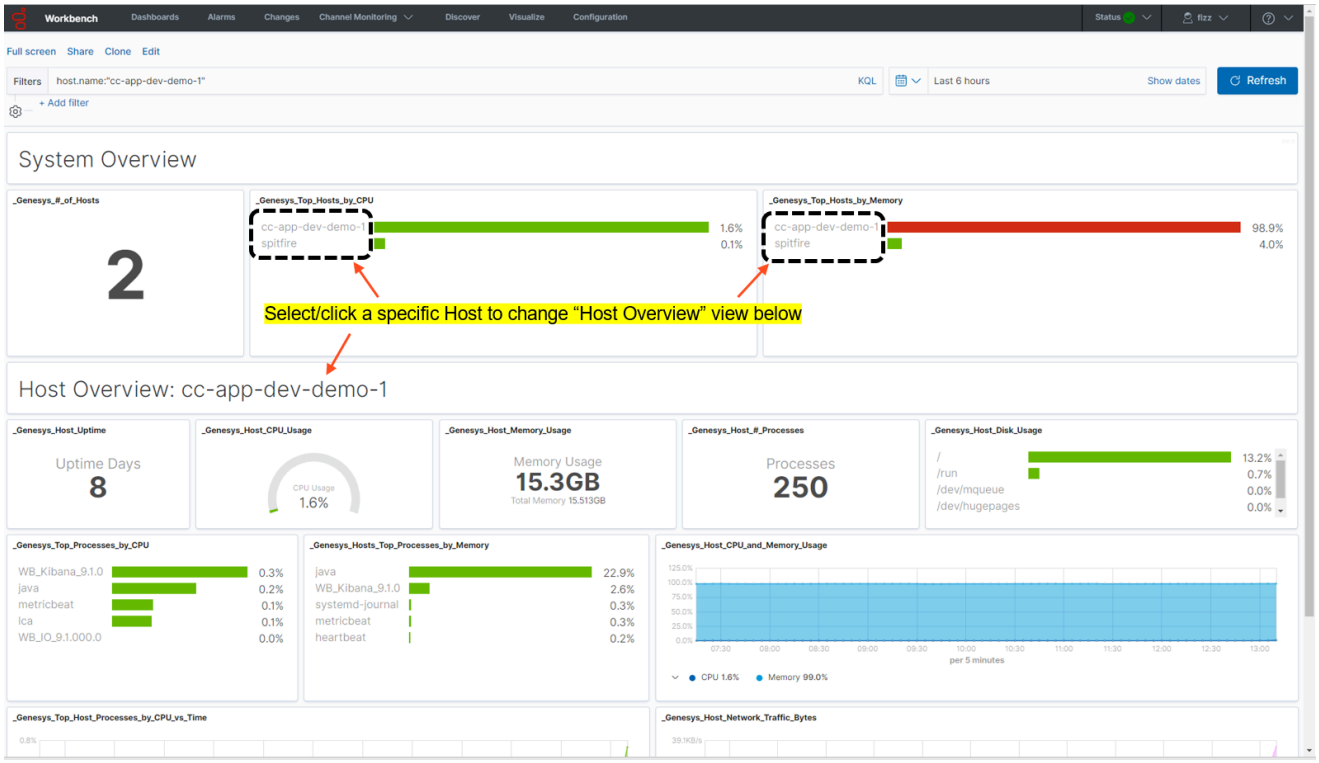
Dashboard Examples

Workbench ships with the following example Dashboard templates:

- _Genesys Alarms Example
- _Genesys Applications Example
  - Note: Workbench only monitors *Server* Type applications and not *Client* applications; therefore the Total/Up/Down/Unknown *counts* may be different from GAX and GA
- _Genesys Changes Example
- _Genesys Channel Monitoring Example
- _Genesys HA Pairs Example
- _Genesys Home
- _Genesys Hosts Example
- _Genesys Insights Status Example
- _Genesys Insights Summary Example
- _Genesys Metrics Overview Example
- _Genesys Remote Alarm Monitoring Example
- _Genesys Solutions Example
- _Genesys Workbench Summary Example

Metrics Overview Example Dashboard

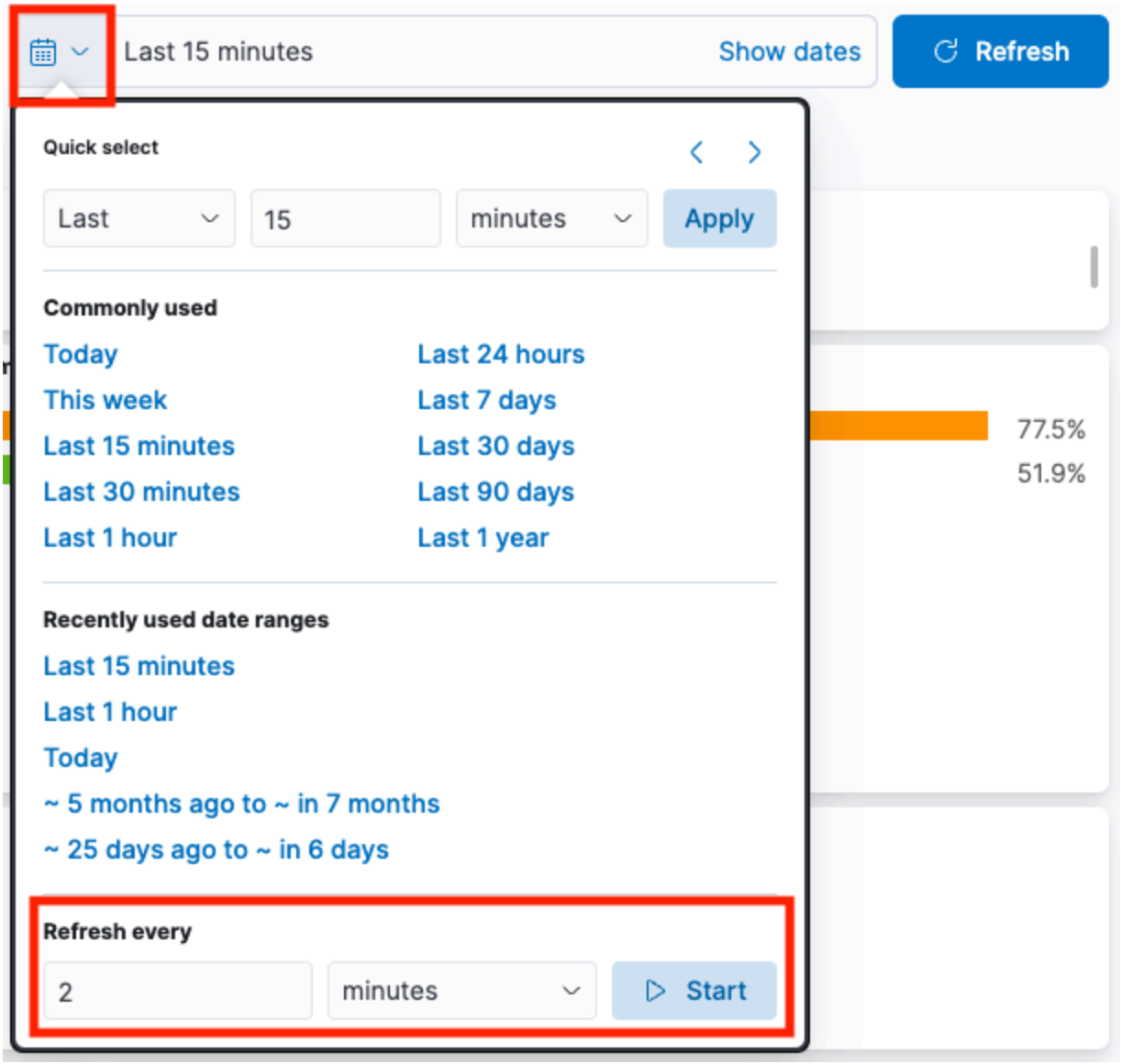
Workbench 9.1 adds a Metric data ingestion feature that enables observability of host and process CPU, Memory, Disk and Network metric data, providing rich insights and analysis capability into host and process metric utilization, performance and trends.



Considerations

Important

- From WB 9.3+ the Dashboards/Visualizations do not update by default in real-time
- Use the 'Quick Select' feature below to 'Start' auto Refresh functionality of Dashboards/ Visualizations



Important

- For Workbench 9.2 to 9.3 upgrades, existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
- The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
- As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/ message will be displayed
- Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

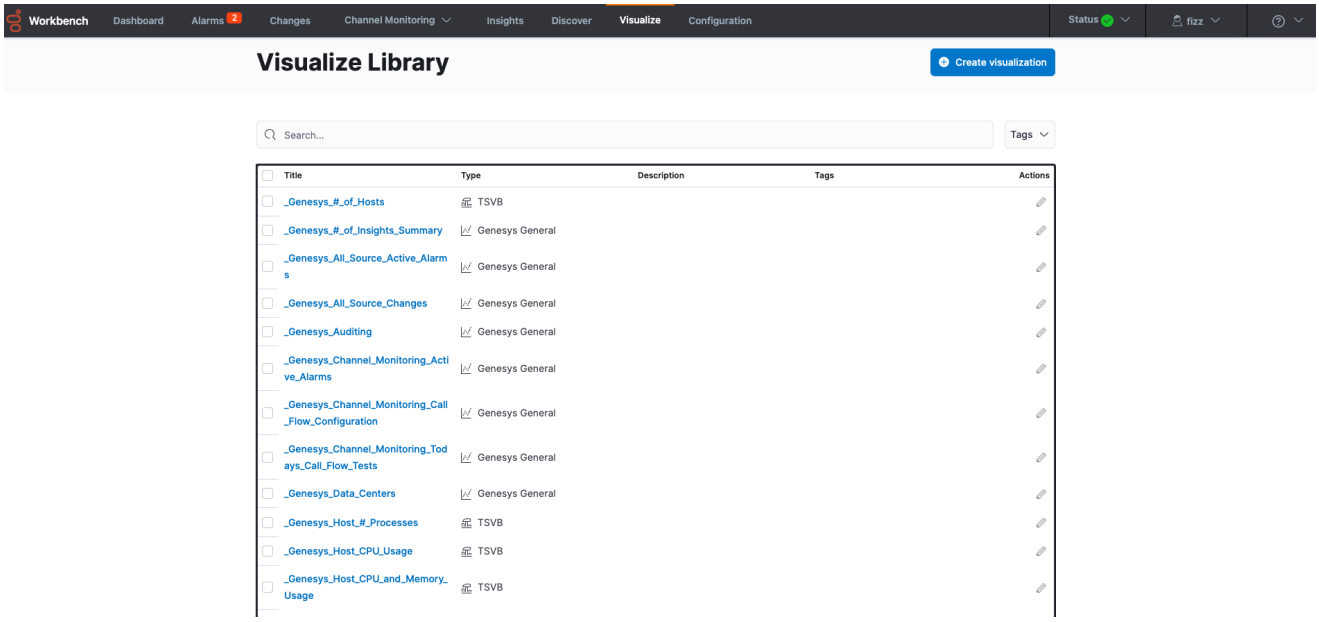
Important

- Workbench Dashboards and Visualizations leverage the Elastic Kibana component, please review the Kibana documentation (https://www.elastic.co/kibana) for further comprehensive guidance on Dashboards and Visualizations.

Workbench Visualizations

Workbench Visualizations is an analysis and visualization component that enables the user to create real-time and historic visualizations of Workbench ingested data; the Workbench Visualizations are then used to build Workbench Dashboards to present the data to the user.

To view and use Workbench Visualizations, click **Visualize** on the Workbench top navigation bar; post installation Visualize contains 40+ shipped examples to view and utilise.



Visualizations Functionality

With Workbench Visualizations you can:

- Create new Visualizations from the shipped Genesys General and Genesys Health-Maps Visualization Types
- Create new Visualizations from the standard Kibana Visualization Types
- Search for Visualizations
- Save Visualizations
- Share Dashboards
- Clone/Copy Visualizations
- Edit/Customize Visualizations

- Arrange Visualizations within the Dashboards.
- Gain monitoring and troubleshooting insights from the shipped Visualizations and newly created Visualizations.
- Use and learn from shipped example Visualizations.
- View the shipped Visualizations within the shipped Dashboards.

Genesys Visualizations Types

Workbench ships with the following example Workbench Visualizations that are created from the **Genesys General** Visualization Type:

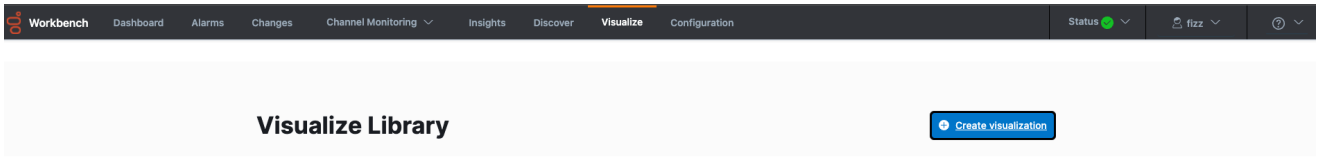
Genesys General

- Alarms
  - All Source Active Alarms
  - Workbench Active Alarms
  - Genesys Engage Active Alarms
- Changes
  - All Source Changes
  - Workbench Changes
  - Genesys Engage Changes
- Channel Monitoring
  - Active Alarms
  - Call Flow Configuration
  - Today's Call Flow Tests Summary
- Remote Alarm Monitoring
  - Alarms Sent to RAM Service
- System Status & Health
  - Workbench Status Summary
  - Workbench Agents
  - Channel Monitoring
  - Remote Alarm Monitoring
  - Genesys Engage Integration
  - Data-Centers
  - Auditing

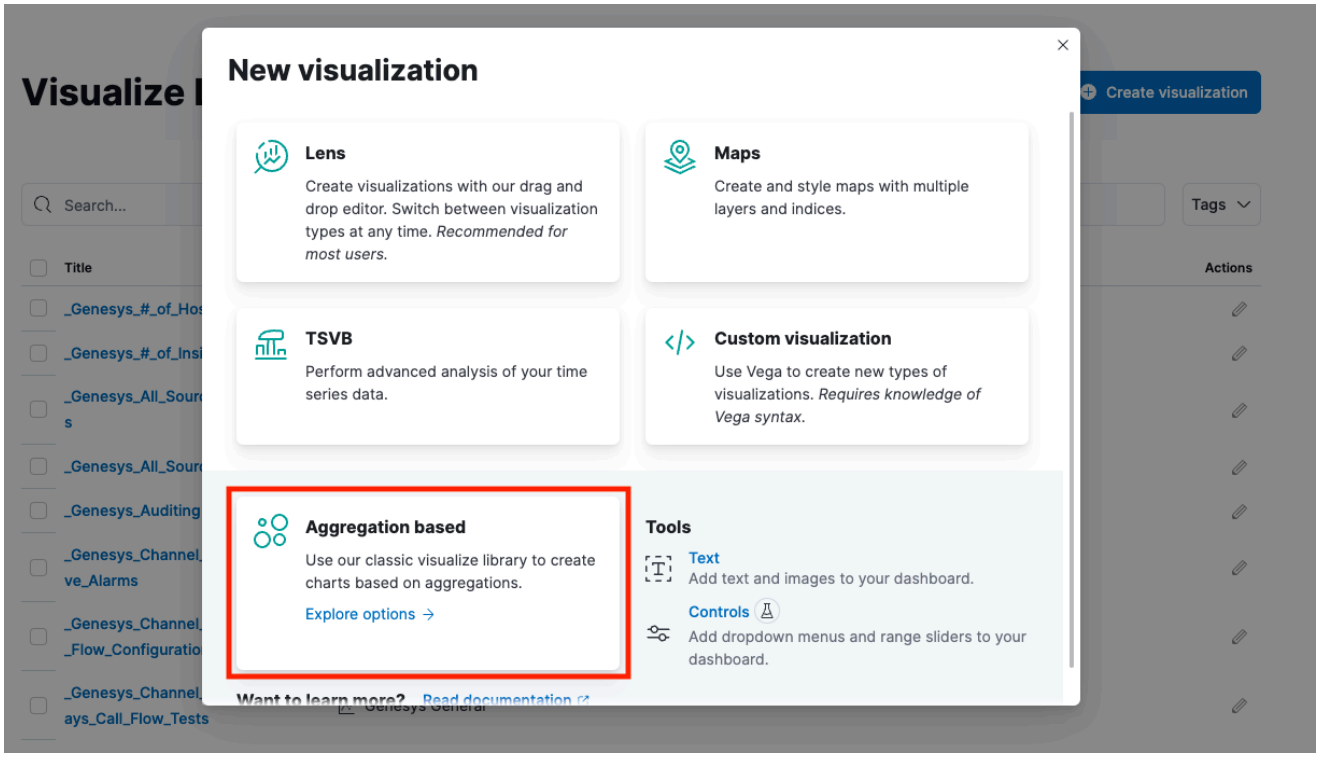
    - General
    - Insights (Anomaly Detection)
- Workbench Summary
    - Workbench Applications
    - Workbench Hosts
- Genesys Engage Summary
    - Genesys Engage Applications
    - Genesys Engage Hosts
    - Genesys Engage Solutions
    - Genesys Engage HA Pairs

To use the Genesys General Visualization Types:

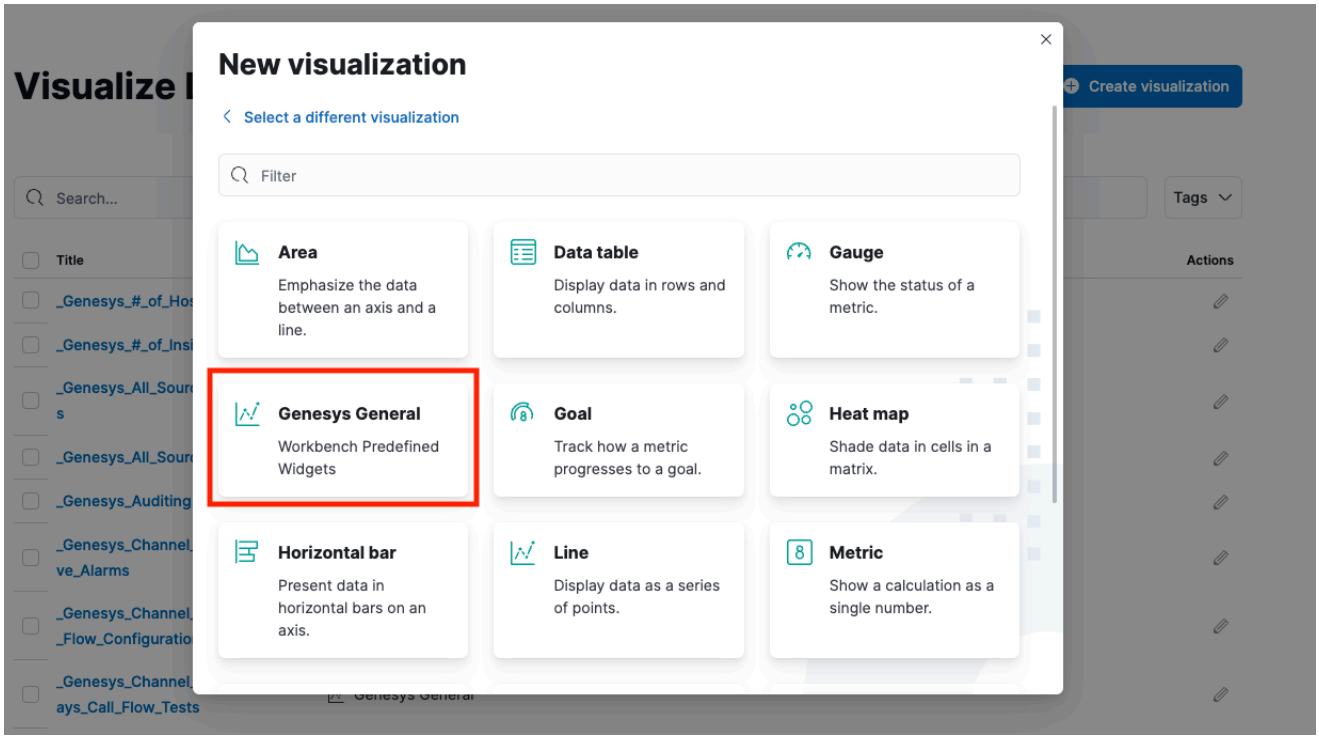
- Via the top menu bar, navigate to Visualize
- Click the Create visualization button



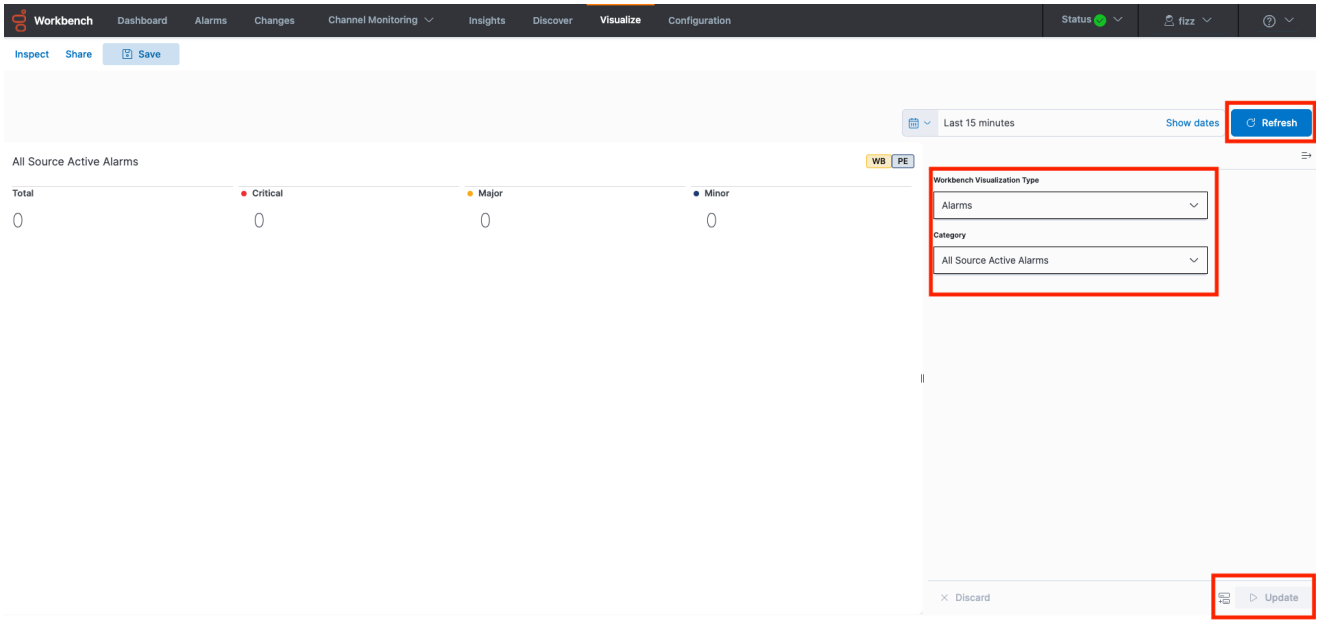
- Click the Aggregation based option



- Click the Genesys General option



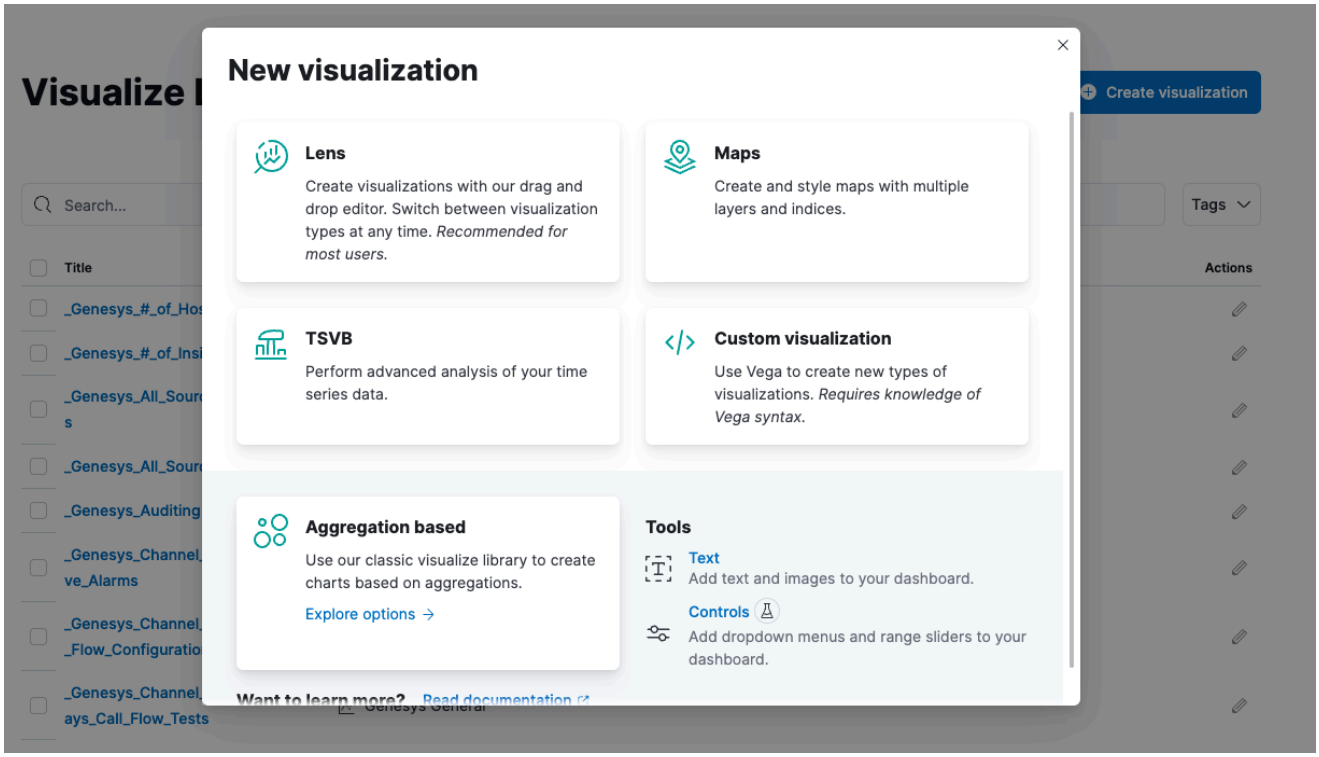
- Use the highlighted options below to select Type, Category, then Update/Refresh to view and refresh the data accordingly



- Click **Save** to store the Visualization and use in Dashboards

Kibana Visualizations Types

In addition to the shipped Genesys Visualization Types, the user can also leverage the standard Kibana Visualization Types:



Health-Map's

Health-Map's provide a quick and easy status view of:

- Genesys Engage Applications
- Genesys Engage Hosts
- Genesys Engage Solutions

> **Important**
>
> - Workbench 9.0 to 9.2, Health-Maps can only be created for Genesys Engage Hosts, Applications and Solutions; Workbench Health-Maps cannot be created
> - Workbench 9.3 does NOT currently support Health-Maps

Please review the below for an example of:

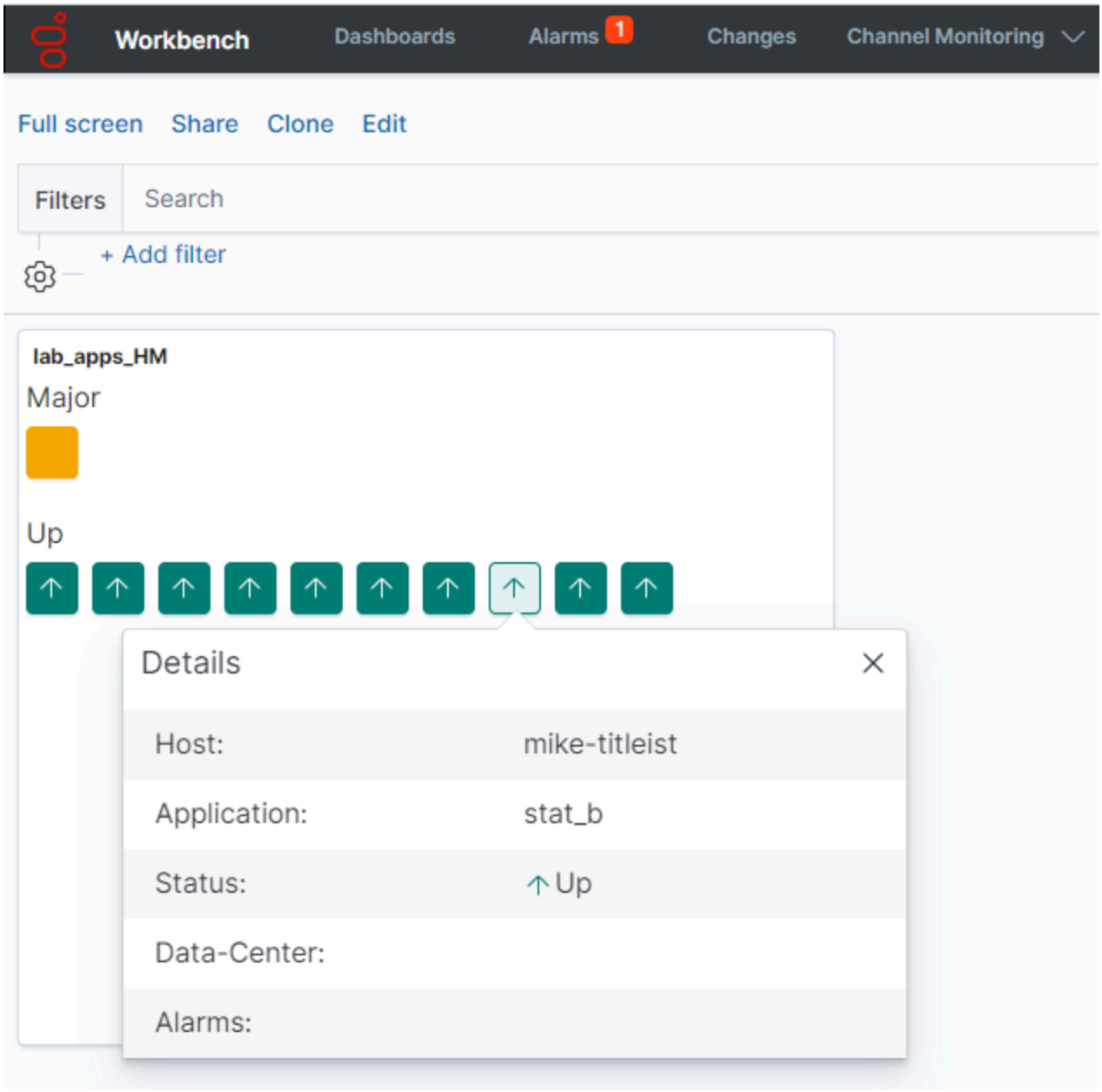
- Creating a new Health-Map for Genesys Engage Chat Applications

- Creating a new Dashboard
- Adding the newly created Health-Map to the new Dashboard
- Saving the Dashboard

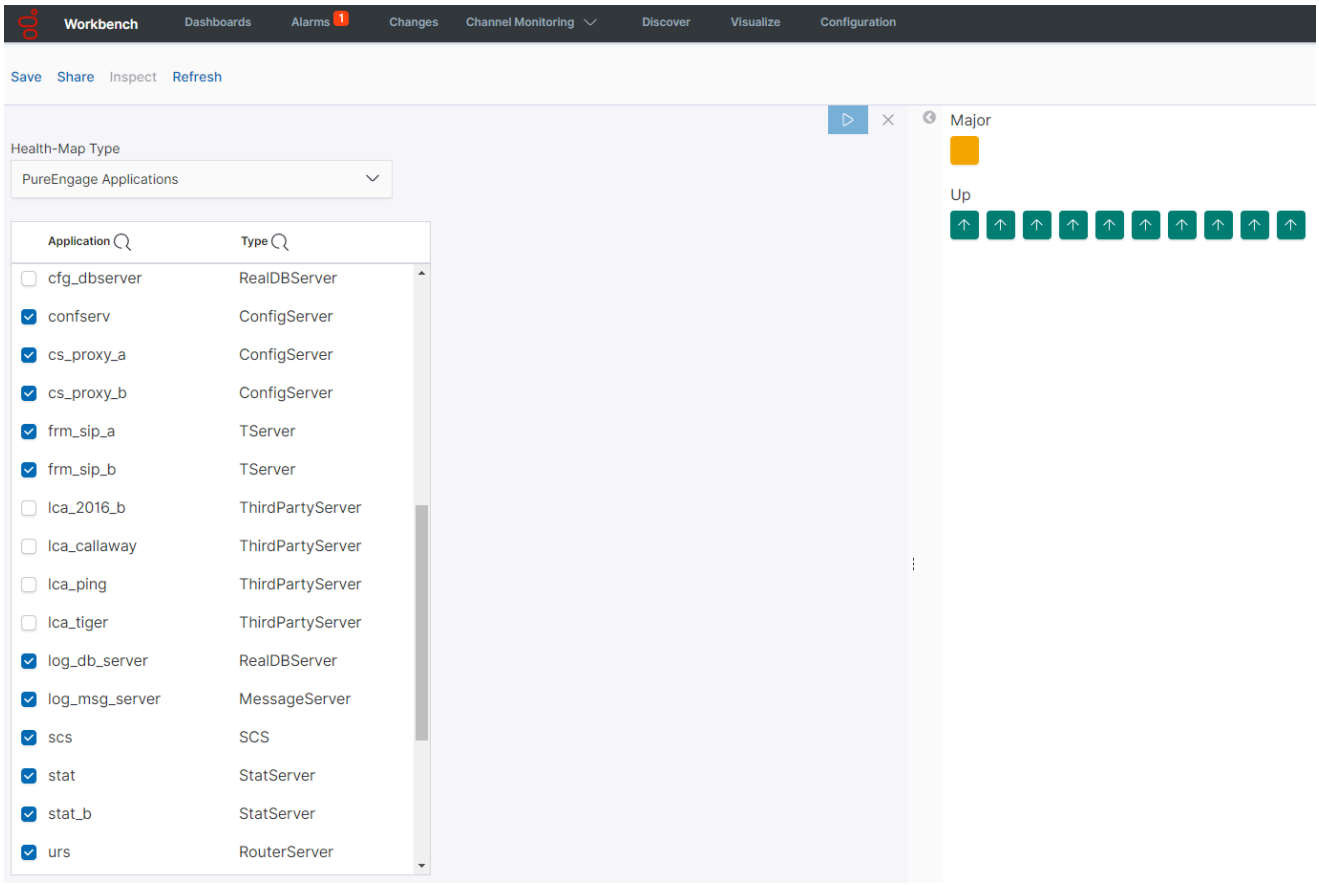
1. Navigate to **Visualize** from the top Workbench navigation bar
2. Click the **+** button
3. Select **Genesys Health-Maps**
4. Ensure **Genesys Engage Applications** is selected for the Health-Map Type
5. Check the relevant Genesys Engage Chat Applications you want displayed in the Health-Map
    1. review example below
6. Click the **Apply Changes** button
7. Click **Save**
8. Provide a Visualization name i.e. *lab_apps_HM*
9. Click **Confirm Save**
10. Click **Dashboards**
11. Click **Create new dashboard**
    1. Presented with "This dashboard is empty. Let's fill it up!" message
12. Click **Add** to add a Visualization to this Dashboard
13. Find and click the *HM_Chat_Applications* Visualization
14. Click the **X** to close the Add Panels dialog
15. The *HM_Chat_Applications* Visualization has now been added to the Dashboard
16. Click **Save**
17. Provide a *lab_apps_db* and click **Confirm Save**

The example **Lab Application** Health-Map Dashboard is displayed.

Clicking on a Health-Map object will provide additional status context; click **X** or press **ESC** to close the pop-up



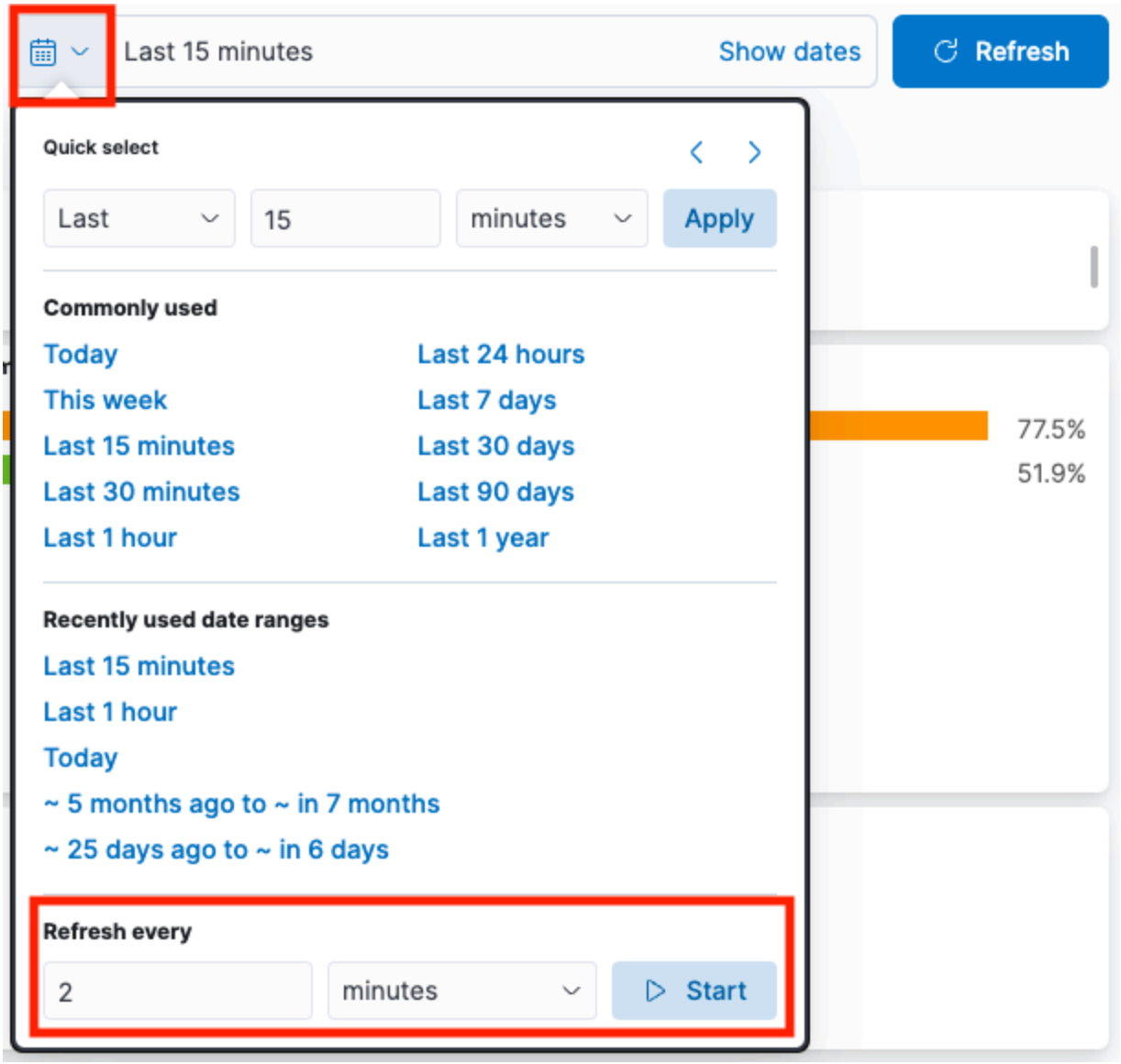
An example image showing the selection of *Lab Applications* to include in the new Health-Map:



Considerations

Important

- From WB 9.3+ the Dashboards/Visualizations do NOT update by default in real-time
- Use the 'Quick Select' feature below to 'Start' auto Refresh functionality of Dashboards/ Visualizations



Important

- For Workbench 9.2 to 9.3 upgrades, existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
- The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
- As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/ message will be displayed
- Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

Important

- Workbench Dashboards and Visualizations leverage the Elastic Kibana component, please review the Kibana documentation (https://www.elastic.co/kibana) for further comprehensive guidance on Dashboards and Visualizations.

Workbench Discover Console

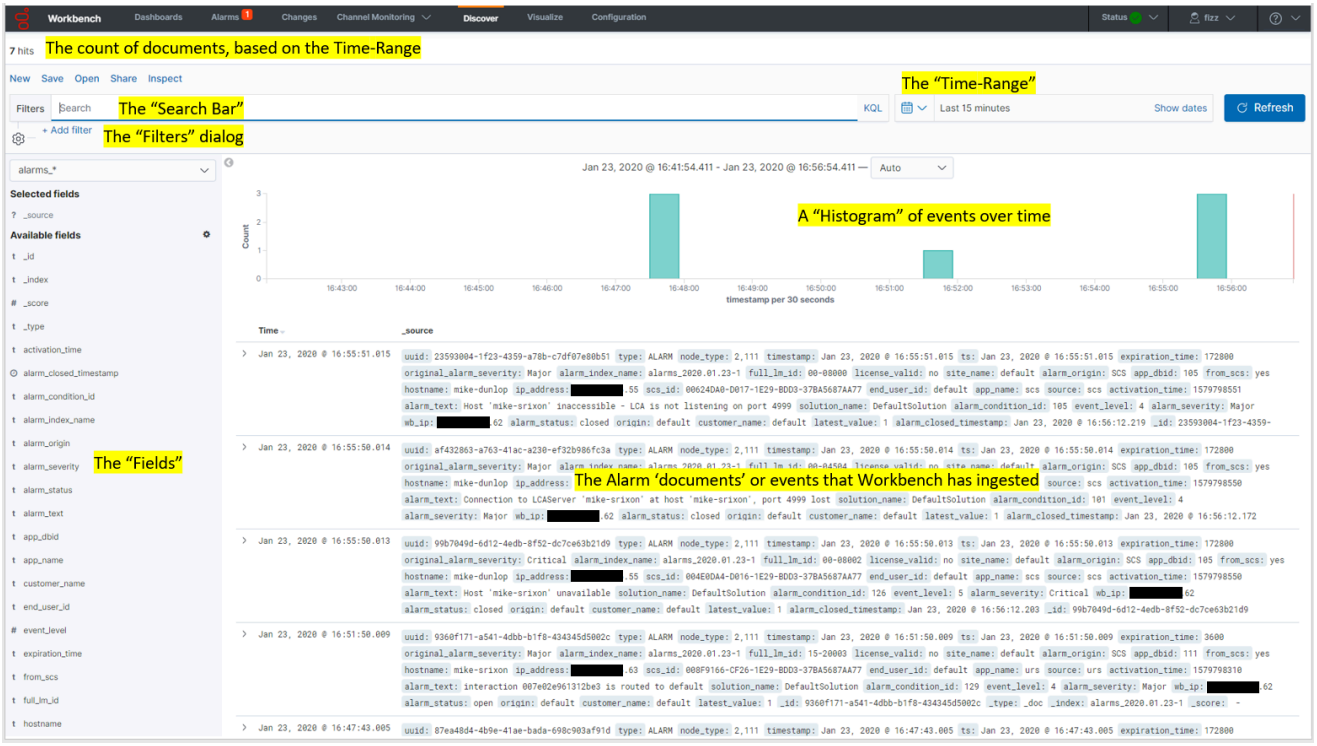
The Workbench Discover Console allows the user to explore and visualize the raw data events ingested into Workbench.

Use the Discover Console to:

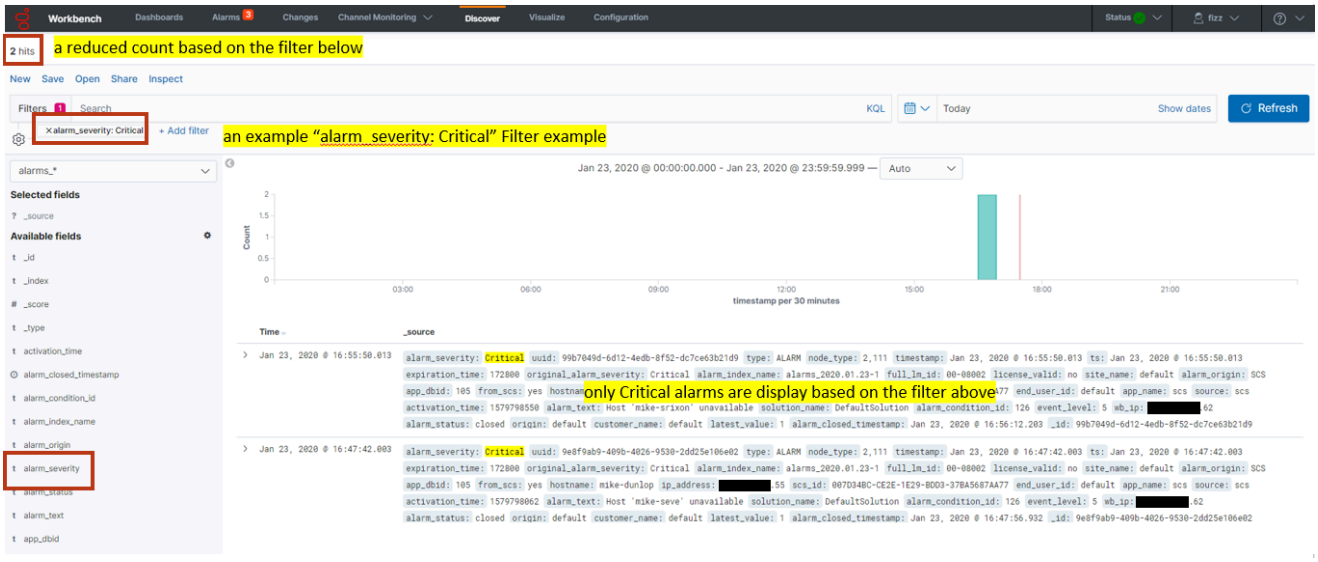
- View and analyze raw ingested document data for a given time range
- Submit searches via the "Search bar"
- Add Filters based on the fields in the document
- View the count of ingested documents over time via the top histogram

Discover Console Examples

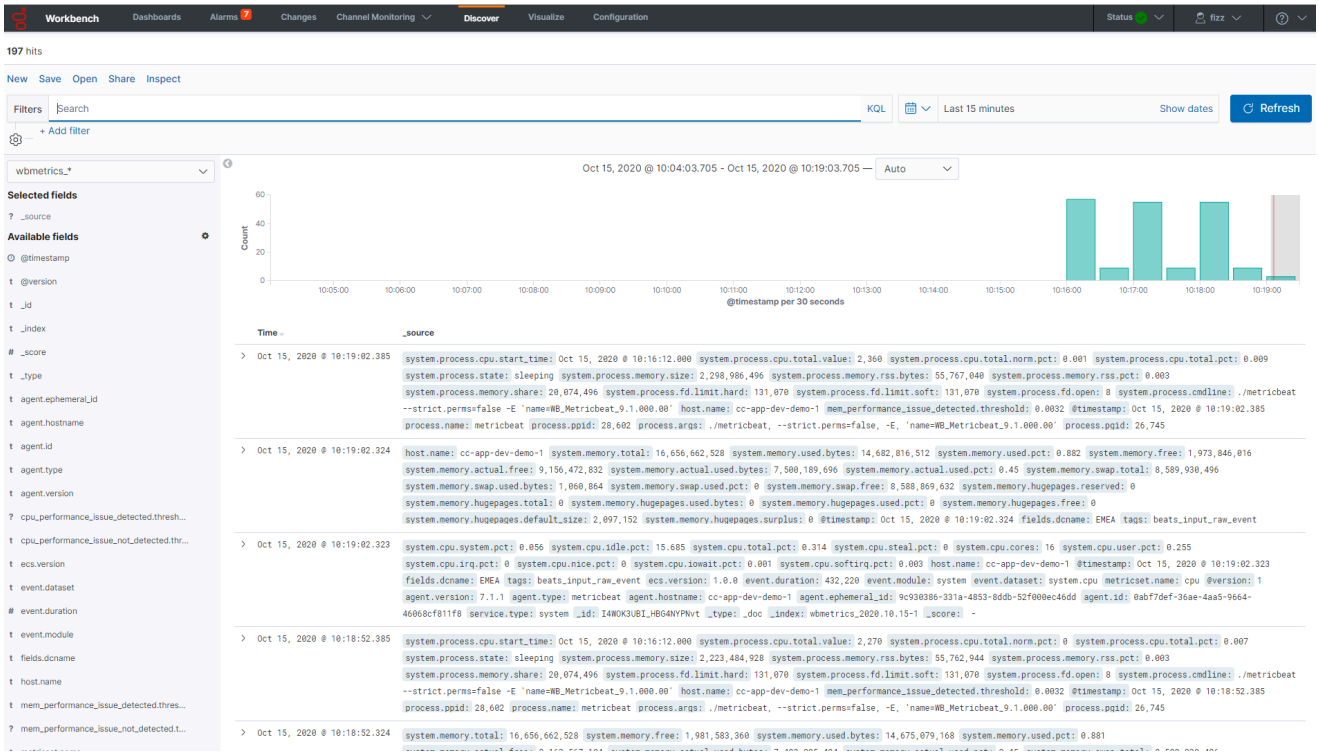
An example Discover output:



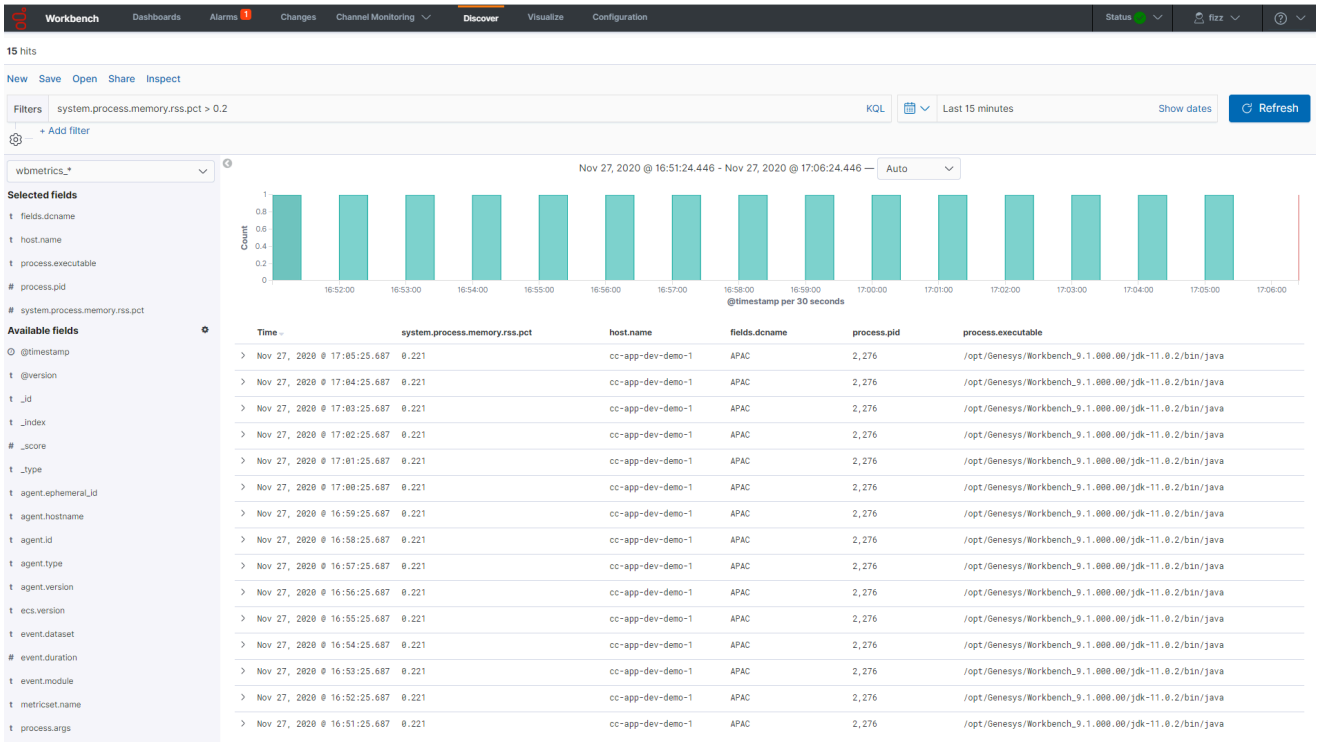
An example Discover output with an **alarm_severity: Critical** filter applied:



An example Discover output with the "wbmetric_*" ingested data:



An example Discover output with a "system.process.memory.rss.pct > 0.2" filter and specific fields selected:


Workbench
Dashboards
Alarms
Changes
Channel Monitoring
Discover
Visualize
Configuration
Status
fizz
15 hits
New Save Open Share Inspect
Filters
system.process.memory.rss.pct > 0.2
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
wbmetrics_*
Selected fields
t fields.dcname
t host.name
t process.executable
process.pid
system.process.memory.rss.pct
Available fields
@timestamp
t @version
t _id
t _index
_score
t _type
t agent.ephemeral_id
t agent.hostname
t agent.id
t agent.type
t agent.version
t ecs.version
t event.dataset
event.duration
t event.module
t metricset.name
t process.args
Nov 27, 2020 @ 16:51:24.446 - Nov 27, 2020 @ 17:06:24.446 —
Auto
Count
@timestamp per 30 seconds
Time
system.process.memory.rss.pct
host.name
fields.dcname
process.pid
process.executable
Nov 27, 2020 @ 17:05:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 17:04:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 17:03:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 17:02:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 17:01:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 17:00:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:59:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:58:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:57:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:56:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:55:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:54:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:53:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:52:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java
Nov 27, 2020 @ 16:51:25.687 0.221 cc-app-dev-demo-1 APAC 2,276 /opt/Genesys/Workbench_9.1.000.00/jdk-11.0.2/bin/java

Notification Channels

Workbench Notification Channels enable integration from Workbench to other external systems.

Currently Workbench supports Notification Channels of type **Webhook**.

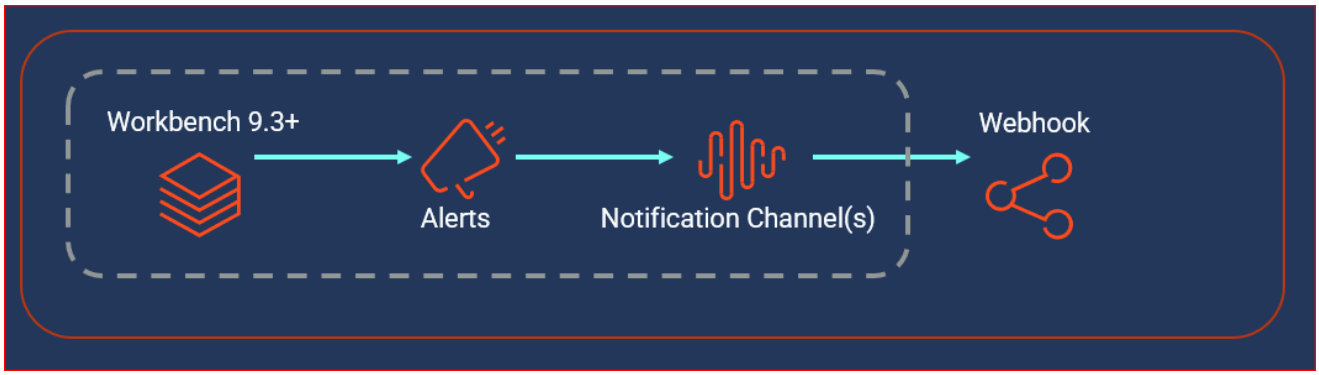
The **Webhook** Notification Channel type is a standard in the monitoring/observability/tracing vendor space, it is a simple and efficient method to send information (currently that information is limited to Active Alarms within Workbench; either Engage [i.e. Host Unavailable] Alarms received from Engage SCS and/or Workbench [i.e. Channel Monitoring - Call Flow - No Answer] generated) from Workbench, to a customer developed, or external, HTTP[S] endpoint.

Once the Workbench Alert payload is received from the Workbench Notification Channel, by the customer developed HTTP[S] Webhook endpoint, the customer has the flexibility to transition further, for example, send the Workbench Alert payload/event to Slack, Teams or a Case Management System for empowered observability.

With the Workbench **Webhook** Notification Channel feature you can:

- Create a Notification Channel of type **Webhook** by configuring HTTP request properties that define the internal/external HTTP[S] service that is going to expose the HTTP endpoint.
  - if required, secure HTTPS connections can be specified and different authentication mechanisms can be used (username/password, API Key, TLS)
- Keep a list of existing Notification Channels that allows to edit/delete any of the existing Notification Channels
- Test a Notification Channel to guarantee that the configuration created in Workbench correctly represents the external HTTP endpoint
  - these tests can be performed during creation/edition as well as from the list of Notification Channels.

The diagram below shows the internal context of Workbench Notification Channels and how Workbench Alerts use those Notification Channels to send events to external systems and/or services:



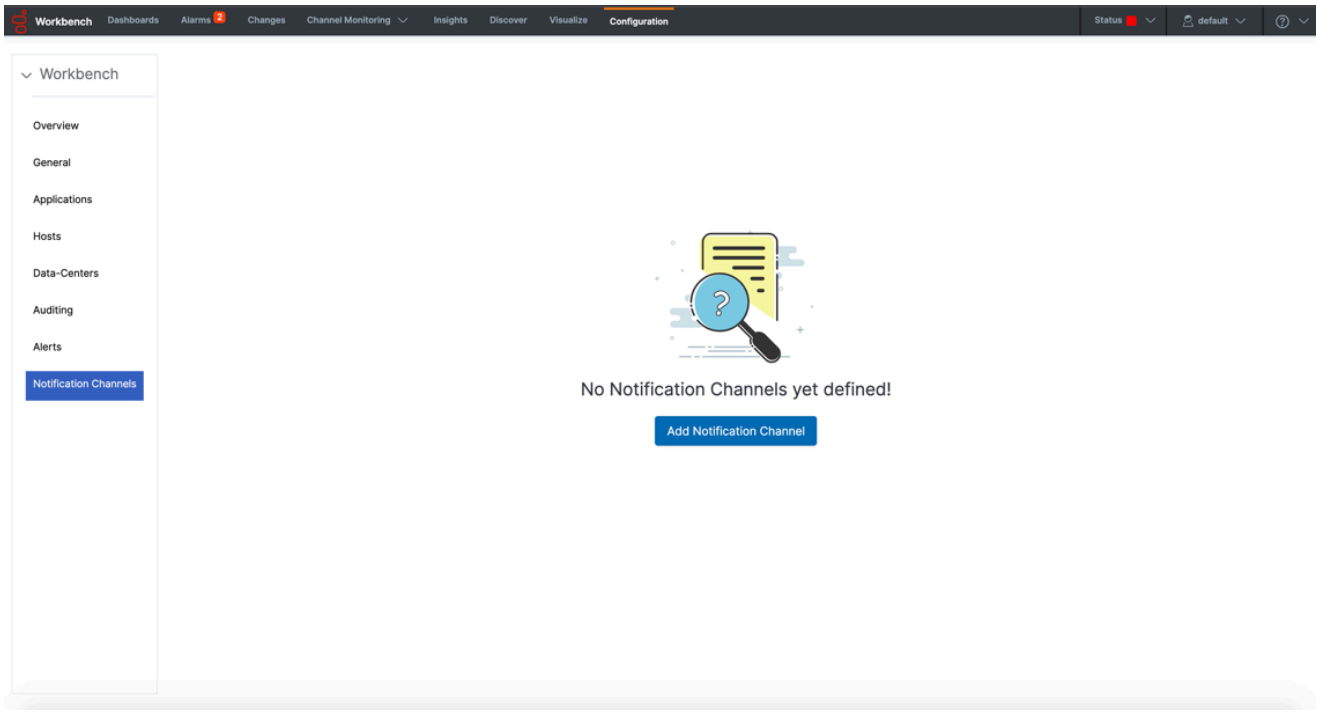
The following sections describe the steps to "Create, Edit, "Delete" and "Test" **Webhook** Notification Channels.

Create/Edit a Notification Channel

To create a Notification Channel for the first time:

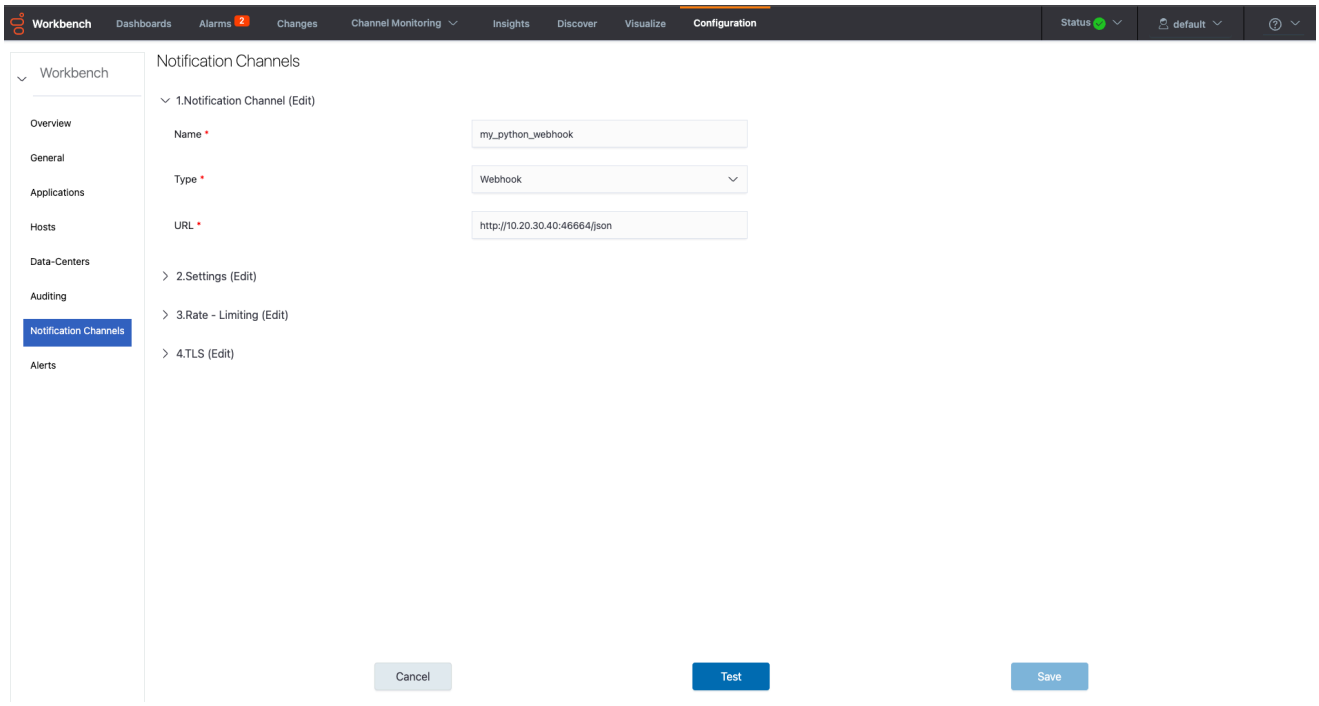
- Navigate to the Workbench ‘Configuration Console’ on the top menu
- Click ‘Notification Channels’ sub-menu

The following page will be displayed:



- Click the ‘Add Notification Channel’ button
- Review and complete the following Notification Channel configuration sections based on your requirements

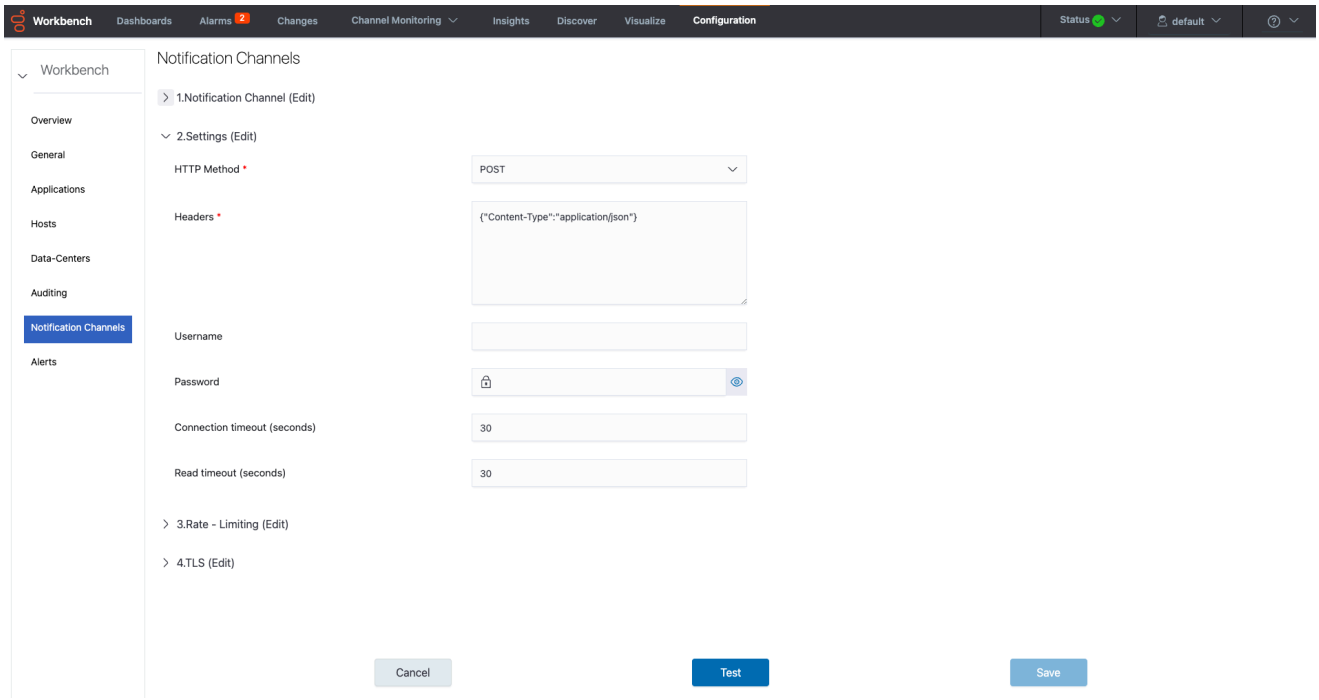
1. Notification Channels



Details of the above fields being:

- **Name** (Required - i.e. *my_python_webhook*)
  - A unique name used to identify the Notification Channel
  - the name must be unique - max 25 characters - should only include alphanumeric characters, dot, hyphen, and/or underscore
- **Type** (Required - i.e. *Webhook*)
  - Currently the only Workbench Notification Channel Type available is **Webhook**
- **URL** (Required - i.e. *http://<HOSTNAME_OR_IP>:<PORT>/workbench_alerts*)
  - The URL of the customers developed HTTP[S] endpoint to which Workbench will send the Alarm payload to

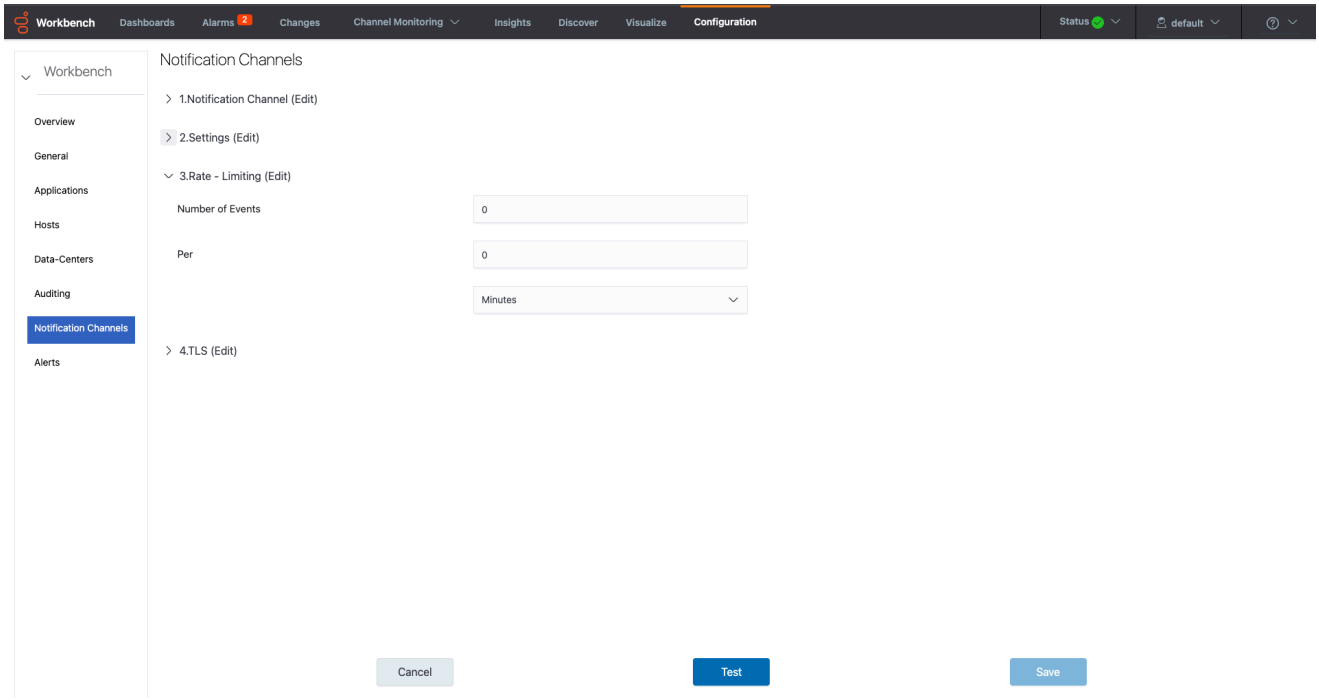
2. Settings



Details of the above fields being:

- **HTTP Method** (Required):
  - The HTTP Method that should be used when invoking the HTTP Endpoint; possible values are POST (default) and PUT
- **Headers** (Required)
  - Any additional HTTP headers required to be sent with the request
- **Username** (Optional)
  - If the Endpoint has username/password authentication this field is required
- **Password** (Optional)
  - If the Endpoint has username/password authentication this field is required
- **Connection timeout** (Optional)
  - Expiration time for an attempt to create a HTTP[S] connection; specified in seconds
- **Read timeout** (Optional)
  - Timeout for reading the HTTP[S] response after the connection was established; specified in seconds

3. Rate - Limiting (optional)



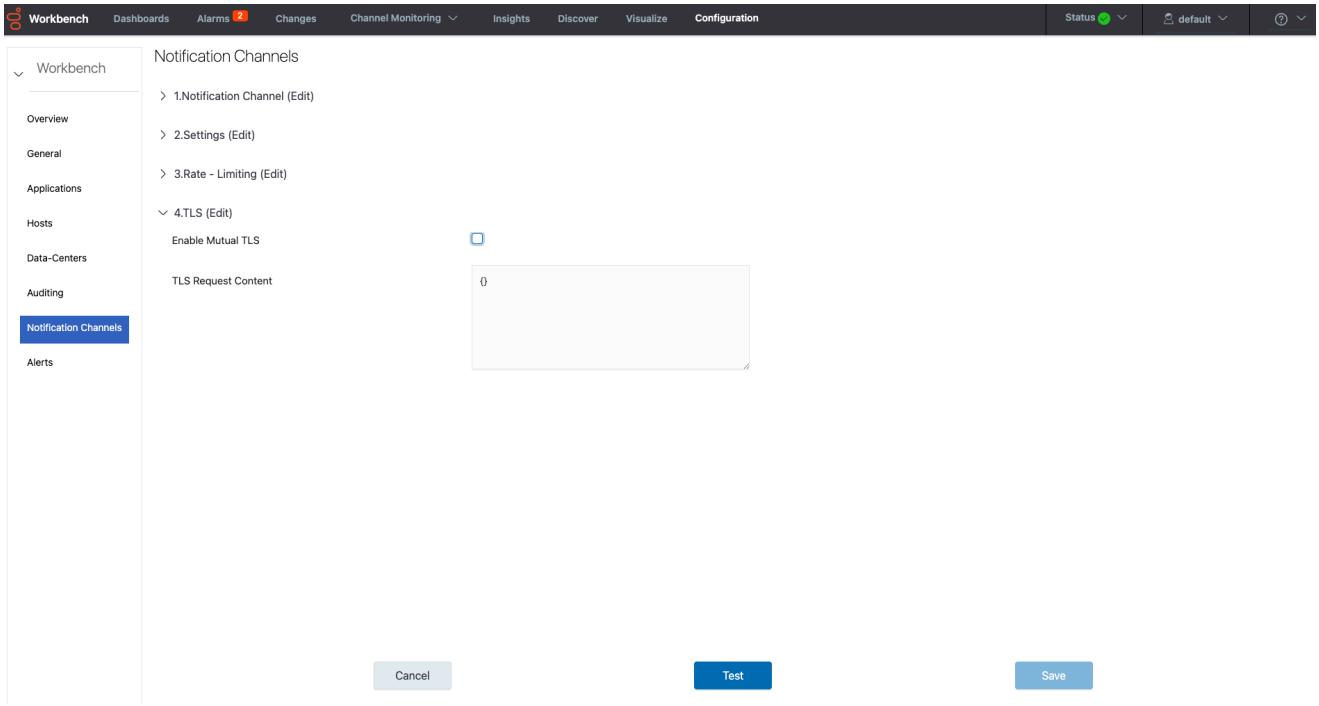
Details of the above fields being:

- **Number of Events** (Optional)
  - The maximum number of Alarm events to be sent to the HTTP endpoint
  - Used in conjunction with "Per" settings below
  - The default value of "0" means there is no limit - ALL Alarms will be sent to the HTTP endpoint with no rate-limiting
  - If/when set to a non-zero value then "Limit - Frequency" must also be set to a non-zero value - else setting will be ignored
- **Per** (Optional)
  - The time interval between HTTP requests
  - Used in conjunction with "Number of Events" above
  - The default value of "0" means there is no limit - ALL Alarms will be sent to the HTTP endpoint with no rate-limiting
  - If/when set to a non-zero value then "Number of Events" above must also be set to a non-zero value - else setting will be ignored
  - Select either "Seconds" or "Minutes"

> **Important**
>
> - To apply/enable rate-limiting, both "Number of Events" and "Per" settingsneed to be assigned non-zero values; else rate-limiting will be ignored/disabled

4. TLS (optional)

This is an optional section that allows TLS Authentication to be configure based on the customers developed or external HTTP Endpoint.



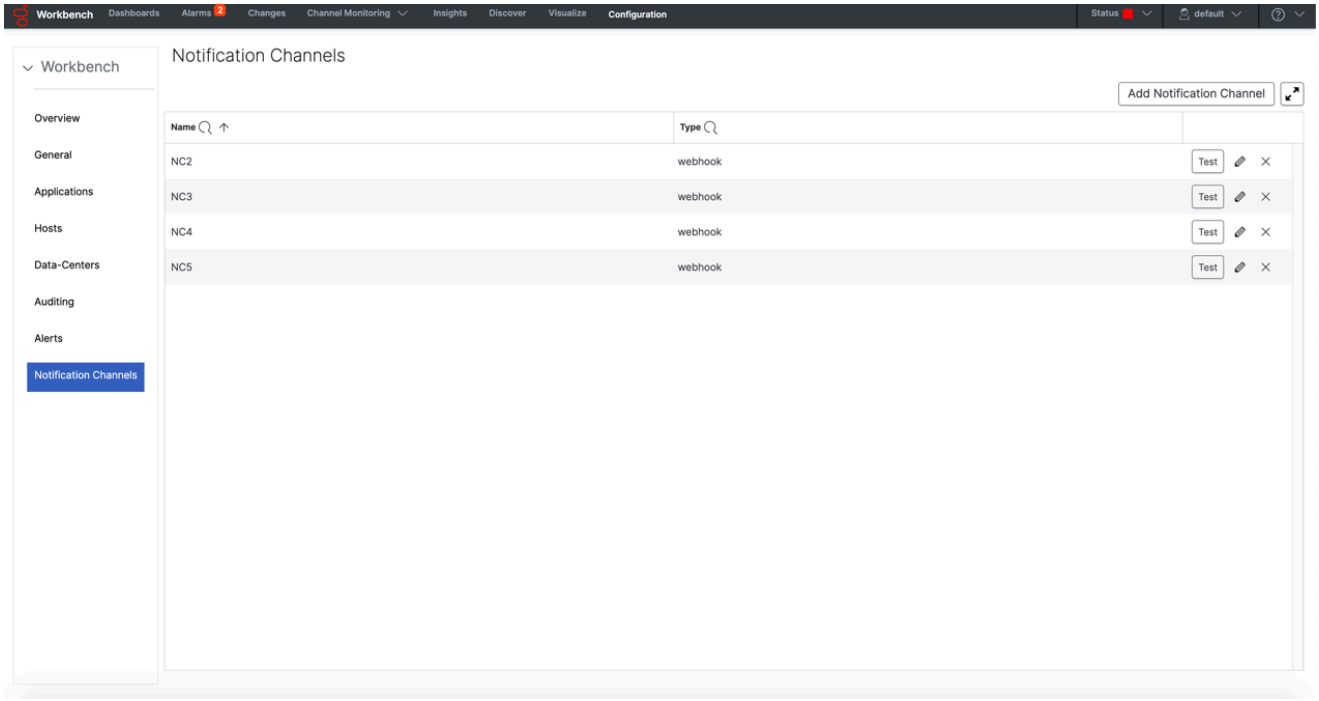
- When your configuration is complete
- Click **Save** to create the new Notification Channel
- Optionally click **Test** to invoke a test request to the HTTP[S] endpoint configured; the test functionality is detailed below

List of Notification Channels

If/when at least one Notification Channel exists, a list of Notification Channels is displayed.

- **Name** and **Type** properties are displayed to identify each Notification Channel

- Each Notification Channel has 3 action buttons: **Test**, **Edit** and **Delete**



Test a Notification Channel

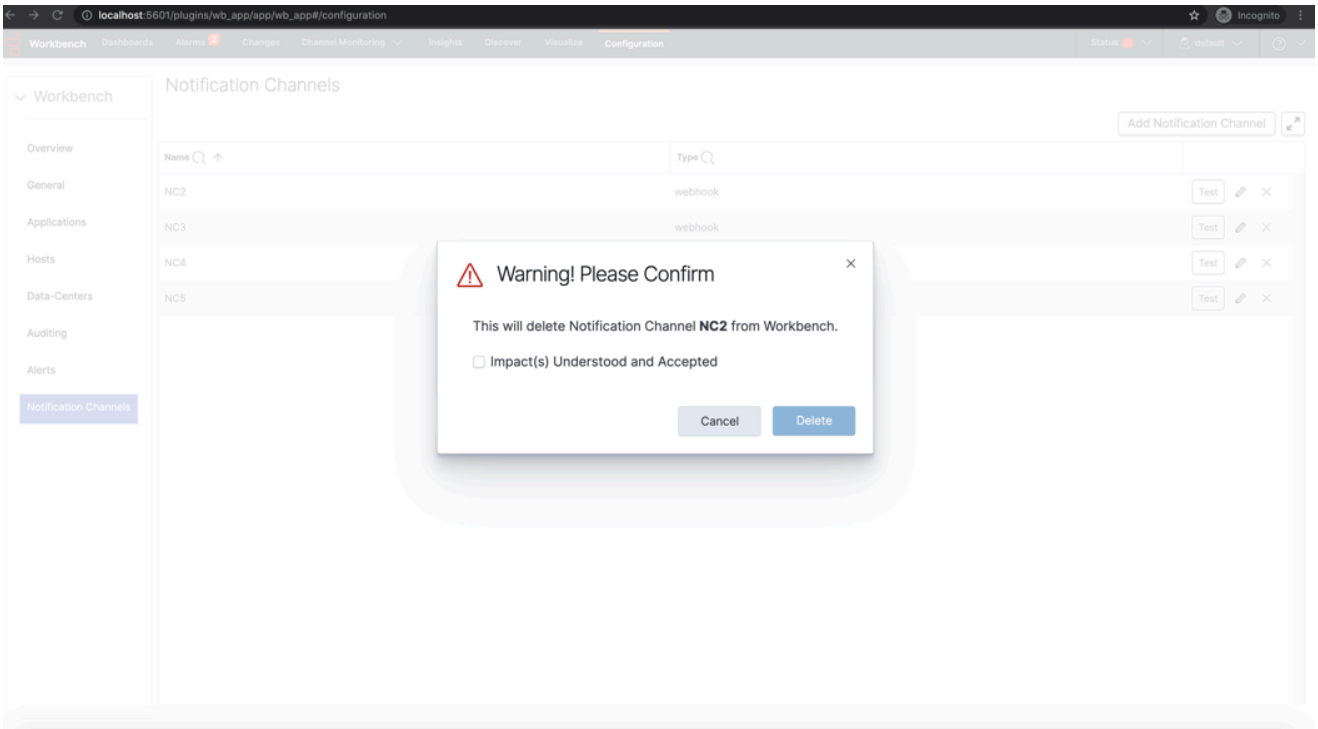
When the **Test** action button is clicked, a **test Alert** is sent to the corresponding Notification Channel; specifically, for Webhook Notification Channels, all the configured values are used to make an HTTP[S] request and depending on the response of the call a message of success or failure is shown at the bottom right of the page.

Edit Notification Channel

When the **Edit** action button is clicked, the Notification Channel form is opened in **Edit** mode, and it is populated with all the configuration properties that are associated to that Notification Channel; the form is the same as per the ‘Create Notification Channel’ section.

Delete a Notification Channel

When the **Delete** action button is clicked, a warning dialog is displayed to confirm the **Delete** action. If the delete action is confirmed, the Notification Channel will be **removed** from the Notification Channels list and a success dialog will be shown.



Example Python Webhook

The example Webhook code below provides a basic, test (not production), example Python code snippet that receives active Alarm payloads from Workbench, via the respective Notification Channel and Alerts configuration.

Important

- The Python code below is not supported and/or warranted by Genesys - it's merely an example of how a customer can create a simple Webhook

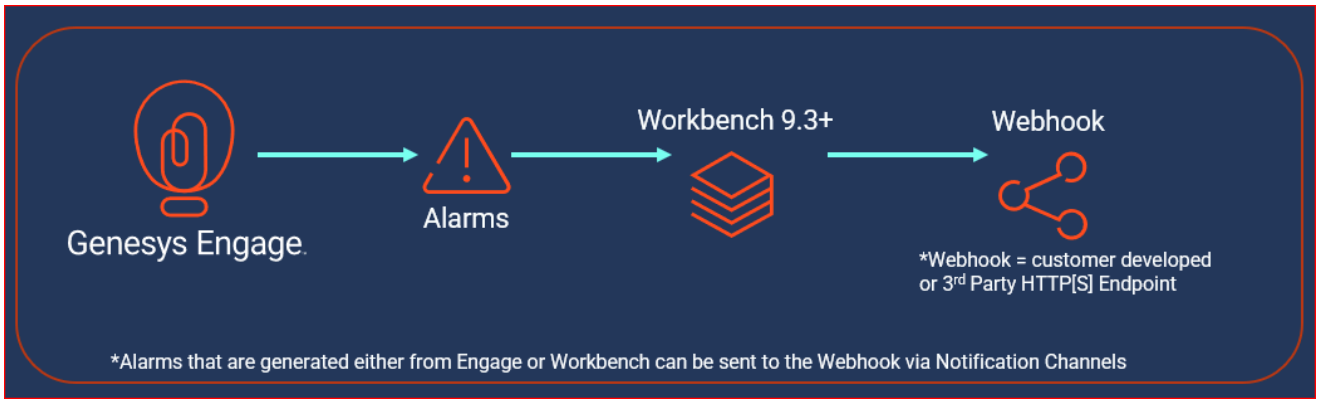
```python
#! /usr/bin/env python
from flask import Flask, jsonify, request  # pip install flask

app = Flask(__name__)

@app.post('/')
def json_dump():
    _data = request.get_json()
    print(_data)  # do something with the JSON payload - i.e. send to an email server, Slack/Teams channel, Case Management System, etc, etc
    return jsonify(_data), 200

if __name__ == "__main__":
    app.run(host='0.0.0.0', port=46664, debug=True)
```

Alerts

Workbench **Alerts** allows the user to configure the type of Workbench events that should be sent from Workbench, to a service, via Workbench Notification Channels.

Currently Workbench Alerts can be configured to send Genesys Engage On-Premise (i.e. Host Unavailable) and Workbench (i.e. Call Flow - No Answer) **Active Alarms** only.

The diagram below shows the external context of Workbench Alerts sending events to an external system and/or service via the Notification Channels:



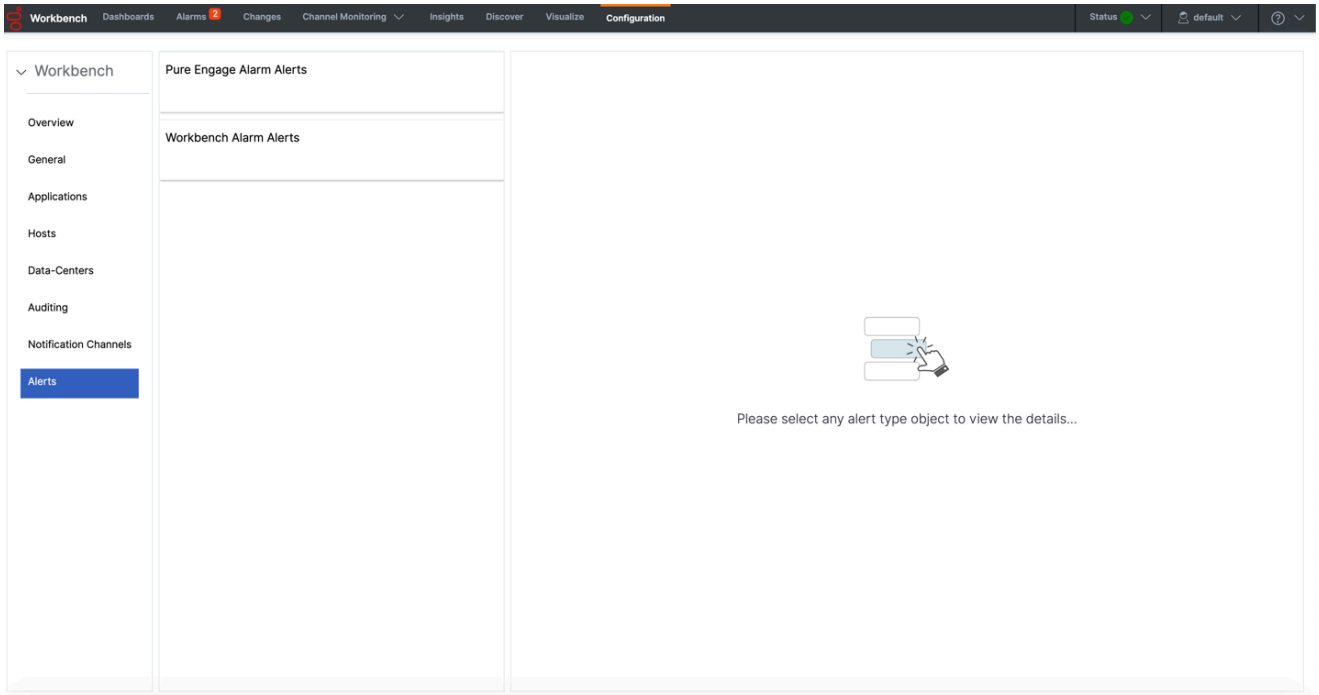
The following sections describes how to configure Alerts in Workbench.

Configuring Alerts

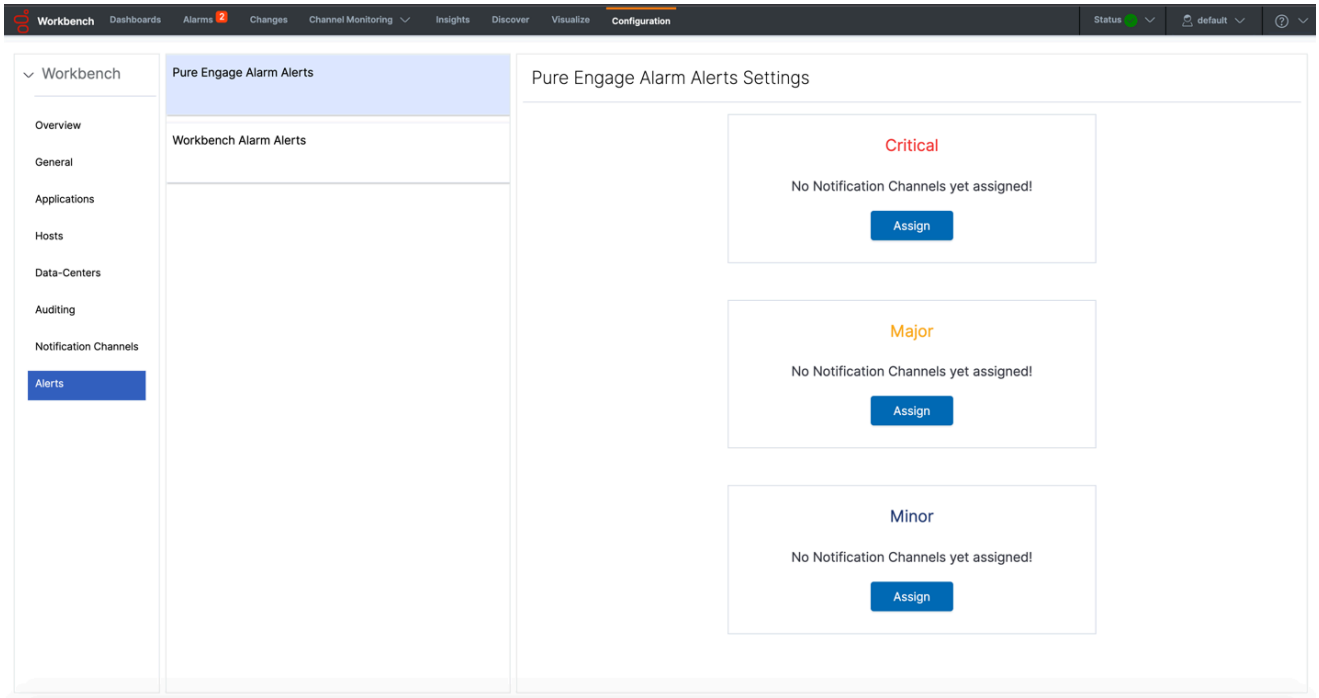
To configure an Alert for the first time:

- Navigate to the Workbench ‘Configuration Console’ on the top menu
- Click the ‘Alerts’ sub-menu

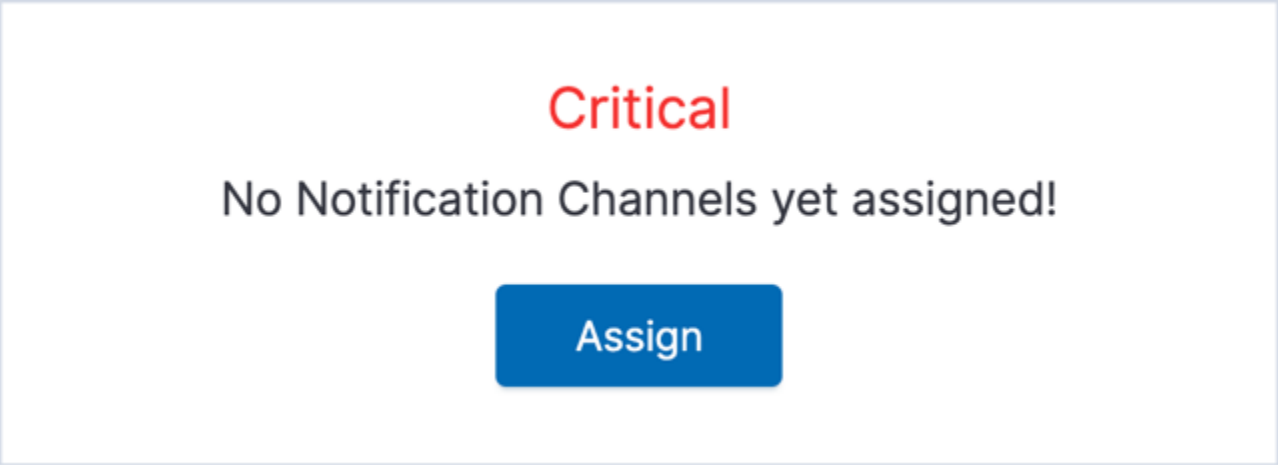
The following page will be displayed:



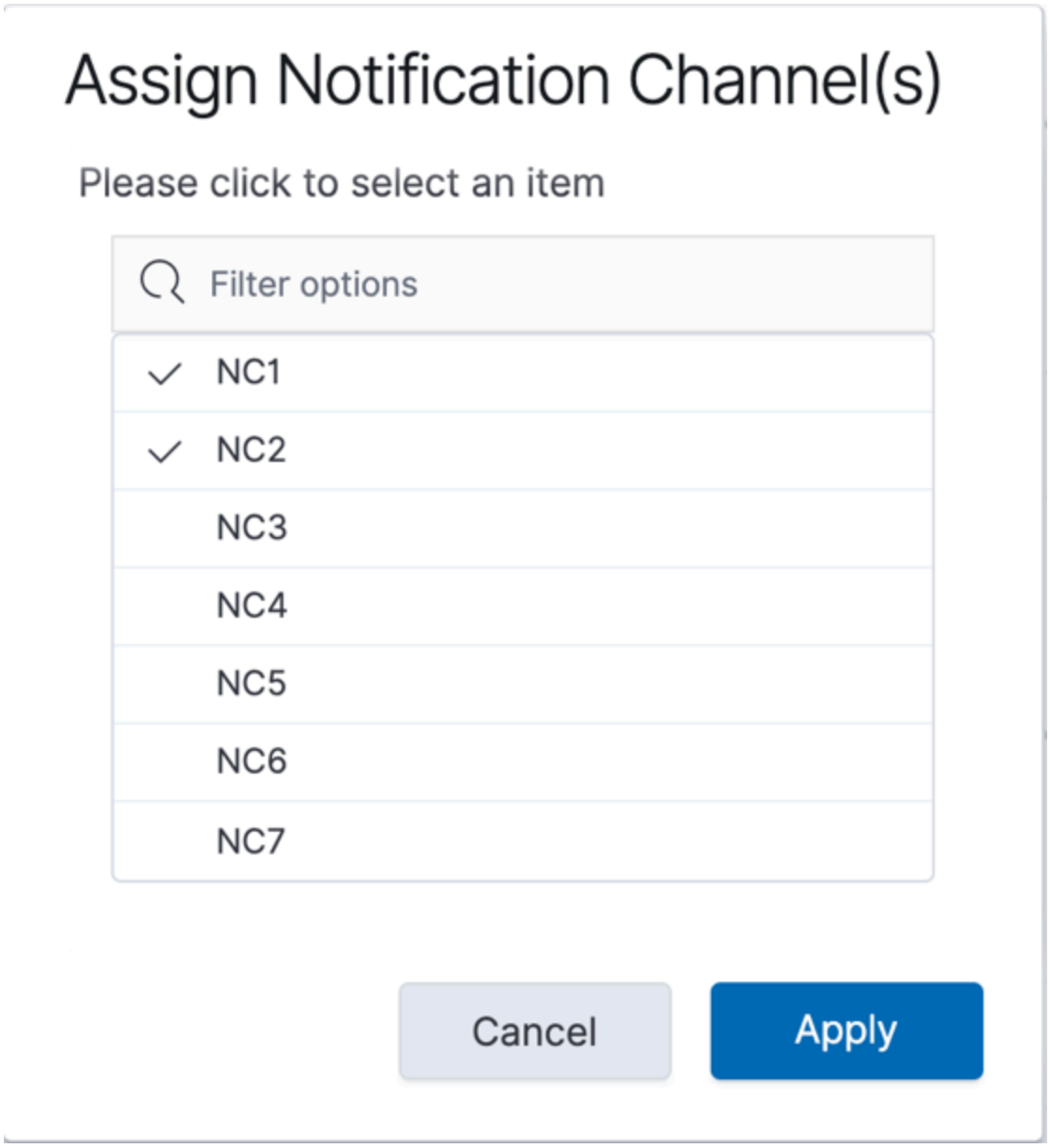
- From the middle pane (below), select the type of Alert to be configured - click either "PureEngage Alarm Alerts" or "Workbench Alarm Alerts"



- **PureEngage Alarm Alerts** and **Workbench Alarm Alerts** use the same UI layout
- Therefore, for purposes of this guide, **PureEngage Alarm Alerts** is the example scenario; repeat for "Workbench Alarm Alerts" if/when required
- Alarm Alerts have 3 Severity categories - **Critical**, **Major** and **Minor**
- Each *Critical*, *Major* or *Minor* Severity category can be configured to be associated to **one or more** Notification Channels
- Click the **Assign** button to assign a new Notification Channel(s) for the Critical Severity



- A dialog (below) is presented displaying the list of available Notification Channels that can be selected
  - **One or more** Notification Channels can be selected from the list by clicking on the corresponding row
  - To unselect, click the corresponding row of the already selected Notification Channel
- Once you have all the required Notification Channels selected for the particular Severity, click **Apply** button

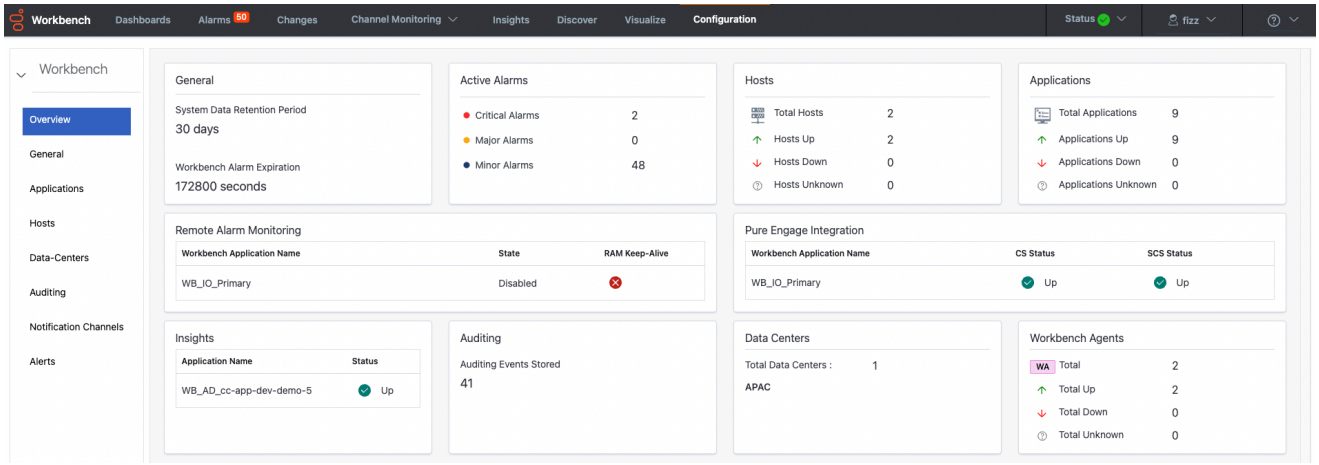


- Each Alarm category can be Enabled/Disabled individually
- To Enable/Disable transmission of Workbench Alerts, check/uncheck the checkbox displayed at the top of the respective alert section:

- The above configuration will now send "Critical Alarms" (received from Engage into Workbench) to the respective Notification Channel(s)
- Repeat the above steps for the "Workbench Alarm Alerts" type and/or also for each "Severity" thereof

Workbench Configuration

The Workbench Configuration Console allows the user to manage, configure and view the state/status of the Workbench components.



The Workbench 'Configuration Console' has the following sub menus:

- **Overview**
  - Gain an at-a-glance overview of the state, status and content of the Workbench components and features
- **General**
  - *System Data Retention Period*
    - this applies to the data stored within Workbench and the duration for which its stored; if this setting is enabled, data will be permanently deleted post this value; the default is Enabled and 30 days
      - Note: Data Retention values not updated in real-time when viewing this page
  - *Alarm Expiration*
    - this applies to the 'Workbench' *Active Alarms* duration, if not resolved, if this setting is enabled, Workbench alarms (not Genesys Engage) will be automatically closed post this value - i.e. to avoid *manually* clearing 100 Channel Monitoring active alarms, they would be automatically cleared post this value; the default is Enabled an 172800 seconds (2 days)
      - Note: Alarm Expiration values not updated in real-time when viewing this page
  - *Session Expiration*
    - this applies to the timeout of sessions; Users will be auto logged out of Workbench if/when a new request is greater than the Session Expiration; if/when the Session Expiration setting is unchecked/disabled, Users will *never* be auto logged out
- **Hosts**

- These are either Workbench hosts or Engage hosts
- Engage hosts will only be present if the Workbench Agent is installed on the respective Engage host (i.e. SIP Server host)
- Only deploy the Workbench Agent on Engage hosts that you wish to ingest metric data (CPU/RAM/DISK/NETWORK) from
- This Configuration section allows read-only *visibility* of Workbench Host Objects
  - The WB Host objects can be:
    - Deleted (i.e. should there be a need to move/re-install Workbench Additional components to a new Host/Server)

Warning

- Use the **Delete** option with extreme caution; please read and uderstand these instructions before progressing.
- This will permanently delete the WB Host Object from the WB UI and also backend configuration
- The WB Delete action will NOT delete the respective binaries from the host; that will be a manual task via the respective host post deleting in the WB UI

Warning

- WB Primary Host deletion is NOT supported - only Workbench **Additional** Hosts/Nodes can be deleted
- Pre-Cluster formation
  - Delete WB Secondary WB Host object from configuration page under Host section
    - **ALL** associated WB component config data will be permanently removed
    - Now and only when the WB Host is deleted, delete the associated Hosts WB Application component config objects one-by-one under Applications section
- Post-Cluster formation WB Host deletion is NOT recommended

- **Applications**
  - In Workbench 9.x there are 8 x Workbench Application Objects:
    - Workbench IO (for WB UI and integration to Genesys Engage including the Channel Monitoring feature)
    - Workbench Agent (for WB status, control and configuration - in WB 9.0 Workbench Agents are ONLY installed on Workbench hosts, not Genesys Engage hosts)
    - Workbench Elasticsearch (for WB storage)

- Workbench Kibana (for WB UI)
- Workbench Logstash (an ETL pipeline primarily relating to Workbench Agent Metric data ingestion)
- Workbench Heartbeat (for WB component health monitoring)
- Workbench Metricbeat (for Host/Process Metric data ingestion in conjunction with the Workbench Agent component)
- Workbench ZooKeeper (for WB configuration)

- This Configuration section allows visibility and managment of the Application Objects above
  - The Application Objects can be:
    - Renamed (i.e. "WB_IO_Primary" to "APAC_WB_IO_P")
    - Edited (i.e. change the *[WB_Kibana_Primary\HTTP Port]* setting from the default *8181* to *9191*)
    - Deleted (not the Workbench Primary host Applications)

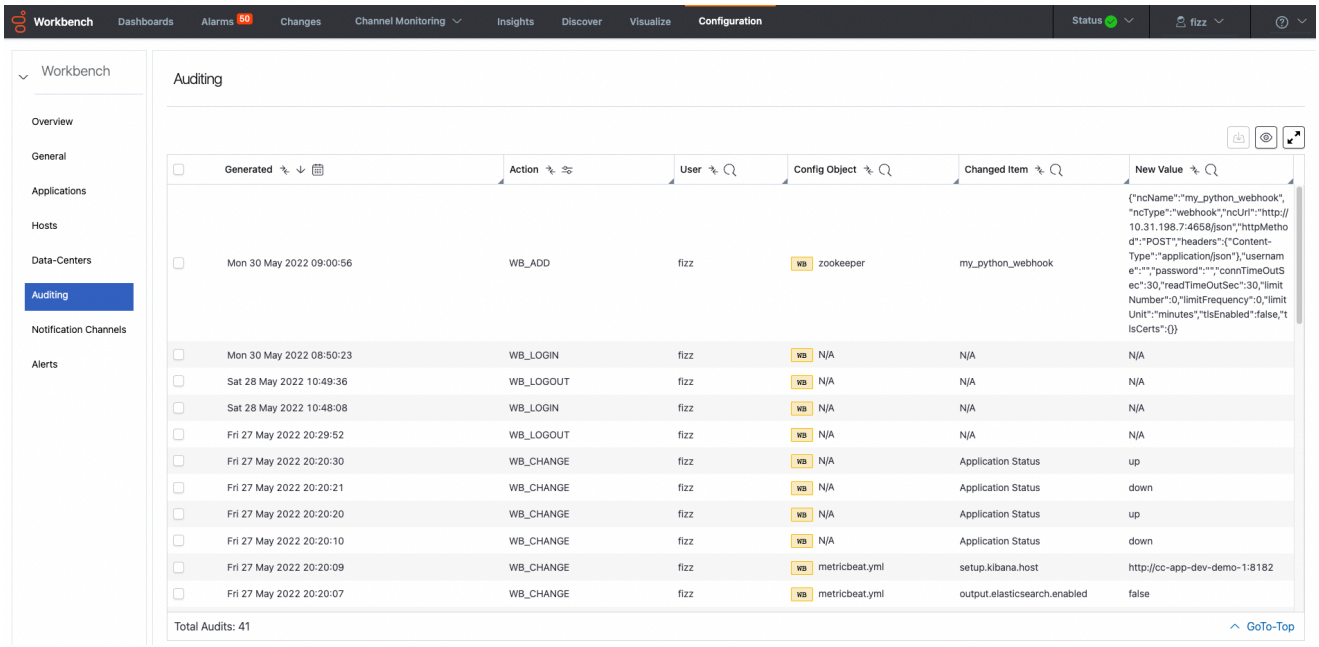
Warning

- Use the **Delete** option with extreme caution; please read and uderstand these instructions before progressing.
- This will permanently delete the WB Application Object from the WB UI and also backend configuration
- If the Workbench IO, Workbench Agent or Workbench Kibana *Application Types* are deleted, **a full re-install** will be required
- The WB Delete action will NOT delete the respective binaries from the host; that will be a manual task via the respective host

Warning

- WB Primary Host deletion is NOT supported - only Workbench **Additional** Hosts/Nodes can be deleted
- Pre-Cluster formation
  - Delete WB Secondary WB Host object from configuration page under Host section
    - **ALL** associated WB component config data will be permanently removed
    - Only when the WB Host object is deleted, delete the associated Hosts WB Application component config objects one-by-one under Applications section
- Post-Cluster formation WB Application deletion is NOT recommended

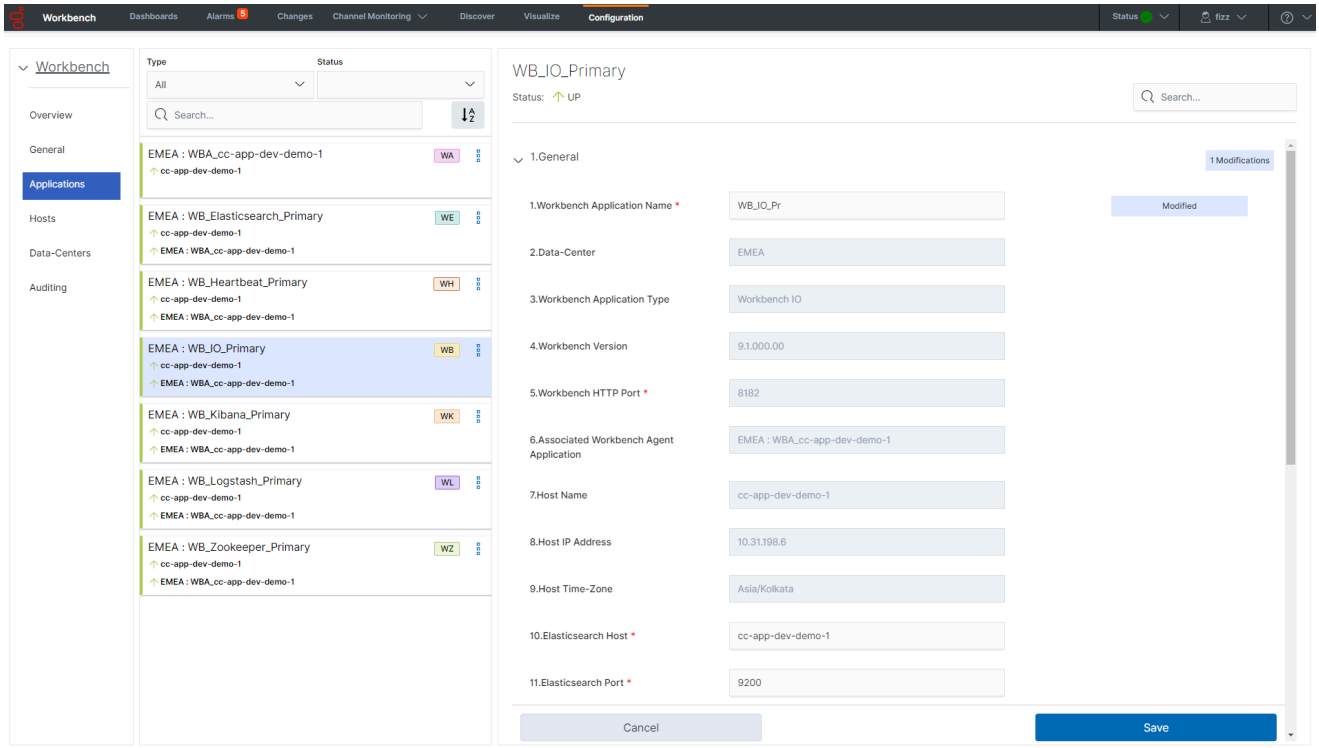
- **Data-Centers**
  - The Data-Center(s) name(s) are provided during WB installation and will be displayed according to the value(s) entered
- **Auditing**
  - The Workbench Audit Console is similar to the Changes Console but also provide visibility of WB User Logins/Logouts; the Audit events will also evolve overtime
    - Note: Audit events are not updated in real-time when viewing this page



Configuration Edit Example

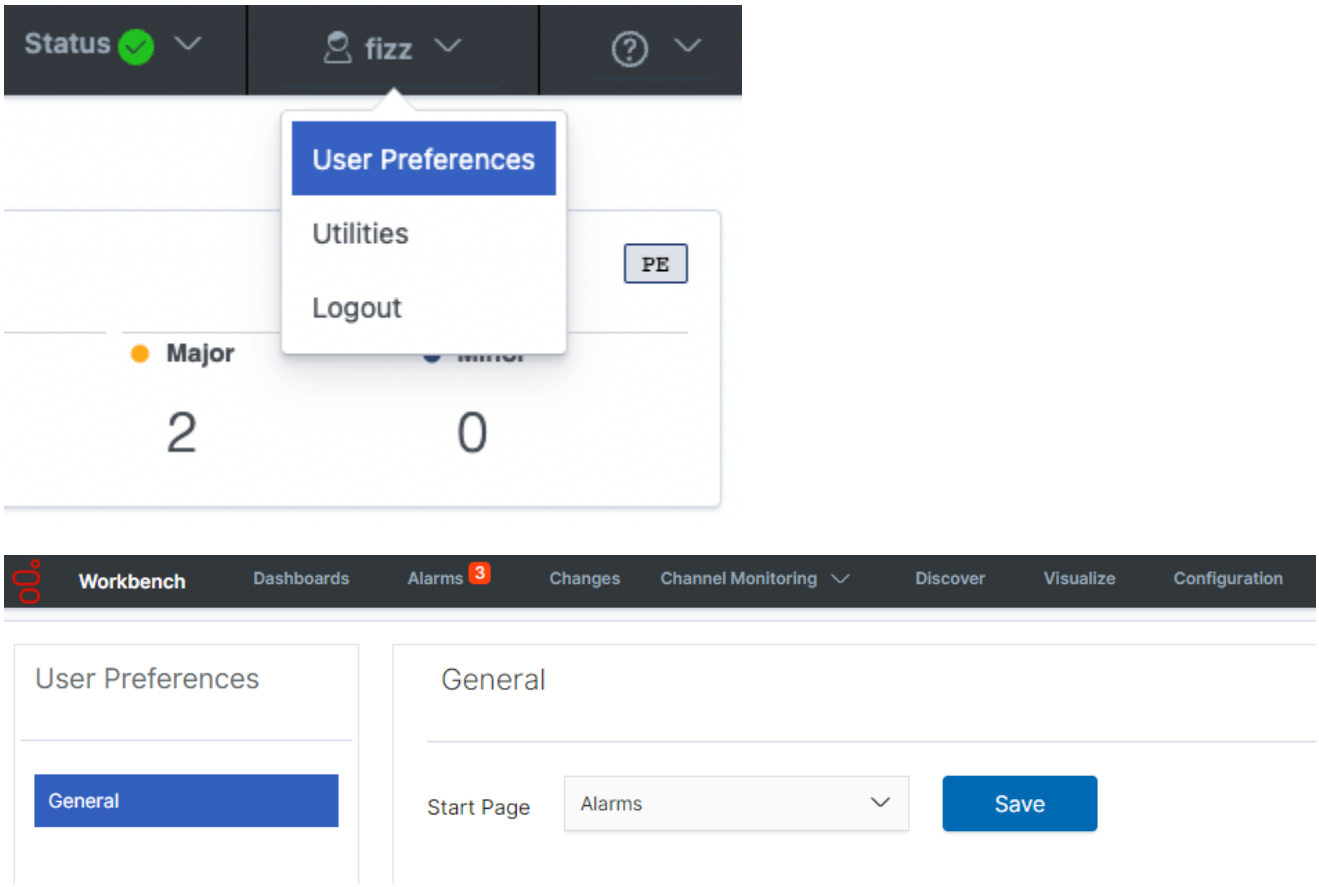
This example below show the "WB_IO_Primary" application being edited:

- The application name is being changed from "WB_IO_Primary" to "WB_IO_Pri"
- There's indication that 1 option/setting and has modified
- The **Save** button is enabled and when the user clicks Save the application will be subseqently renamed.


Workbench
Dashboards
Alarms 5
Changes
Channel Monitoring
Discover
Visualize
Configuration
Status
fizz
Workbench
Overview
General
Applications
Hosts
Data-Centers
Auditing
Type
All
Status
Search...
EMEA : WBA_cc-app-dev-demo-1
WA
cc-app-dev-demo-1
EMEA : WB_Elasticsearch_Primary
WE
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Heartbeat_Primary
WH
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_IO_Primary
WB
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Kibana_Primary
WK
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Logstash_Primary
WL
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
EMEA : WB_Zookeeper_Primary
WZ
cc-app-dev-demo-1
EMEA : WBA_cc-app-dev-demo-1
WB_IO_Primary
Status: UP
Search...
1.General
1 Modifications
1.Workbench Application Name *
WB_IO_Pr
Modified
2.Data-Center
EMEA
3.Workbench Application Type
Workbench IO
4.Workbench Version
9.1.000.00
5.Workbench HTTP Port *
8182
6.Associated Workbench Agent Application
EMEA : WBA_cc-app-dev-demo-1
7.Host Name
cc-app-dev-demo-1
8.Host IP Address
10.31.198.6
9.Host Time-Zone
Asia/Kolkata
10.Elasticsearch Host *
cc-app-dev-demo-1
11.Elasticsearch Port *
9200
Cancel
Save

Workbench User Preferences

Workbench enables users to configure their **Start Page** via the User/User Preferences navigation bar option.



The Workbench **Start Page** options being:

- Home Dashboard
- Dashboards
- Alarms
- Changes
- Channel Monitoring
- Insights
- Discover
- Visualize

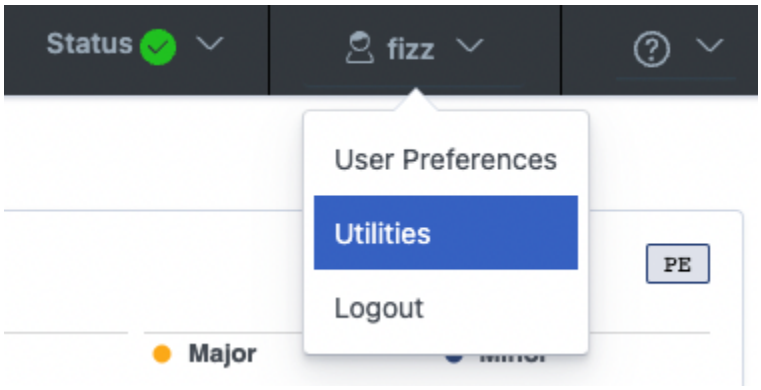
- Configuration

By default the Workbench **Start Page** is a shipped **Genesys Home** Dashboard displaying information such as:

- Workbench Status Summary
- Workbench Hosts Status Summary
- Workbench Application Summary
- Wokrbench Agent Status Summary
- Workbench to Genesys Engage Integration Summary
- Workbench Data-Center Summary
- Workbench Remote Alarm Monitoring (RAM) Status Summary
- Workbench General Information Summary

Utilities

Workbench 9.3+ has an "Utilities" option under User Preferences.



This Utilities option (Admin Users only) may be used to collect diagnostic data when troubleshooting Workbench issues.

Remote Alarm Monitoring

With the Workbench **Remote Alarm Monitoring** (RAM) Service activated, the customers on-premise Workbench instance transitions/transmits a specific subset of Genesys Engage Critical and Major Alarms, externally, to Genesys Customer Care, who will then proactively create a Genesys Case and will liaise, if required, with the customer accordingly to proactively progress and resolve the issue(s); the alarms can also sent to the customers mobile device via the Genesys Care Mobile App.

Workbench Remote Alarm Monitoring is an annual service available to customers, please contact your Genesys Care representive for further details.

The following pages will guide you on the following:

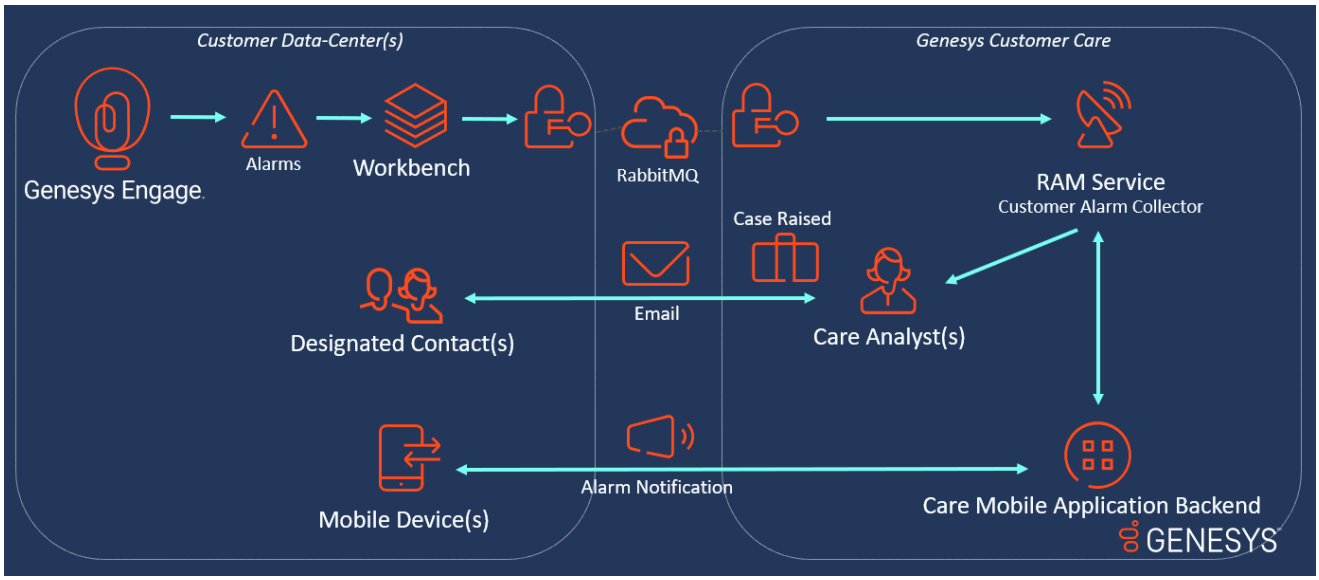
- How to get started with Remote Alarm Monitoring
- How to activate Workbench Remote Alarm Monitoring
- Using the Genesys Care Mobile App (for alarm notifications and to view alarm details)
- What alarm types are supported by Workbench Remote Alarm Monitoring
- What is the process when an alarm is received by Genesys Customer Care from the customers on-site Workbench installation
- Advising Customer Care about Maintenance Windows

> **Important**
>
> - Entitlement to the Workbench Remote Alarm Monitoring feature can be confirmed via your Genesys Care maintenance representative; if/when entitled, please follow the Getting Started section/page within this Remote Alarm Monitoring chapter.

Workbench with Remote Alarm Monitoring Architecture

When Remote Alarm Monitoring is also deployed, Workbench communicates over a secure RabbitMQ connection with Genesys, where additional service components are located, as shown in the figure below.

- Genesys Customer Alarm Collector to process alarms detected in your environment
- Genesys Care Mobile Application to notify you about alarms as they are detected
- Genesys Customer Care to route each Critical and Major alarm to a support expert, who proactively opens a case and immediately begins to troubleshoot the issue


Customer Data-Center(s)
Genesys Customer Care
Genesys Engage
Alarms
Workbench
RabbitMQ
RAM Service
Customer Alarm Collector
Case Raised
Email
Designated Contact(s)
Care Analyst(s)
Alarm Notification
Mobile Device(s)
Care Mobile Application Backend
GENESYS

Getting Started

> **Important**
>
> - Entitlement to the Workbench Remote Alarm Monitoring feature can be confirmed via your Genesys Care maintenance representative; if/when entitled please follow the section/page below.

Workbench is required for Remote Alarm Monitoring, therefore Workbench must be installed before you can activate Remote Alarm Monitoring.

1. You will also need a Remote Alarm Monitoring License Key.
2. You will also need to determine your Public Corporate IP Address.

Post Workbench installation, please complete the steps documented below to enable Workbench Remote Alarm Monitoring:

Determine your Public IP address

For security and Remote Alarm Monitoring activation, Genesys requires your **corporate public IP address** for each Workbench site installation, before we can issue you a Workbench RAM license key.

> **Important**
>
> Please liaise with your internal IT department to determine/clarify your corporate public IP address.

Request a License Key (must be a Designated Contact)

1. Login to My Support
2. Select **Open Admin Case** - located after selecting **Manage Profile** from the header.
3. If asked, select your End User / Sold To Account combination.
4. Populate each Mandatory Field with the required information.
5. Add the text **Alarm Monitoring License Request** in the **Subject line**.
6. In the **Description box**, provide your **company public IP address**.

1. Also in the **Description** field, please provide a **Group Email Address** (i.e. *support_team@mycompany.com*).
    1. When a Support Case is opened as a result of an alarm, the email notification will be sent to this group email address.
    2. It is required that at least **one Designated Contact** at your company be included in this group email.
    3. The Designated Contact can be the same person who is requesting the Remote Alarm Monitoring License Key or a different Designated Contact at your company.
    4. You may have more than one Designated Contact in the group email.
    5. Other employees on the group email should consider requesting **My Support Read-Only Access** if they would like to view case details.
    6. Please see the table below for details on My Support Access Levels and Privileges.
7. Lastly, select **Priority 4-Low** and select case sub type **Request: CC Tools License**.
8. **Save** your Admin Case.

You will receive your Workbench Remote Alarm Monitoring license key, via email, within 72 hours.

> **Important**
>
> Once your Workbench Remote Alarm Monitoring license key is received review Remote Alarm Monitoring - Activation for details on activating Workbench Remote Alarm Monitoring.

My Support Access Levels and Privileges

At least one employee in the group email address you provided should be a Genesys **Designated Contact**; we recommend that additional employees have My Support Read-Only Access.

Visit the My Support Registration Page to request access. You can read about My Support Access Levels for more information and Manage Profiles to change your current My Support access level.

The chart below details the privileges available to users on the alarm monitoring group email list. Note that for full benefits, users must have My Support access and have downloaded the Genesys Care Mobile App.

Privilege	My Support Designated Contact	My Support Read-Only
Open cases on My Support	X	
Receive alarm notifications on mobile app	X	X

Privilege	My Support Designated Contact	My Support Read-Only
View alarm details on mobile app	X	X
View case information on mobile app	X	X
Email from Customer Care when a case is opened due to an alarm received	X	X
View support cases opened due to an alarm	X	X
Manage and close alarm support cases via My Support	X	
Respond to and close alarm support cases via email	X	X
View Alarms Console in Workbench	X	X
See additional alarm events in the event correlation display	X	X
Acknowledge alarms in Workbench Alarm Monitoring console and have that acknowledgement synched with Solution Control Server (SCS) and vice versa	X	X

Remote Alarm Monitoring Activation

Once you receive your Workbench Remote Alarm Monitoring license key from Genesys Customer Care, use the steps below to activate your subscription:

> ### Warning
>
> - Only 1 x WB IO application in a multi node Workbench Cluster should have a RAM license enabled
>   - If you have APAC, EMEA and LATAM Data-Centers - assign the RAM License to either APAC, EMEA or LATAM - do NOT add/enabled on all 3 Data-Centers

1. **Login** to Workbench
2. Navigate to **Configuration** via the navigation bar
3. **Select** Applications
4. **Select** the Workbench IO Primary application (i.e. post installation and by default this would be **WB_IO_Primary**)
    1. The Workbench IO application configuration details are displayed
5. Within the Workbench IO Application Configuration panel expand the **8.Remote Alarm Monitoring (RAM) Service** section
6. **Click/Check** the **Enabled** checkbox - to enable WB to send Alarms to the Remote Alarm Monitoring Service
7. Enter your *License Key/End User ID* into the **End User ID** field
8. Enter your *Origin* into the **Origin** field (i.e. "EMEA" - a text value of your choice to better describe the region/location/data-center/site of Workbench)
9. Verify the above
10. Click **Save**
11. Restart the Workbench IO Application **Service** on the respective host; required for the license/service to take effect.

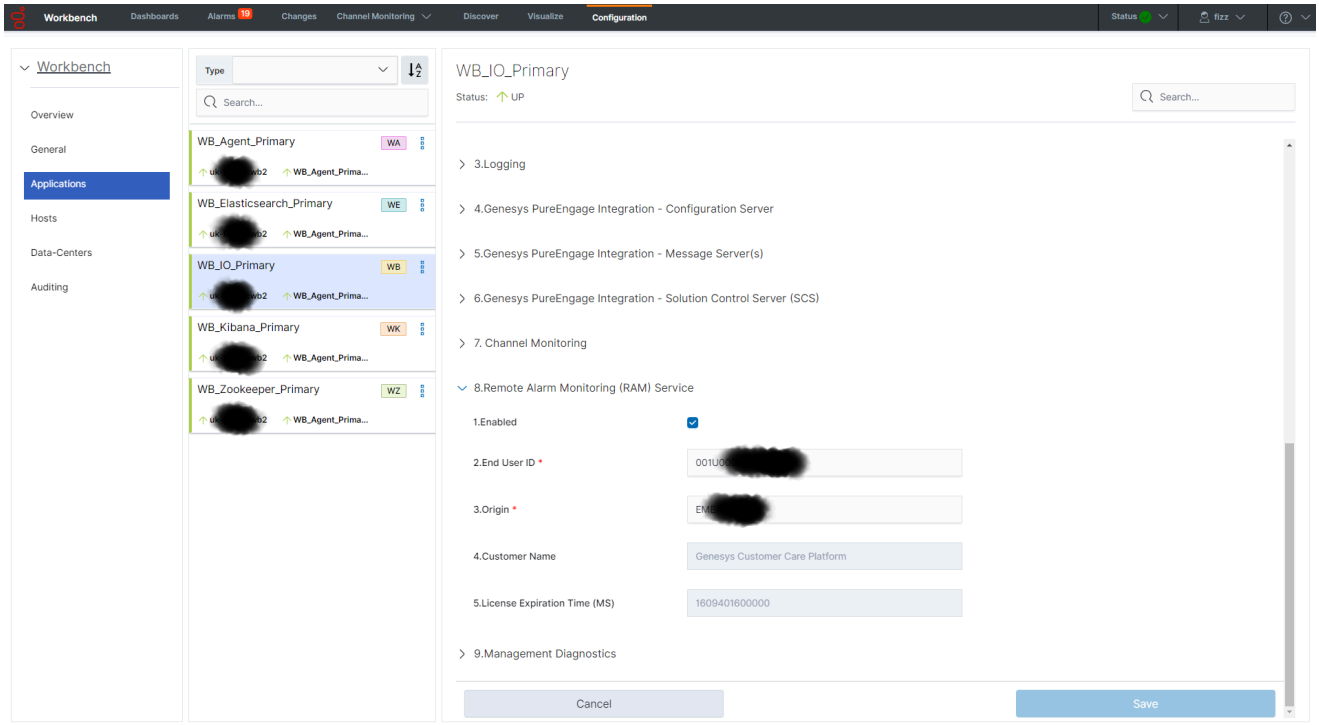
Once the Workbench IO Application Service has been restarted the **Customer Name** and **License Expiration Time** fields will be auto-populated, this is an indicate of successful communication between the on-premise Workbench instance and the Remote Alarm Monitoring Service.

From here on the supported Workbench RAM Alarms will be transitioned to the RAM Service and intelligently routed into Genesys Customer Care and subsequently a Genesys Customer Care Analyst, from there a Genesys Support Case will be raised by the Genesys Analyst..

Important

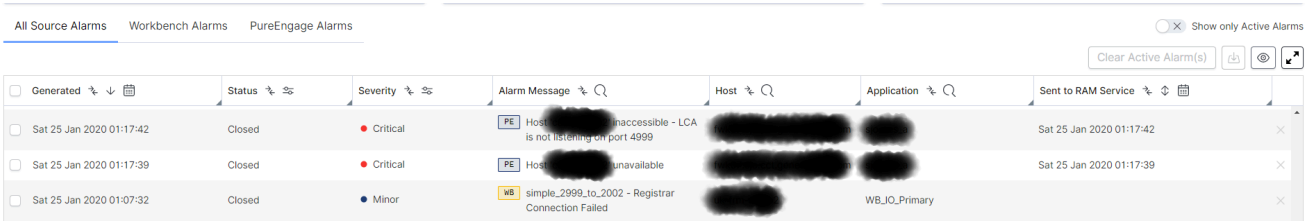
- The Workbench IO Application Service on the respective host needs to be restarted for the license/service to take effect.
- The **Customer Name** field is read-only; this name is obtained via the communication between Workbench and the RAM Service.
- The **License Expiration Time** field is read-only; this name is obtained via the communication between Workbench and the RAM Service
- Since Remote Alarm Monitoring is implemented at the Genesys Account level, only **one Workbench RAM License Key/End User ID is required per company/ organisation**

The image below provides some content on RAM configuration:



Remote Alarm Monitoring Event Visibility

Use the Alarm Console to view which Alarms were routed to the Remote Alarm Monitoring Service, utilise/show the "Sent to RAM Service" column to visualize when the alarm was sent from Workbench to the RAM service.


All Source Alarms
Workbench Alarms
PureEngage Alarms
Show only Active Alarms
Clear Active Alarm(s)
Generated
Status
Severity
Alarm Message
Host
Application
Sent to RAM Service
Sat 25 Jan 2020 01:17:42
Closed
Critical
PE
inaccessible - LCA is not listening on port 4999
Sat 25 Jan 2020 01:17:42
Sat 25 Jan 2020 01:17:39
Closed
Critical
PE
unavailable
Sat 25 Jan 2020 01:17:39
Sat 25 Jan 2020 01:07:32
Closed
Minor
WB
simple_2999_to_2002 - Registrar Connection Failed
WB_IO_Primary

Mobile App

The Genesys Mobile App provides the convenience to view and manage Genesys Support Cases from your mobile device (iOS and Android); utilise the Genesys Mobile App to review and post Genesys Case updates, initiate Chat sessions with Genesys Analysts, request Case Escalation or Case Closure.

In addition, with the Workbench Remote Alarm Monitoring (RAM) service activated and if push notifications are enabled, Workbench RAM will push alarm notifications to your mobile device so that you can view and manage the alarm Support Cases that have been generated from your Genesys Engage platform.

Designated Contacts can view/manage the alarm Support Case(s) and post Case updates via the mobile app; Read-Only access levels can view alarms and Support Case details.

Getting Started

Please review the Genesys Care Mobile App Guide for information on where to download (iOS and Android available) our mobile app, how to use the mobile app, and the type of alarm data you can view.

Supported Alarms

This table shows the types of alarms supported specifically for the Workbench Remote Alarm Monitoring Service from Genesys.

More alarms may display within Workbench, but only the alarm types listed below will be forwarded to Genesys as part of the Remote Alarm Monitoring Service.

Alarm Name	Alarm Level	Alarm Description
Not Enough Disk Space	Critical	An application detects low disk space
Licensing violation is identified, the violation type [type]	Critical	Licensing violation is identified, the violation type [type]
Cannot connect to server	Major	Reports that the application cannot connect to the server
Cannot open port	Major	Cannot open port [port number] for listening, reason [reason]
Client / Server incompatibility	Major	Client version [number-1] is incompatible with server version [number-2]
Application terminated due to internal condition	Major	Application terminated due to internal condition
Host [host name] inaccessible. LCA is not listening on port [port number]	Major	Host [host name] inaccessible. LCA is not listening on port [port number]
Host [host name] unavailable	Major	A host where Genesys daemon applications are running is unavailable (turned off)
Host [host name] unreachable	Major	The Management Layer cannot reach the host where Genesys daemon applications are running (no route to the host)
All [total licenses] licenses are in use already, registration rejected	Major	All [total licenses] licenses are in use already, registration rejected
Error reading backup file '[name]': '[errtext]'	Major	Error reading backup file '[name]': '[errtext]'
Backup file '[name]' is corrupt	Major	Backup file '[name]' is corrupt
Failed to store statistics ([definition]) into backup file '[name]' (error: '[errtext]')	Major	Failed to store statistics ([definition]) into backup file '[name]' (error: '[errtext]')
Configuration Server Error: [error]	Major	Configuration Server Error: [error]
CTI Link disconnected	Major	Failure of connection between any T-Server and its switch

Alarm Routing

When Genesys Customer Care receives a Workbench Remote Alarm Monitoring alarm from the customers Workbench instance, the following process is actioned:

- The respective alarm (the supported subset of Genesys Engage alarms ingested by Workbench) is routed to Genesys Customer Care and a Support Case is opened by a Genesys Customer Care Analyst
- The customer provided **Group Email** will receive an email from Genesys Customer Care informing you that an alarm Support Case has been opened
- The Genesys Support Case will follow standard service level targets based on your Genesys Care contract
- Only the Designated Contact can view, manage and close the support case via My Support; however, all members on the group email can provide case updates via email.
- An Alarm notification is sent to you via the Genesys Care Mobile App, if notifications are enabled

Maintenance Windows

Our Customer Care team would appreciate knowing in advance when you have scheduled Maintenance Windows so that we can suppress alarms during that timeframe.

To notify us of an upcoming Maintenance Window, please send an email to customercare@genesys.com with “Alarm Monitoring – Maintenance Window” in the subject line and provide the following information:

- Your Account name
- The Site name
- Date and Time of maintenance in including timezone
- or, a schedule of planned maintenance

> **Important**
>
> All Maintenance Window requests, whether new or revised, must be submitted 2 (two) working days prior to it taking effect.

> **Important**
>
> Aternatively the Workbench RAM Service can be disabled via the Workbench>Configuration>Workbench IO>Remote Alarm Monitoring (RAM) Service section for the duration of the maintenance window; this would require a restart of the Workbench IO application so that the disablement would take effect.

Workbench Configuration Options

This section describes the configuration options used to configure the Workbench application components, including:

- Workbench Configuration Options Dependencies
- Workbench Host Application Type Configuration Options
- Workbench IO Application Type Configuration Options
- Workbench Agent Application Type Configuration Options
- Workbench Elasticsearch Application Type Configuration Options
- Workbench Kibana Application Type Configuration Options
- Workbench Logstash Application Type Configuration Options
- Workbench Heartbeat Application Type Configuration Options
- Workbench Zookeeper Application Type Configuration Options

Workbench Configuration Option Dependencies

Workbench IO - Configuration Dependencies

- If/when WB_IO_Primary application **Section 1 [General\Workbench HTTP Port]** is changed:
  - For WB 9.0 to 9.2 - **8182** is the default
  - For WB 9.3 - **8181** is the default (the main Workbench login page)
  - the new HTTP Port value now also needs to be updated in:
    - **workbench.url** config key in the **kibana.yml** (located in *C:\Program Files\Workbench_9.x.xxx.xx\Kibana* by default)
    - **WB_Logstash_Primary\Metrics Pipeline\Event IO Output Host** would need the new Workbench HTTP Port value
    - **WB_Logstash_Primary\Status Pipeline\Event IO Output Host** would need the new Workbench HTTP Port value
  - A **restart** of the Workbench IO, Workbench Heartbeat and Workbench Logstash(s) components is also required pertaining to this Workbench Data-Center node/cluster

Workbench Kibana - Configuration Dependencies

- If/when WB_Kibana_Primary application **Section 4 [Workbench Kibana Identifiers\HTTP Port**] is changed:
  - For WB 9.0 to 9.2 - **8181** is the default (the main Workbench login page)
    - The Chrome Browser URL for Workbench will now be *http://WB_Primary_HOST_OR_IP:<NEW PORT>*
      - i.e. http://WB1:9797
  - For WB 9.3 - **8182** is the default (localhost access only)
  - A **restart** of the Workbench Kibana, Workbench Heartbeat components is also required pertaining to this Workbench Data-Center node/cluster

Workbench Elasticsearch - Configuration Dependencies

- If/when Workbench Elasticsearch application(s) **Section 5 - [Workbench Elasticsearch Identifiers\HTTP Port**] is changed (**9200** by default):
  - the new HTTP Port value now also needs to be updated in:
    - **WB_IO_Primary\[General\Elasticsearch Port]**
      - i.e. <NEW_PORT>
    - **WB_IO_Primary\[General\Elasticsearch Nodes]**
      - i.e. WB1:<NEW_PORT>,WB2:<NEW_PORT>,WB3:<NEW_PORT>
    - **WB_Kibana_Primary\[Workbench Kibana Identifiers\Workbench Elasticsearch Host]**
      - i.e. http://WB1:<NEW_PORT>,http://WB2:<NEW_PORT>,http://WB3:<NEW_PORT>
    - **WB_Logstash_Primary\[Metrics Pipeline\Event Elastic Output Host]**
      - i.e. http://WB1:<NEW_PORT>,http://WB2:<NEW_PORT>,http://WB3:<NEW_PORT>
  - A **restart** of the Workbench IO, Workbench Elasticsearch, Workbench Kibana, Workbench Heartbeat and Workbench Logstash(s) components is also required pertaining to this Workbench Data-Center node/cluster

Workbench Logstash - Configuration Dependencies

- If/when Workbench Logstash application(s) **Section 7 - [Metrics Pipeline\Event Input Port**] is changed (**5048** by default):
  - the new Port value now also needs to be updated in:
    - **WBA_<HOSTNAME>\Metrcbeat General\Metricbeat Output**
      - i.e. WB1:<NEW_PORT>
  - A restart of **ALL** the Workbench Agents, Workbench Heartbeat and Workbench Logstash(s) is also required pertaining to this Workbench Data-Center node/cluster
- If/when Workbench Logstash application(s) **Section 8 - [Status Pipeline\Event Input Port**] is changed (**5047** by default):
  - the new Port value now also needs to be updated in:
    - **WB_Heartbeat_Primary\Workbench Heartbeat Identifiers\Logstash Output**
      - i.e. WB1:<NEW_PORT>

- A **restart** of Workbench Heartbeat and Workbench Logstash(s) components is also required pertaining to this Workbench Data-Center node/cluster

Workbench Zookeeper - Configuration Dependencies

- If/when Workbench Zookeeper application(s) **Section 5 [Workbench Zookeeper\Workbench Zookeeper Port**] is changed (*2181* by default):
  - the new ZooKeeper Port value now also needs to be updated in:
    - **WB_IO_Primary\[General\ZooKeeper Nodes]**
      - i.e. WB1:6181,WB2:6181,WB3:6181
  - A **restart** of Workbench ZooKeeper, Workbench IO, Workbench Heartbeat components is also required pertaining to this Workbench Data-Center node/cluster

Workbench MetricBeat- Configuration Dependencies

- If/when WBA_{hostname} application **Section 4 [MetricBeat General\MetricBeat Http Port**] is changed:
  - A **restart** of the Workbench MetricBeat is required pertaining to this Workbench Data-Center node/cluster

Workbench IO Application Type

General Section

Editable Options

Workbench Application Name

Default Values: "WB_IO_Primary"
Valid Values: Any String name (i.e. "EMEA_WB_IO")
Changes Take Effect: Immediately
Description: The name of the Workbench IO (Karaf) Application

Elasticsearch Host

Default Values: The Hostname/IP Address of the Workbench Elasticsearch application
Valid Values: Valid Hostname/IP Address (i.e. "LAB-WB-VM1" or "10.20.30.40")
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The Hostname/IPv4 address of the Workbench Elasticseach application that this Workbench IO application is connecting to

ElasticSearch Port

Default Values: 9200 (or the port number given at custom installation time)
Valid Values: A valid and free port number (i.e. not used by other applications on the host)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The Port of the Workbench Elasticseach Applications that is used by this application

> **Warning**
>
> - Restart of Workbench Elasticsearch, Workbench_IO, Kibana, Logstash and Heartbeat required when this option is changed.
> - Workbench Logstash components will need to be changed to this new port.

Elasticsearch Nodes

Default Values: #ES_NODES
Valid Values: Elasticsearch Nodes:Port (i.e. "WB1:9200,WB2:9200,WB3:9200"
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The list of Elasticsearch Nodes to use for clustering; please review section on Installing

Additional Nodes

> **Warning**
>
> - Restart of Workbench Elasticsearch, Workbench_IO, Kibana, Logstash and Heartbeat required when this option is changed.
> - Workbench Logstash components will need to be changed to this new port.

ZooKeeper Nodes

Default Values: <PRIMARY_NODE_HOSTNAME>:2181
Valid Values: ZooKeeper Nodes
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The list of ZooKeeper Nodes to use for clustering; please review section on Installing Additional Nodes

Read Only Options

Workbench Application Type

Default Values: Workbench IO
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The Workbench Application Version

Workbench HTTP Port

Default Values:

- For WB 9.0 to 9.2 - the default port is: **8182** (or the port number given at custom installation time)
- For WB 9.3 - the default port is: **8181** (or the port number given at custom installation time)

Valid Values: A valid and free Port number (i.e. not used by other applications on the host)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description:
For WB 9.0 to 9.2 - used for integration from the Kibana Http Port
For WB 9.3 - the main UI port at which Workbench Users connect via their Chrome browser

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: default
Valid Values: Read-Only
Changes Take Effect: Aftern Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench IO application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The Hostname of the host where this Workbench IO application is running

Host IP Address

Default Values: *IP Address* of the Workbench IO application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The IPv4 Address of the host where this Workbench IO application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench IO application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: The Time-Zone of the host where this Workbench IO application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\Karaf"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.1.0000.00\Karaf")
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\Karaf\etc"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.1.0000.00\Karaf\etc")
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: INFO
Valid Values: ALL, INFO, DEBUG, ERROR, WARNING, FATAL, TRACE, OFF
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Application/Component Logging Level (e.g. INFO or DEBUG)

Log File Location

Default Values:<WORKBENCH_HOME>\Karaf\data\log
Valid Values: Valid Path (i.e. "C:\Program Files\Workbench_9.1.0000.00\Karaf\data\log")
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Absolute path of the folder where the Workbench IO application log file is located

Segment (MB)

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Maximum count of log files before rotated/cycled

Genesys Engage Integration - Configuration Server

Editable Options

Primary/CSProxy Configuration Server Host Name or IP Address

Default Values: Hostname/IP Address of the Genesys Engage Configuration Server (CS) provided during Workbench installation
Valid Values: Valid Hostname/IP Address
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Hostname/IPv4 address of the Genesys Engage Configuration Server that is used by the Workbench IO application

Primary/CSProxy Configuration Server Port

Default Values: Port number of Genesys Engage Configuration Server given during installation time (i.e. 2020)
Valid Values: Valid positive integer (i.e. not used in other application)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Port of the Genesys Engage Configuration Server that is used by the Workbench IO application

Genesys Engage Workbench Client Application Name

Default Values: Workbench Client Application name in the Genesys Engage Configuration Server provided during Workbench installation
Valid Values: The correct Genesys Engage *Workbench Client* Application name created prior to Workbench installation (i.e. **WB9Client**)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The Genesys Engage "Workbench Client" application name; this has to be configured in Genesys Engage prior to Workbench installation

Genesys Engage Workbench Server Application Name

Default Values: Workbench Server Application name in the Genesys Engage Configuration Server provided during Workbench installation
Valid Values: The correct Genesys Engage *Workbench IO (Server)* Application name created prior to Workbench installation (i.e. **WB9IO**)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The Genesys Engage "Workbench Server" application name; this has to be configured in Genesys Engage prior to Workbench installation

Genesys Engage Integration - Message Server(s)

Editable Options

Enabled

Default Values: Enabled
Valid Values: Enabled/Disabled
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Determines if Workbench IO connects to the Genesys Engage Message Servers; if not Changes Console "ChangedBy" field will be "N/A"

Genesys Engage Message Server Application(s)

Default Values:
Valid Values: Valid String: The correct Genesys Engage Log Message Application name (i.e. "log_message_server")
Changes Take Effect: After IO application (i.e. "WB_IO_Primary") restart
Description: Genesys Engage Message Server application name to which Workbench will connect for *Changes ChangedBy* metadata information

Genesys Engage Integration - Solution Control Server (SCS)

Editable Options

Genesys Engage Solution Control Server Application

Default Values: The selected Genesys Engage Solution Control Server application provided during Workbench installation
Valid Values: Valid String: The correct Genesys Engage Solution Control Server (SCS) application name (i.e. "emea_scs_primary")
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Genesys Engage Solution Control Server application name to which Workbench will connect for Genesys Engage Alarm integration

Remote Alarm Monitoring (RAM) Service

Editable Options

Enabled

Default Values:
Valid Values: True/False
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Is Remote Alarm Monitoring enabled; only enable if/when a RAM license has been received from Genesys Customer Care

End User ID

Default Values:default
Valid Values: The RAM End User ID/License Key received from Genesys
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The *End User ID* (License Key) allocated to the customer by Genesys Customer Care

Origin

Default Values:default
Valid Values: Valid String)
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: A descriptive region/location/data-center name of the where the Workbench is installed (i.e. EMEA, APAC, Chicago)

Read Only Options

Customer Name

Default Values:
Valid Values: Obtained automatically via Workbench to RAM communication
Changes Take Effect: After valid RAM License Activation and Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Customer Name

License Expiration Time (ms)

Default Values:0
Valid Values: Epoch Milliseconds
Changes Take Effect: Post every (20 minutes) Workbench to RAM keep-alive
Description: RAM license Expiration time in epoch milliseconds

Management Diagnostics

Editable Options

SSH Enabled

Default Values:
Valid Values: True/False
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Is Secure Access enabled/disabled

SSH Port

Default Values:8101
Valid Values: Valid free positive integer Port number
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Secure access Port number where the SSHd server is bound

Workbench Distributed Mode

Editable Options

Remote WB Primary ZooKeeper

Default Values:#REMOTE_ZK_Address Host:Port#
Valid Values: <ZK_IP:ZK_PORT>
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Is Secure Access enabled/disabled

TLS Enabled

Default Values:false
Valid Values: false/true
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Secure the Workbench IO to Workbench IO application communication

Workbench Agent Application Type

General Section

Editable Options

Workbench Application Name

Default Values: "WBA_<HOSTNAME>"
Valid Values: Any String (i.e. "WBA_MY-VM")
Changes Take Effect: Immediately
Description: The name of the Workbench Agent application

Workbench Agent Port

Default Values: **9091** (or the port number given at custom installation time)
Valid Values: A valid and free Port number (i.e. not used by other applications on the host)
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: The Port at which clients connect

Read Only Options

Workbench Application Type

Default Values: "Workbench Agent"
Valid Values: Valid Workbench Application Type
Changes Take Effect: N/A
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: The Workbench Application Version

Data-Center

Default Values: default
Valid Values: Read-Only
Changes Take Effect: Aftern Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that

will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench Agent application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: The Hostname of the host where this Workbench Agent application is running

Host IP Address

Default Values: *IP Address* of the Workbench Agent application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: The IPv4 Address of the host where this Workbench Agent application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench Agent application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: The Time-Zone of the host where this Workbench Agent application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\WorkbenchAgent"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\WorkbenchAgent")
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\WorkbenchAgent"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\WorkbenchAgent")
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: INFO
Valid Values: ALL, INFO, DEBUG, ERROR, WARNING, FATAL, TRACE, OFF
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: Application/Component Logging Level (e.g. INFO or DEBUG)

Log File Location

Default Values: "<WORKBENCH_HOME>\WorkbenchAgent\logs"
Valid Values: Valid Path (i.e. "C:\Program Files\Workbench_9.x.xxx.xx\WorkbenchAgent\logs")
Changes Take Effect: After Workbench Agent (i.e. "WB_Agent_Primary") restart
Description: Absolute path of the folder where the configuration file of this application is located

Segment (MB)

Default Values: 50
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: Maximum count of log files before rotated/cycled

MetricBeat General Section

Editable Options

Log File Location

Default Values: "<WORKBENCH_HOME>\WorkbenchAgent\logs"
Valid Values: Valid Path (i.e. "C:\Program Files\Workbench_9.x.xxx.xx\WorkbenchAgent\logs")
Changes Take Effect: After Workbench Agent (i.e. "WB_Agent_Primary") restart
Description: Absolute path of the folder where the configuration file of this application is located

Segment (MB)

Default Values: 50
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: Maximum count of log files before rotated/cycled

MetricBeat Output

Default Values: <Hostname>:<Port> of the destination Workbench Logstash application
Valid Values: Valid <Hostname>:<Port> combination
Changes Take Effect: After Workbench Agent application (i.e. "WBA_cc-app-demo-1") startup
Description: The Hostname of the host where this Workbench Agent application is running

MetricBeat Http Port

Default Values:

- For Workbench 9.0 to 9.2 - **5067** (or the port number given at custom installation time)
- For Workbench 9.3+ - **6067** (or the port number given at custom installation time)

Valid Values: A valid and free Port number (i.e. not used by other applications on the host)
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") restart
Description: The MetricBeat Port

MetricBeat Host Metrics Section

Editable Options

Disk

Default Values: true/checked
Valid Values: true/false
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: Collect and transmit [Disk] metrics from this Host

Network

Default Values: true/checked
Valid Values: true/false
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: Collect and transmit [Network] metrics from this Host

Uptime

Default Values: true/checked
Valid Values: true/false
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: Collect and transmit [Uptime] metrics from this Host

Host Metric Collection Frequency (seconds)

Default Values: 60 (seconds)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: The collect/transmit frequency for [Host] metrics from this Host

Read Only Options

CPU

Default Values: true/checked
Valid Values: true/false
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: Transmit CPU stats to Workbench

Memory

Default Values: true/checked
Valid Values: true/false
Changes Take Effect: After Workbench Agent application (i.e. "WB_Agent_Primary") startup
Description: Transmit Memory (RAM) stats to Workbench

MetricBeat Associated Application Metrics Section

Editable Options

Top / Specific

Default Values: Top 10
Valid Values: Top or Specific

Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description:

- If **Top** - collect and transmit the Top X (i.e. 10) [Application] metrics from this Host
- If **Specific** - collect and transmit certain (i.e. "sip" - based on a Regex match) [Application] metrics from this Host

Process Summary

Default Values: Enabled/True
Valid Values: Enabled/Disabled (True/False)
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: Collects high level statistics about the running processes.

Application/Process Metric Collection Frequency (seconds)

Default Values: 60 (seconds)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Agent (i.e. "WBA_cc-app-demo-1") restart
Description: The collect/transmit frequency for [Application/Process] metrics from this Host

Workbench Elasticsearch Application Type

General Section

Editable Option

Workbench Application Name

Default Values: "WB_Elasticsearch_Primary"
Valid Values: Any String name (i.e. "WB_ES_Pri")
Changes Take Effect: Immediately
Description: The name of the Workbench Elasticsearch application

Read Only Options

Workbench Application Type

Default Values: "Workbench Elasticsearch"
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The Workbench Application Version

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: <DATA_CENTER_NAME>

Valid Values: Read-Only
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that will evolve in WB 9.x

Host Name

Default Values: <HOSTNAME> of the Workbench Elasticsearch application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The Hostname of the host where this Workbench Elasticsearch application is running

Host IP Address

Default Values: <IP Address> of the Workbench Elasticsearch application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The IPv4 Address of the host where this Workbench Elasticsearch application is running

Host Time-Zone

Default Values: <Time-Zone> of the Workbench Elasticsearch application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The Time-Zone of the host where this Workbench Elasticsearch application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\ElasticSearch"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\ElasticSearch")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\ElasticSearch\config"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\ElasticSearch\config")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: INFO
Valid Values: ALL, INFO, DEBUG, ERROR, WARNING, FATAL, TRACE, OFF
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Application/Component Logging Level (e.g. INFO or DEBUG)

Log File Location

Default Values:<WORKBENCH_HOME>\\ElasticSearch\\logs
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.x.xxx.xx\\ElasticSearch\\logs")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Absolute path of the folder where the Workbench Elasticsearch application log file is located

> **Important**
>
> - Note for Windows OS the required double '\\' separator used in the Elasticsearch log file location

Segment (MB)

Default Values: 128
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire (GB)

Default Values: 2
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Maximum size of combined Elasticsearch log files before rotated/cycled

> **Important**
>
> - Note the **Expire (GB)** option is NOT a count, its the **Size** (in GB) of the **combined** Elasticsearch log files before rotated/cycled

Workbench ElasticSearch Locations

Read Only Option

Data Directory

Default Values: <WORKBENCH_HOME>\\ElasticSearch\\logs
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9_0\\ElasticSearch\\data")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: Absolute path of the folder where the Elasticsearch data is stored

Workbench ElasticSearch Identifiers

Editable Options

Cluster Name

Default Values: "GEN-WB-Cluster"
Valid Values: Any String name (i.e. "MY-WB-CLUSTER")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The name of the workbench Elasticsearch Cluster

> **Important**
>
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/cluster.name.html for more information

Node Name

Default Values:"node-<WORKBENCH_HOSTNAME>_Elasticsearch"
Valid Values: Valid String (i.e. "MY-WB-NODE1")
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: This a human readable identifier for a particular instance of Elasticsearch so it is included in the response of many APIs. It defaults to the hostname that the machine has when ElasticSearch starts but can be configured explicitly.

> **Important**
>
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/node.name.html for more information.

HTTP Port

Default Values: "9200" (or the port number provided at custom installation
Valid Values: Valid free port integer
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Port to bind to for incoming HTTP requests.

> **Warning**
>
> - Do not change the Elasticsearch Port (i.e. 9200) post Data-Center synchronization - if the default requires change, change before Data-Center Sync

> **Important**
>
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-network.html for more information.

Read Only Options

Network Host

Default Values: <HOSTNAME> of the Workbench Elasticsearch application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: The Hostname of the host where this Workbench Elasticsearch application is running.

> **Important**
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/network.host.html for more information.

Workbench ElasticSearch Discovery

Editable Options

Discovery Host(s)

Default Values: Hostname of the Workbench Elasticsearch application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: Used to provide a list of other nodes in the cluster that are master-eligible and likely to be live and contactable in order to seed the discovery process. This setting should normally contain the addresses of all the master-eligible nodes in the cluster. This setting contains either an array of hosts or a comma-delimited string. Each value should be in the form of host:port or host (where port defaults to the setting transport.profiles.default.port falling back to transport.port if not set).

> **Important**
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/discovery-settings.html for more information.

Read Only Options

Initial Master Nodes(s)

Default Values: "node-<WORKBENCH_HOSTNAME>_Elasticsearch"
Valid Values: Valid String
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") startup
Description: When you start a brand new Elasticsearch cluster for the very first time, there is a cluster bootstrapping step, which determines the set of master-eligible nodes whose votes are counted in the very first election. In development mode, with no discovery settings configured, this step is automatically performed by the nodes themselves. .

> **Important**
>
> Please see https://www.elastic.co/guide/en/elasticsearch/reference/current/discovery-settings.html for more information.

Workbench ElasticSearch Shards

Read Only Options

Number of Shards

Default Values: Populated based on the Workbench installation settings
Valid Values: Valid positive integer number
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Elasticsearch provides the ability to subdivide your index into multiple pieces called **shards**. When you create an **index**, you can simply define the number of *shards* that you want. Each *shard* is in itself a fully-functional and independent "index" that can be hosted on any node in the cluster.

> **Important**
>
> *Sharding* is important for two primary reasons:
>
> - It allows you to horizontally split/scale your content volume.
> - It allows you to distribute and parallelize operations across shards (potentially on multiple nodes) thus increasing performance/throughput.

Number of Replicas

Default Values: Populated based on the Workbench installation settings
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Elasticsearch application (i.e. "WB_Elasticsearch_Primary") restart
Description: Elasticsearch allows you to make one or more copies of your index’s shards into what are called *replica shards*, or **replicas** for short.

Important

Replication is important for two primary reasons:

- It provides high availability in case a shard/node fails. For this reason, it is important to note that a replica shard is never allocated on the same node as the original/primary shard that it was copied from.
- It allows you to scale out your search volume/throughput since searches can be executed on all replicas in parallel.

Workbench Kibana Application Type

General Section

Editable Option

Workbench Application Name

Default Values: "Workbench_Kibana_Primary"
Valid Values: Any String name (i.e. "WB_Kibana_Pri")
Changes Take Effect: Immediately
Description: The name of the Workbench Kibana application

Read Only Options

Workbench Application Type

Default Values: Workbench Kibana
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The Workbench Application Version

Associated Workbench Agent Application

Default Values: "WB_Kibana_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: default
Valid Values: Read-Only
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that

will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench Kibana application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The Hostname of the host where this Workbench Kibana application is running

Host IP Address

Default Values: *IP Address* of the Workbench Kibana application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The IPv4 Address of the host where this Workbench Kibana application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench Kibana application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The Time-Zone of the host where this Workbench Kibana application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\Kibana"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Kibana")
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\Kibana\config"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Kibana\config")
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log File Folder

Default Values: "<WORKBENCH_HOME>\Kibana\logs\kibana.log"
Valid Values: Valid folder path
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description: Absolute path of the log file location

Verbose Log

Default Values: False
Valid Values: True, False
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description: Set the value of this setting to true to log all events, including system usage information and all requests.

Silent Log

Default Values: False
Valid Values: True, False
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description: Set the value of this setting to true to suppress all logging output.

Quiet Log

Default Values: False
Valid Values: True, False
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description: Set the value of this setting to true to suppress all logging output other than error messages.

> **Important**
>
> - Only enabled 1 of the "Verbose Log", "Quiet Log" or "Silent Log" options above; else the Workbench Kibana component could fail to start.

> **Warning**

- Kibana does not provide Kibana log file rotation.
- Therefore please monitor/manage this Kibana log file accordingly to ensure it does not grow indefinitely and negatively impact the host and/or its applications

Workbench Kibana Identifiers

Editable Options

HTTP Port

Default Values:

- For WB 9.0 to 9.2 the default port is: 8181 (or the port number given at custom installation time)
- For WB 9.3 the default port is: 8182 (or the port number given at custom installation time)

Valid Values: Valid free port integer
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description:

- For WB 9.0 to 9.2 - the main UI 8181 port for incoming HTTP Chrome Browser requests.
- For WB 9.3 - changed to 8182 by default

Warning

- Restart of Workbench Kibana and Workbench Heartbeat is required when changing this option.
- The new Workbench URL would be http://<WB_Primary_Host>:<THE_NEW_HTTP_PORT>.

Workbench Elasticsearch Host

Default Values: "http://<HOSTNAME>:9200 (i.e. "http://MY-WB-VM:9200")
Valid Values: Valid Elasticsearch Hostname and Port)
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") restart
Description: IPv4 address of the host where Elasticsearch (to which Kibana is going to connect) is running

Read Only Options

Host Name

Default Values: Hostname of the Workbench Kibana application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Kibana application (i.e. "WB_Kibana_Primary") startup
Description: The Hostname of the host where this Workbench Kibana application is running.

Workbench Logstash Application Type

General Section

Editable Option

Workbench Application Name

Default Values: "WB_Logstash_Primary"
Valid Values: Any String name (i.e. "WB_Logstash_Pri")
Changes Take Effect: Immediately
Description: The name of the Workbench Logstash application

Read Only Options

Workbench Application Type

Default Values: Workbench Logstash
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Workbench Application Version

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: <DC value enter at installation
Valid Values: Read-Only
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that

will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench Logstash application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Hostname of the host where this Workbench Logstash application is running

Host IP Address

Default Values: *IP Address* of the Workbench Logstash application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench Logstash application (i.e. "WB__Primary") startup
Description: The IPv4 Address of the host where this Workbench Logstash application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench Logstash application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Time-Zone of the host where this Workbench Logstash application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\Logstash"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Logstash")
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\Logstash\config"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Logstash\config")
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: info
Valid Values: info, debug, error, warning, fatal, trace
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: Application/Component Logging Level (e.g. info or debug)

Log File Location

Default Values:<WORKBENCH_HOME>\\Logstash\\logs
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.x.xxx.xx\\Logstash\\logs")
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: Absolute path of the folder where the Workbench Logstash application log file is located

> **Important**
>
> - Note for Windows the required double '\\' separator used in the Logstash log file location

Segment (MB)

Default Values: 50 (MB)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: Maximum number of log files before being rotated/cycled

Workbench Logstash Locations

Read Only Option

Data Directory

Default Values: <WORKBENCH_HOME>\\Logstash\\data
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.x.xxx.xx\\Logstash\\data")
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: Absolute path of the folder where the Logstash data is stored

Workbench Logstash Identifiers

Editable Options

Node Name

Default Values:"node-<THE_WORKBENCH_HOSTNAME>_Logstash"
Valid Values: A valid "node-"<HOSTNAME>_<Logstash> combination
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Elasticsearch_Primary") startup
Description: This a human readable identifier for a particular instance of Logstash so it is included in the response of many APIs. It defaults to the hostname that the machine has when Logstash starts but can be configured explicitly.

HTTP Port

Default Values: "9600" (or the port number provided at custom installation
Valid Values: Valid free port integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: Logstash Port to bind to for incoming HTTP requests.

Read Only Options

Network Host

Default Values: Hostname of the Workbench Logstash application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Hostname of the host where this Workbench Logstash application is running.

Workbench Logstash Queue Settings

Editable Option

Queue Page Capacity

Default Values: "64" (MB)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The maximum size of a queue page in bytes. The queue data consists of append-only files called "pages". The default size is 64mb. Changing this value is unlikely to have performance benefits.

Queue Max Events

Default Values: "0" (Zero)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The maximum number of events that are allowed in the queue. The default is 0 (unlimited).

Queue Max Bytes

Default Values: "1024" (MB)
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The total capacity of the queue in number of bytes. The default is 1024mb (1gb). Make sure the capacity of your disk drive is greater than the value you specify here.

Metrics Pipeline

Editable Option

Event Input Port

Default Values: "5048"
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The Metrics Input Port.

Event IO Output Host

Default Values: Hostname of the Workbench Logstash application associated host (i.e. "LAB-WB-VM1")

Valid Values: Valid Hostname
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Metrics Pipeline Output Host.

Event Elastic Output Host

Default Values: http://<HOSTNAME>:9200
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Elasticsearch Host:Port.

Status Pipeline

Editable Option

Event Input Port

Default Values: "5047"
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The Status Pipeline Port.

Event IO Output Host

Default Values:

- For WB 9.0 to 9.2 - http://<HOSTNAME>:8182
- For WB 9.3 - http://<HOSTNAME>:8181

Valid Values: Valid Hostname
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") startup
Description: The Status Pipeline Output Host.

Insights Pipeline

Editable Option

Port

Default Values: "9090"
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Logstash application (i.e. "WB_Logstash_Primary") restart
Description: The Anomaly Detection "Insights" Pipeline Port.

Workbench Heartbeat Application Type

General Section

Editable Option

Workbench Application Name

Default Values: "WB_Heartbeat_Primary"
Valid Values: Any String name (i.e. "WB_Heartbeat_Pri")
Changes Take Effect: Immediately
Description: The name of the Workbench Heartbeat application

Read Only Options

Workbench Application Type

Default Values: Workbench Heartbeat
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The Workbench Application Version

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: <DC value enter at installation
Valid Values: Read-Only
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that

will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench Heartbeat application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The Hostname of the host where this Workbench Heartbeat application is running

Host IP Address

Default Values: *IP Address* of the Workbench Heartbeat application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The IPv4 Address of the host where this Workbench Heartbeat application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench Heartbeat application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The Time-Zone of the host where this Workbench Heartbeat application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\Heartbeat"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Heartbeat")
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\Heartbeat"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\Heartbeat")
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: INFO
Valid Values: INFO, DEBUG, ERROR, WARNING
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: Application/Component Logging Level (e.g. INFO or DEBUG)

Log File Location

Default Values:<WORKBENCH_HOME>\\Heartbeat\\logs
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.x.xxx.xx\\Heartbeat\\logs")
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: Absolute path of the folder where the Workbench Heartbeat application log file is located

> **Important**
>
> - Note for Windows the required double '\\' separator used in the Logstash log file location

Segment (MB)

Default Values: 50
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Logstash_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Logstash_Primary") restart
Description: Maximum number of log files before being rotated/cycled

Workbench Heartbeat Locations

Read Only Option

Data Directory

Default Values: <WORKBENCH_HOME>\\Heartbeat\\data
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.x.xxx.xx\\Heartbeat\\data")
Changes Take Effect: After Workbench Heartbeath application (i.e. "WB_Heartbeat_Primary") startup
Description: Absolute path of the folder where the Heartbeat data is stored

> **Important**
>
> - Note for Windows the required double '\\' separator used in the Logstash log file location

Workbench Heartbeat Identifiers

Editable Options

Node Name

Default Values:"node-<THE_WORKBENCH_HOSTNAME>_Heartbeat"
Valid Values: Valid String
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: This a human readable identifier for a particular instance of Heartbeat so it is included in the response of many APIs.

HTTP Port

Default Values: "<Logstash URL>:<Port>"
Valid Values: Valid host/port combination
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The Workbench Heartbeat events will be sent to this Workbench Logstash output destination for processing/storage in Workbench Elasticsearch.

Logstash Output

Default Values: "5077" (or the port number provided at custom installation
Valid Values: Valid free port integer
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: Workbench Heartbeat Port to bind to for incoming HTTP requests.

Read Only Options

Network Host

Default Values: Hostname of the Workbench Heartbeat application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") startup
Description: The Hostname of the host where this Workbench Heartbeat application is running.

Monitors

Editable Option

WB IO

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench IO component/port.

WB Agent

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Agent component/port.

WB Elasticsearch

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Elasticsearch component/port.

WB Kibana

Default Values: "10"

Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Kibana component/port.

WB Logstash

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Logstash component/port.

WB ZooKeeper

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench ZooKeeper component/port.

WB Metricbeat

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Metricbeat component/port.

WB Heartbeat

Default Values: "10"
Valid Values: Valid positive integer
Max Value: 60 seconds Changes Take Effect: After Workbench Heartbeat application (i.e. "WB_Heartbeat_Primary") restart
Description: The frequency in seconds of Workbench Heartbeat checking the health of the Workbench Heartbeat component/port.

Workbench Zookeeper Application Type

General Section

Editable Option

Workbench Application Name

Default Values: "WB_Zookeeper_Primary"
Valid Values: Any String name (i.e. "WB_ZK_Pri")
Changes Take Effect: Immediately
Description: The name of the Workbench ZooKeeper application

Read Only Options

Workbench Application Type

Default Values: Workbench ZooKeeper
Valid Values: Valid Workbench Application Type
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: Workbench Application Type

Workbench Version

Default Values: "9.x.xxx.xx"
Valid Values: WB Version
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The Workbench Application Version

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Name of associated Workbench Agent application
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The name of the Workbench Agent associated with this application/host

Data-Center

Default Values: default
Valid Values: Read-Only
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The name of the Data-Centre associated with this application; a prepatory setting that

will evolve in WB 9.x

Host Name

Default Values: *Hostname* of the Workbench ZooKeeper application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The Hostname of the host where this Workbench ZooKeeper application is running

Host IP Address

Default Values: *IP Address* of the Workbench ZooKeeper application associated host (i.e. "10.20.30.40")
Valid Values: Valid IP address
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The IPv4 Address of the host where this Workbench ZooKeeper application is running

Host Time-Zone

Default Values: *Time-Zone* of the Workbench ZooKeeper application associated host (i.e. "Europe/London")
Valid Values: Valid Host Time-Zone
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The Time-Zone of the host where this Workbench ZooKeeper application is running

Deployment Section

Read Only Options

Installation Directory

Default Values: "<WORKBENCH_HOME>\ZooKeeper"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\ZooKeeper")
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: Absolute path of the folder where this application is installed

Configuration Directory

Default Values: "<WORKBENCH_HOME>\ZooKeeper\conf"
Valid Values: Valid Path (i.e. C:\Program Files\Workbench_9.x.xxx.xx\ZooKeeper\conf")
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: Absolute path of the folder where the configuration file of this application is located

Logging Section

Editable Options

Log Level

Default Values: INFO
Valid Values: INFO, ERROR, DEBUG, TRACE, OFF
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_Elasticsearch_Primary") restart
Description: Application/Component Logging Level (e.g. INFO or DEBUG)

Log File Location

Default Values:<WORKBENCH_HOME>\\ZooKeeper\\logs
Valid Values: Valid Path (i.e. "C:\\Program Files\\Workbench_9.1.0000.00\\ZooKeeper\\logs")
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_Elasticsearch_Primary") restart
Description: Absolute path of the folder where the Workbench ZooKeeper application log file is located

Segment (MB)

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Maximum size of the log file before it is rotated/cycled

Expire

Default Values: 10
Valid Values: Valid positive integer
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Maximum count of log files before rotated/cycled

Cluster Configuration Section

Editable Options

Unique ID

Default Values: 1
Valid Values: Read-Only integer
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup

Description: Unique ID for the ZooKeeper instance running on this host

Node 1

Default Values: null
Valid Values: <Valid IP Address:Valid Port number>
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Unique ID for the ZooKeeper instance designated as Node 1

Node 2

Default Values: null
Valid Values: <Valid IP Address:Valid Port number>
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Unique ID for the ZooKeeper instance designated as Node 2

Node 3

Default Values: null
Valid Values: <Valid IP Address:Valid Port number>
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Unique ID for the ZooKeeper instance designated as Node 3

Node 4

Default Values: null
Valid Values: <Valid IP Address:Valid Port number>
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Unique ID for the ZooKeeper instance designated as Node 4

Node 5

Default Values: null
Valid Values: <Valid IP Address:Valid Port number>
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: Unique ID for the ZooKeeper instance designated as Node 5

Workbench Zookeeper

Read Only Option

Workbench Zookeeper Hostname

Default Values: *Hostname* of the Workbench ZooKeeper application associated host (i.e. "LAB-WB-VM1")
Valid Values: Valid Hostname (i.e. "LAB-WB-VM1")

Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") startup
Description: The Hostname of the host where this Workbench ZooKeeper application is running

Editable Option

Workbench ZooKeeper Port

Default Values: "2181" (or value provided at custom installation)
Valid Values: Valid free positive Port integer
Changes Take Effect: After Workbench ZooKeeper application (i.e. "WB_ZooKeeper_Primary") restart
Description: The IPv4 Address of the host where this Workbench ZooKeeper application is running

> **Warning**
>
> - Do not change the ZooKeeper Port (i.e. 2181) post Data-Center synchronization - if the default requires change, change before Data-Center Sync

Workbench Host Object Type

General Section

Read Only Options

Host Name

Default Values: Hostname of the host/server
Valid Values: Valid Hostname (i.e. "LAB-WB-VM1")
Changes Take Effect: After Workbench startup
Description: Name of the host

Host IP Address

Default Values: IP Address of the host
Valid Values: Valid IP Address (i.e. 10.20.30.40)
Changes Take Effect: After Workbench startup
Description: The IPv4 Address of the host

OS

Default Values: The Operating System type of the host
Valid Values: Windows 2012 or Windows 2016
Changes Take Effect: After Workbench startup
Description: Name of the Operating System running on the host

Host Time-Zone

Default Values: The Time-Zone of the host
Valid Values: Valid Time-Zone (i.e. Australia/Brisbane)
Changes Take Effect: After Workbench startup
Description: The Time-Zone of the host based on regional location

Associated Workbench Agent Application

Default Values: "WB_Agent_Primary"
Valid Values: Any String name (Eg: WBAgentService)
Changes Take Effect: After Workbench startup
Description: Name of the Workbench Agent application running on the host

Data-Center

Default Values: default
Valid Values: Read-Only
Changes Take Effect: After Workbench startup
Description: The name of the Data-Center associated with this host/node

Associated Applications

Default Values:
WB_Zookeeper_Primary,WB_Agent_Primary,WB_IO_Primary,WB_Kibana_Primary,WB_Elasticsearch_Primary
Valid Values: Workbench application names
Changes Take Effect: After Workbench startup
Description: List of Workbench applications installed on this host

Workbench TLS Communication

Editable Options

Keystore Path

Default Values: Blank
Valid Values: Valid Path to Keystore
Changes Take Effect: After Workbench startup
Description: The path to the TLS Keystore

Keystore Password

Default Values: Blank
Valid Values: Truststore Password
Changes Take Effect: After Workbench startup
Description: The TLS Truststore Password

Truststore Path

Default Values: Blank
Valid Values: Valid Path to Keystore
Changes Take Effect: After Workbench startup
Description: The path to the TLS Keystore

Truststore Password

Default Values: Blank
Valid Values: Truststore Password
Changes Take Effect: After Workbench startup
Description: The TLS Truststore Password

Protocol

Default Values: TLSv1.2
Valid Values: Valid TLSv1.2
Changes Take Effect: After Workbench startup
Description: The supported TLS Protocol Versions

Algorithms

Default Values: TLS_RSA_WITH_AES_128_CBC_SHA
Valid Values: TLS_RSA_WITH_AES_128_CBC_SHA
Changes Take Effect: After Workbench startup
Description: Supported Algorithms

Mutual TLS

Default Values: False
Valid Values: False/True
Changes Take Effect: After Workbench startup
Description: Is Mutual TLS Enabled?

Workbench General Settings

Alarm Expiration

Editable Options

Alarm Expiration Enabled

Default Values: True
Valid Values: True/False
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Is the automatic closure of Workbench Active Alarms post the Alarm Expiration value Enabled/Disabled

Alarm Expiration (Seconds)

Default Values: 172800
Valid Values: 3600 to 31536000 seconds
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: The number of seconds when the Workbench Active Alarms will be closed automatically if Alarm Expiration is Enabled

Retention Period

Editable Options

Workbench Data Retention Period Enabled

Default Values: True
Valid Values: True/False
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Is the purging of Workbench data Enabled/Disabled

Workbench Data Retention Period (Days)

Default Values: 30
Valid Values: 30 to 365 Days
Changes Take Effect: After Workbench IO application (i.e. "WB_IO_Primary") restart
Description: Workbench data will be purged post the Workbench Data Retention Period

Session Expiration

Editable Options

Enabled

Default Values: True
Valid Values: True/False
Changes Take Effect: Immediately
Description: Is Session Expiration Enabled/Disabled

Session Expiration

Default Values: 30
Valid Values: 900 to 31536000 seconds
Changes Take Effect: Immediately
Description: This applies to the **Idle** timeout of sessions, if Enabled=True above, Users will be automatically logged out of Workbench if/when a new request is greater than the Session Expiration value; Users will never be auto logged out if Enabled=False above.

Additional Information

This section provides additional information for users and administrators that are deploying, configuring and using Workbench.

- FAQ’s
- Known Issues and Limitations
- Migration
- Best Practices
- Troubleshooting
- GDPR
- Release Notes
- Related Documentation

FAQ's

This section provides a useful list of Workbench 9 Frequently Asked Question’s (FAQ’s):

Workbench Host/Server Operating System Support

- Which Operating Systems are supported by Workbench 9?
  - Answer: Windows 2012 and 2016 - RHEL 7 - CentOS 7

Browser Support

- Which Internet Browsers are supported by Workbench 9.x?
  - Answer: Chrome; the latest stable release

Genesys Platform Integration

- Which Genesys platforms does Workbench currently support integration with?
  - Answer: Genesys Engage On-Premise.
- Is Workbench a managed/Cloud service?
  - Answer: No - Workbench 9.x is On-Premise ONLY and integrates to the customers Genesys Engage On-Premise platform.
- Which versions of Genesys Engage are supported by Workbench?
  - Answer: Workbench integrates to Configuration Server (CS), Solution Control Server (SCS) and Message Server (MS) 8.x
- Does Workbench display Genesys Engage Alarms?
  - Answer: Yes, via the dedicated Workbench Alarms Console. Genesys Engage Alarms are ingested via the Workbench IO application and the integration to the Genesys Engage Solution Control Server(s) (SCS) component(s)
- Does Workbench display Genesys Engage Configuration Changes?
  - Answer: Yes, via the dedicated Workbench Changes console. Genesys Engage Configuration Changes are ingested via the Workbench_IO application and the integration to the Genesys Engage Configuration Server(s) component(s)
- Which Genesys Engage Configuration Changes are displayed by Workbench?
  - Answer: Genesys Engage *Application, Host and Solution* Object configuration changes only; (i.e. not

URS Strategy changes or Agent Skill changes).

- Workbench Channel Monitoring integrates to the Genesys SIP Server?
  - Answer: Yes; Workbench Channel Monitoring integrates directly to the Genesys SIP Server and not the SIP Server Proxy

Workbench Deployment

- Does Genesys recommend a lab/test deployment before production?
  - Answer: Yes - please determine if Workbench 9.x and its features/limitations are useful for production use before considering a production deployment
- Does Workbench 9 need its own dedicated host infrastructure?
  - Answer: Yes; please review the documentation *Planning and Deployment* section
- Is the Workbench Agent application required on the Workbench hosts?
  - Answer: Yes
- Should Workbench at ALL Data-Centers be running the same version?
  - Answer: Yes; releases of Workbench on ALL Nodes and at ALL Data-Centers should be the same version
- Is Workbench Kibana installed on ALL Workbench Nodes/Hosts?
  - Answer: No - Workbench Kibana is only installed on the Workbench Primary Node

Workbench Agent Remote

- Which components need to be installed on remote hosts such as the SIP, URS, and GVP hosts?
  - Answer: Workbench Agent Remote (WAR); this is required for metric (CPU/RAM/DISK/NET) data ingestion
    - WAR deployment is optional - if you don not want to view Metric data from remote hosts then don't install WAR
- What is the maximum number of remote WAR hosts supported by Workbench 9.1.x
  - Answer: Currently Workbench **9.x is limited to a maximum of 100 Hosts** (the global combined Workbench or Engage Hosts), due to delays in loading the Configuration Host and Application objects/details; this limitation will be addressed in a future release of Workbench.
- When are the Workbench Agent Remote (WAR) components upgraded?
  - Answer: The respective Workbench Agent Remote (WAR) components, installed on hosts such as SIP, URS, GVP etc, will be upgraded based on the WAR **Upgrade Time** (default 02:00)
- What are the impacts when upgrading to Workbench 9.3:
  - Answer: For WB 9.3 the WAR [General] **Log File Location**, **Segment** and **Expire** fields will be blank

post an upgrade until the WAR **Upgrade Time** (default=02:00) is triggered and the WAR upgrade is completed

Workbench Data-Centers

- What is a Workbench Data-Center?
- Answer: Workbench Data-Centers is a logical concept to categorize and optimize the respective Workbench Hosts, Applications and ingested data for event distribution, visualization context and filtering purposes
  - Each Workbench host, and the respective applications within that host, are assigned to a Data-Center, this is mandatory
  - Note: The Data-Center name is case-sensitive, limited to a maximum of 10, Alphanumeric and underscore characters only.
- Is there any post impacts when renaming a Workbench Data-Center
  - Yes - please review Section: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/DC_Sync_Config and the Warning sections at the bottom of the page
- Is there any post impacts when forming a Workbench Data-Center
  - Yes - please review Section: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/DC_Sync_Config and the Warning sections at the bottom of the page

Workbench Cluster

- How many nodes does Workbench support for cluster formation?
  - Answer: Workbench supports odd number of nodes (1,3,5) for cluster formation.
- Does Workbench support scaling?
  - Answer: No. Once all nodes are installed form a Zookeeper and Elasticsearch cluster. Current version of Workbench does not support scaling
- What components need to be up and running to initiate Workbench Data-Center syncing?
  - Answer: Agent, Elasticsearch, Zookeeper and Workbench IO needs to be up and running in all associated Data-Centers
- What values are allowed for cluster formation?
  - Answer: Workbench Cluster supports Hostname, IP Address or a combination of both; it does not support Fully Qualified Domain Name.

Workbench Infrastructure/Footprint

- How many hosts/VM’s are required for the Workbench solution?
  - Answer: This depends on the customer environment and requirements; please review the documentation *Planning and Deployment* section.

Workbench Authentication

- How do users log into Workbench?
  - Answer: In Workbench 9, the login/authentication is provided by the Genesys Engage Configuration Server integration.
- Does Workbench have a ‘Role’ concept?
  - Answer: Yes, Workbench has a basic ‘Role’ concept whereby if the associated Genesys Engage ‘User’ has ‘Admin’ access the Workbench Configuration will be visible; ‘Normal’ Users do not have access to Workbench Configuration.

Workbench Alarms and Changes

- Does Workbench display Alarms and Changes relating to the Workbench solution itself?
  - Answer: Yes; Workbench related Alarms and Changes are also displayed in the dedicated Alarms and Changes consoles.
- Which Engage CME Objects are monitored for Configuration Changes?
  - Answer: Currently only Engage CME Host, Application and Solution object changes are tracked/ presented
- What is required to accurately populate the Changes Console **ChangedBy** field for Genesys Engage configuration changes?
  - Answer: A connection from the respective Genesys Engage Configuration Server or Configuration Server Proxy to the Genesys Engage Message Server that Workbench is connected to; in addition, **standard=network** added to the **log** section of the Configuration Server or Configuration Server Proxy that Workbench is connected to.

Dashboards and Visualizations

- Does Workbench ship with example Dashboards and Visualizations/Widgets?
  - Answer: Yes. Genesys example Dashboards and Visualizations are provided. Please review section ?.? for further details.
- Does Workbench ingest metric and log data from the Genesys Application Servers, e.g. SIP, URS, GVP etc., ?

    - Answer: Workbench 9.1 can ingest metric data from Genesys Application Servers e.g. SIP, URS, GVP etc.
    - Log data ingestion is not yet supported; timescale TBD.
- Does Workbench monitor Engage Client application types
    - Answer: No, Workbench only monitors *Server* Type applications and not *Client* applications; therefore the Total/Up/Down/Unknown *counts* may be different from GAX and GA

Workbench Data Retention

- How/when is data purged/deleted from Workbench?
    - Answer: The “Retention Period” option in the “General” section of Workbench Configuration controls if/when data is deleted from Workbench, please the documentation accordingly.

Workbench and the Remote Alarm Monitoring (RAM) Service

- Does Workbench 9.x support the RAM Service?
    - Answer: Yes; please review the RAM sections of the documentation.

Workbench Ports

- Which Ports are used by Workbench?
    - Answer:
        - For WB 9.0 to 9.2:
            - **8181** (Kibana - the main UI port for Workbench 9.0 to 9.2)
            - **8182** (Workbench IO)
            - **5556** and **2553** (Workbench IO)
            - **9091** (Workbench Agent & Workbench Agent Remote)
            - **9200** (Elasticsearch)
            - **9600** (Logstash)
            - **5066** (Heartbeat)
            - **2181** (ZooKeeper default)
            - **2888** and **3888** (ZooKeeper Cluster)
            - **5067** for the **optional** Workbench Agent Remote (WAR)/Metricbeat component

        - that is installed on the Genesys Application Servers (i.e. SIP, URS, FWK)
        - which sends Metric data (CPU/RAM/DISK/NET) to the Workbench instance/cluster
        - for the observability of host and process CPU, Memory, Disk and Network metric data
        - providing rich insights and analysis capability into host and process metric utilization, performance and trends.
    - For WB 9.3+:
        - **8181** (Workbench IO - the main UI port for Workbench)
        - **8182** (Kibana - - not accessible in WB 9.3+)
        - **5556** and **2553** (Workbench IO)
        - **9091** (Workbench Agent & Workbench Agent Remote)
        - **9200** (Elasticsearch)
        - **9600** (Logstash)
        - **5066** (Heartbeat)
        - **2181** (ZooKeeper default)
        - **2888** and **3888** (ZooKeeper Cluster)
        - **6067** (WB 9.3+) for the **optional** Workbench Agent Remote (WAR)/Metricbeat component
            - that is installed on the Genesys Application Servers (i.e. SIP, URS, FWK)
            - which sends Metric data (CPU/RAM/DISK/NET) to the Workbench instance/cluster
            - for the observability of host and process CPU, Memory, Disk and Network metric data
            - providing rich insights and analysis capability into host and process metric utilization, performance and trends.
- Do not use Ports below 1024 for Workbench components as these ports are typically used for system services

Warning

- Workbench Agent 9.0 to 9.2 uses Port 5067 - this unfortunately clashes with GVP
    - if/when your Genesys deployment contains GVP using port 5067, please change the Workbench Agent(s) Port - i.e. to 6067
        - restart the Workbench Agent(s) and Workbench Logstash(s) components.
- Workbench Agent 9.3+ uses Port 6067

Workbench Linux Services

- What Linux Services does Workbench create?
  - **WB_Elasticsearch_9.x.xxx.xx** - example usage: service WB_Elasticsearch_9.0.100.00 start|stop|staus
  - **WB_ZooKeeper_9.x.xxx.xx** - example usage service WB_ZooKeeper_9.0.100.0 start|stop|status
  - **WB_Kibana_9.x.xxx.xx** - example usage service WB_Kibana_9.0.100.00 start|stop|status
  - **WB_Agent_9.x.xxx.xx** - example usage service WB_Agent_9.0.100.00 start|stop|status
  - **WB_IO_9.x.xxx.xx** - example usage service WB_IO_9.0.100.00 start|stop|status

Elastic Stack Version

- Which version of the Elastic stack does Workbench use?
  - Answer: Version 7.17

LFMT Integration

- Does Workbench 9.x integrate to LFMT?
  - Answer: **No**; the roadmap of Workbench 9.x is to ingest both metric and log data directly and provide enhanced event visibility and insights to improve the operational management of Genesys platforms.

Migration/Upgrade

- Is there a Workbench 8.5 to Workbench 9.0 migration path?
  - Answer: **No**, unfortunately not given Workbench 9.0 has been reinvented with a new back-end and front-end design.

> ### Warning
>
> - **Before commencing the Workbench 9.x upgrade - please ensure the Workbench Host(s) have 'free' at least 3 times the size of the "<WORKBENCH_INSTALL>/ElasticSearch/data" directory - else the Workbench upgrade process will fail and data integrity will likely be compromised.**

- What is the Workbench 9.x to Workbench 9.x migration path?
  - Answer: Workbench supports an N-1 migration path - i.e. to upgrade to 9.2.000.00 you must be on the previous release of Workbench 9.1.100.00
  - The same N-1 logic applies for ALL releases of Workbench
- Should Workbench at ALL Data-Centers be running the same version?
  - Answer: Yes; releases of Workbench on ALL Nodes and at ALL Data-Centers should be the same
- Workbench 9.2 to 9.3 upgrade and Dashboards/Visualizations
  - During the upgrade to 9.3, Workbench component statuses may be inaccurate until all Workbench Cluster Nodes are fully upgraded/completed
  - The Workbench Primary Services should be up/running before commencing any Workbench 9.3 Node2, Node3, NodeN upgrades
  - For Workbench 9.2 to 9.3 upgrades, existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
  - The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
  - As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/message will be displayed
  - Even though the migrated "_9.2" Dashboards/Visualizations are not functional and display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations
  - The migrated and suffixed "_9.2" Visualizations cannot be deleted; this limitation will be addressed in a future Workbench 9.x release

Auditing

- Does Workbench have an Auditing capability?
  - Answer: **Yes**, please review the Using Workbench/Workbench Configuration section of the documentation.

GDPR

- How does Workbench accommodate the GDPR policy?
  - Answer: Please review the Additional Information/GDPR section of the documentation.

Licenses

- Does Workbench need a license?
  - Answer: A Workbench license is only needed if the Workbench Remote Alarm Monitoring Service offering is adopted.

TLS

- Workbench and TLS support?
  - Answers:
  - TLS connections to Workbench IO and Kibana (essentially the main Workbench UI) is currently NOT supported
  - TLS connections from Workbench IO Applications at different Data-Centers is supported (i.e. Workbench IO at APAC and Workbench IO at EMEA)
  - TLS connections to Elasticsearch has to be enabled when enabling Elasticsearch Authentication; therefore is supported intrinsically when Elasticsearch Auth is enabled
  - TLS connections to ZooKeeper is NOT supported
  - TLS connection from Workbench to Engage Configuration Server is supported
  - TLS connection from Workbench to Engage Solution Control Server is supported
  - TLS connection from Workbench to Engage Message Server is supported

Best Practices

The following *Best Practises* are recommended by Genesys:

Warning

- Please review the *Planning and Deployment* section of this document before commencing Workbench installation
- Do not change the Elasticsearch Port (i.e. 9200) post Data-Center synchronization - if the default requires change, change before Data-Center Sync
- Do not change the ZooKeeper Port (i.e. 2181) post Data-Center synchronization - if the default requires change, change before Data-Center Sync
- Kibana does not provide Kibana log file rotation.
- Therefore please monitor/manage this Kibana log file accordingly to ensure it does not grow indefinitely and negatively impact the host and/or its applications
- If your Engage Configuration Servers are configured for HA, please ensure the respective CME Host Objects have the IP Address field configured, else Workbench will fail to install.

- Ensure the network ports utilized by Workbench are free and open from a firewall perspective.
- When starting/re-starting Workbench Elasticsearch, ensure the Primary is started before the Elasticsearch 2nd and 3rd Nodes
  - Pause approx. 3-4 minutes between each Elasticsearch Node start
- Suggestion to ensure Genesys application server (i.e. SIP/URS, GVP etc) network traffic has a higher priority than Workbench network traffic
- Suggestion to set a low quality of service (QoS) value for Workbench network traffic

Troubleshooting

This section details Workbench troubleshooting, including:

- Installation
- Ports
- Logs
- Upgrades
- Dashboards
- Services
- Changes Console
- Miscellaneous

Installation

Administrator/Sudo Permissions

> **Important**
>
> - Ensure Workbench is installed with Administrator (Windows) or Sudo (Linux) permissions
>   - i.e. for Windows open a Command/Powershell Console As Administrator and run install.bat.
>   - i.e. for Linux open a Terminal run ./install.sh with a user that has sudo permissions - do not prefix ./install.sh with sudo

CME Templates

> **Important**
>
> - Ensure **each** and **every** Engage CME Application has an assigned **Template** else the Workbench installation will fail.

CME Host IP Addresses

> **Important**
>
> - Ensure Engage CME Hosts Objects have an IP address assigned else the Workbench installation will fail.

Ports

Workbench components use the network ports below, from a firewall perspective, please review, edit and ensure not already in use.

> ## Warning
>
> - Double-check, the network ports, that are used by Workbench, are from a firewall perspective, **open and not already in use** by other applications

Logs

When opening a Genesys Customer Care Workbench support Case, it is useful to include Workbench log files to enable efficient troubleshooting.

Workbench produces log files for several Workbench components, the sections below detail log files to include in support Cases:

Workbench Logs

All logs from "<WORKBENCH_HOME_INSTALL_FOLDER>\karaf\data\log" covering issue occurence

Workbench Kibana Logs

All logs from "<WORKBENCH_HOME_INSTALL_FOLDER>\Kibana\logs" covering issue occurrence (ideally Verbose Log Level)

Client Browser Logs

Ideally Client Browser logs covering issue occurrence

The Chrome Dev-Tools may be useful: https://developers.google.com/web/tools/chrome-devtools

Workbench Log Locations

The list below details the default log file locations of the Workbench components:

- WB IO (Karaf) - <WORKBENCH_INSTALL_DIRECTORY>/Karaf/data/log
  - this component integrates Workbench to Engage Configuration Server, Solution Control Server, Message Server - also responsible for the Channel Monitoring functionality
- WorkbenchAgent (installed on the Workbench Hosts) - <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/logs
  - this component is responsible for Status, Installation and Metric data (i.e. cpu, ram, disk, network) ingestion
- Elasticsearch - <WORKBENCH_INSTALL_DIRECTORY>/Elasticsearch/logs
  - this component is responsible for storing the Workbench data - i.e. Alarms, Changes, Channel Monitoring, Metrics etc
- ZooKeeper - <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/logs

    - this component is responsible for Workbench configuration data
- Kibana - <WORKBENCH_INSTALL_DIRECTORY>/Kibana/logs
    - this component is responsible for Workbench UI
- Logstash - <WORKBENCH_INSTALL_DIRECTORY>/Logstash/logs
    - this component is responsible for the Metric data and Anomaly Detection ingestion pipeline
- Heartbeat - <WORKBENCH_INSTALL_DIRECTORY>/Heartbeat/logs
    - this component is responsible for Workbench component Statuses (i.e. up/down)
- Metricbeat - <WORKBENCH_INSTALL_DIRECTORY>/Metricbeat/logs
    - this component is responsible for Workbench Metric data (i.e. cpu, ram, disk, network) ingestion

- WorkbenchAgent Remote (installed on remote hosts such as sip, urs, gvp etc) - <WORKBENCH_AGENT_REMOTE_INSTALL_DIRECTORY>/logs
    - this component is responsible for Workbench Metric data (i.e. cpu, ram, disk, network) ingestion

Upgrade

Single Node deployment, or Primary node deployment in cluster, upgrade failed

1. To enable troubleshooting, backup logs for Workbench 9.0.1:

- WBAgent logs: C:\Program Files\Workbench_9.0.100.00\WorkbenchAgent\logs
- ElasticSearch logs: C:\Program Files\Workbench_9.0.100.00\ElasticSearch\logs
- Zookeeper logs: C:\Program Files\Workbench_9.0.100.00\ZooKeeper\logs

2. Extract the downloaded **Workbench_9.0.100 .00_Pkg.zip** compressed zip file.

- Browse to Workbench installation folder (C:\Program Files\Workbench_9.0.100.00) and locate file **uninstall.bat**
- Execute **uninstall.bat** file as administrator
- After the uninstall in complete, delete any traces of sub-folder or files in the Workbench_9.0.100.00 or installation folder.

3. After successful uninstall, reinstall Workbench 9.0.1.

Cluster deployment, upgrade failed

If there was a successful upgrade on the primary node but an unsuccessful upgrade in an additional node:

1. To enable troubleshooting, backup logs for Workbench 9.0.1:

- WBAgent logs: C:\Program Files\Workbench_9.0.100.00\WorkbenchAgent\logs
- ElasticSearch logs: C:\Program Files\Workbench_9.0.100.00\ElasticSearch\logs
- Zookeeper logs: C:\Program Files\Workbench_9.0.100.00\ZooKeeper\logs

2. Uninstall Workbench 9.0.1.

- Browse to Workbench installation folder (C:\Program Files\Workbench_9.0.100.00) and locate file **uninstall.bat**
- Execute **uninstall.bat** file as administrator
- After uninstall also delete traces of folder

3. After successful uninstall, reinstall Workbench 9.0.1.

Important

1. Run these steps only on the additional node where the upgrade failed.
2. At the end of an upgrade, all primary and additional nodes should be at same version (Workbench_9.0.100.00).

Dashboards

Workbench 9.3 Dashboard/Visualization error:TOKEN_INVALID, please check web console for details

- If/when the session expires, and a custom Dashboard/Visualization is open, the user may be presented with a "error:TOKEN_INVALID, please check web console for details" error
- If/when this error is presented, please logout/login

Workbench 9.3 Dashboard/Visualization error, please check web console for details

- Typically shown if the Workbench Host(s) are not name resolvable from the client machine; ensure Workbench Host(s) are DNS resolvable

Services

Workbench Services

Workbench should only be Stopped/Started using the respective Workbench Services that are added during installation.

If the Workbench Services are not visible please ensure the Workbench installation was performed as an Administrator (Windows) or with sudo (Linux) permissions.

Changes Console

Changes Console 'ChangedBy' shows User = "N/A"

- For the Changes Console **ChangedBy** field to be accurate (not "N/A"), the following Genesys Engage configuration is required:
  - A connection from the respective Genesys Engage Configuration Server or Configuration Server Proxy to the Genesys Engage Message Server that Workbench is connected to
  - If not already, **standard=network** added to the **log** section of the Configuration Server or Configuration Server Proxy that Workbench is connected to

Important

- The Workbench "WB_IO_Primary" Service will need to be restarted if/when Workbench loses connection to the Message Server and the connection is not re-established within 2 minutes
  - Confirmation that Workbench cannot connect to Message Server can be validated by reviewing the:
    - "<WORKBENCH_INSTALL_DIRECTORY>/Karaf/data/log/PE_ChangesInterface.log" file and searching for:
    - "Unable to create a connection to both Primary and Backup Message Server" - if present, to resolve, restart the "WB_IO_Primary" Service

Miscellaneous

Client Browser URL is big and Kibana might stop working

- For Workbench 9.0 to 9.2:
  - If a **The URL is big and Kibana might stop working** error message is encountered, Genesys recommends:
  - Login into Workbench
  - Open a new Browser tab
  - Navigate to http://<WB_HOST>:8181/app/kibana#/management/kibana/settings/
  - Scroll down to **Store URL's in session storage** and set **state:storeInSessionStorage** to **ON**

Temp Directory

For the Elastic stack components, Elasticsearch and Logstash are the main Workbench components that write to the node/host system Temp directory; these Temp directory locations can be changed via the respective local config files.

For the Logstash component please change the following file:

- {WB_Install_Home_Location}\Logstash\config\jvm.options
- Within the **jvm.options** file, uncomment (remove the “#”) from the start of “-Djava.io.tmpdir=$HOME”
- Replace “$HOME” with the directory location that you would like to use for Temp.
- After saving the file, restart the Windows WB_Logstash_9.1.x Service for the changes to take effect.

For Elasticsearch, change the Temp directory by setting the following environment variable:

- "ES_TMPDIR".
- After setting that environment variable, please restart the WB_Elasticsearch_9.1.x Service for the changes to take effect.

Known Issues and Limitations

Details of Workbench 9 **Known Issues and Limitations** can also be found on the Genesys Customer Care Portal via Release Notes

CVE-2022-22965 vulnerability

- Workbench 9.x is deemed to be not impacted by the CVE-2022-22965 vulnerability.

Workbench 9.0.x to 9.2.000.00 mitigations for the log4j 2.x CVE-2021-44228 vulnerability

> **Important**
>
> - The Workbench 9.2.000.20 release (5th Jan 2022) provides the mitigations below already pre-configured

This page relates to the Genesys Advisory detailed here: https://genesyspartner.force.com/customercare/kA91T000000bltb

Please follow the mitigation steps below in addition to the guidance in the Genesys Advisory above.

Workbench 9.x.xxx.xx (i.e. all WB versions) and Anomaly Detection (AD) 9.2.000.00

- First stop ALL Workbench Services

Workbench IO (Karaf)

Step 1

Remove (i.e. with a shell command or with a tool such as 7Zip) the JndiLookup class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/Karaf/system/org/ops4j/pax/logging/pax-logging-log4j2/1.11.4/ pax-logging-log4j2-* org/apache/logging/log4j/core/lookup/JndiLookup.class**

Step 2

- With the Workbench IO Service stopped, locate the file **<WORKBENCH_INSTALL_DIRECTORY>\Karaf\etc\org.apache.karaf.features.cfg**
- Edit the file:

1. Look for the property **featuresBoot** and uncomment it by removing “#” in the front
2. In addition, uncomment the following lines associated with this property by removing “#” in the front (about 25-30 lines)
3. Save the file changes

- Locate the folder **<WORKBENCH_INSTALL_DIRECTORY>\Karaf\data\cache** and remove all the folders and files in it (generally of the form “bundle<n>” where n is a sequential number).

Workbench ZooKeeper

Remove (i.e. with a shell command or with a tool such as 7Zip) the JndiLookup class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/build/lib/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class**

Workbench Logstash

Remove (i.e. with a shell command or with a tool such as 7Zip) the JndiLookup class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/Logstash/logstash-core/lib/jars/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class**

Workbench Elasticsearch

Remove (i.e. with a shell command or with a tool such as 7Zip) the JndiLookup class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ElasticSearch/lib/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class**

Workbench Agent 9.x

> **Important**
>
> - Perform the Workbench Agent 9.x changes below on ALL Workbench Hosts and ALL Anomaly Detection (AD) Hosts (if AD is installed)

Remove (i.e. with a shell command or with a tool such as 7Zip) the JndiLookup class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/lib/log4j-core-2.* org/apache/logging/log4j/core/lookup/JndiLookup.class**

Workbench Kibana

Not impacted - no changes required.

Workbench Heartbeat

Not impacted - no changes required.

Workbench Metricbeat

Not impacted - no changes required.

Workbench Agent Remote (WAR)

Not impacted - no changes required.

- Finally once the above changes are completed, start ALL Workbench Services

Workbench 9.0.x to 9.2.000.00 mitigations for the log4j 1.2 CVE-2021-4104 and CVE-2019-17571 vulnerabilities

> **Important**
>
> - The Workbench 9.2.000.20 release (5th Jan 2022) provides the mitigations below already pre-configured

Workbench 9.2.000.00

Workbench ZooKeeper

Remove (i.e. with a shell command or with a tool such as 7Zip) the JMSAppender class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**

Remove (i.e. with a shell command or with a tool such as 7Zip) the SocketServer class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**

Workbench 9.1.100.00

Workbench ZooKeeper

Remove (i.e. with a shell command or with a tool such as 7Zip) the JMSAppender class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**

Remove (i.e. with a shell command or with a tool such as 7Zip) the SocketServer class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**

Workbench Agent

Remove (i.e. with a shell command or with a tool such as 7Zip) the JMSAppender class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**

Remove (i.e. with a shell command or with a tool such as 7Zip) the SocketServer class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**

Workbench 9.1.000.00 and 9.0.x

Workbench ZooKeeper

Remove (i.e. with a shell command or with a tool such as 7Zip) the JMSAppender class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**
- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**

Remove (i.e. with a shell command or with a tool such as 7Zip) the SocketServer class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/contrib/rest/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**
- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/ZooKeeper/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**

Workbench Agent

Remove (i.e. with a shell command or with a tool such as 7Zip) the JMSAppender class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/lib/log4j-1.2* org/apache/log4j/net/JMSAppender.class**

Remove (i.e. with a shell command or with a tool such as 7Zip) the SocketServer class from the classpath - by executing the command:

- **zip -q -d <WORKBENCH_INSTALL_DIRECTORY>/WorkbenchAgent/lib/log4j-1.2* org/apache/log4j/net/SocketServer.class**

Workbench 9.0.x to 9.2.000.00 mitigations for the log4j 2.x CVE-2021-45105 vulnerability

> **Important**
>
> - The Workbench 9.2.000.20 release (5th Jan 2022) provides the mitigations below already pre-configured

Following changes are required to remove the Context Lookup from Workbench IO (Karaf) for Workbench builds prior to 9.2.000.10:

- Stop the Workbench IO (Karaf) Service(s)
- In the file <WORKBENCH_INSTALLATION_FOLDER>/Karaf/etc/ org.ops4j.pax.logging.cfg
- Comment out 17 lines after the line “# Sift – MDC routing” by inserting “#” at the beginning of the line.
- Change 16MB to 128MB in the line “log4j2.appender.rolling.policies.size.size = 16MB”
- Start the Workbench IO (Karaf) Service(s)

The effect of the above change is that we no longer have one log file per running bundle but have only one karaf.log that is rolled over as soon as it reached 128 MB in size.

Workbench 8.5 migration to Workbench 9.x

> **Warning**
> There is no migration plan/process from Workbench 8.5 to Workbench 9.x, its a fresh install.

GDPR

> **Important**
>
> Workbench 9 currently does **NOT** support GDPR access or erasure requests for data that is stored for an extended period.

> **Important**
>
> To meet EU GDPR (European Union General Data Protection Regulation) compliance, customers/partners should ensure that the Workbench "**Retention Period**" option within the Configuration/General section is set to **30 days or less** (if adherence to EU GDPR is required).

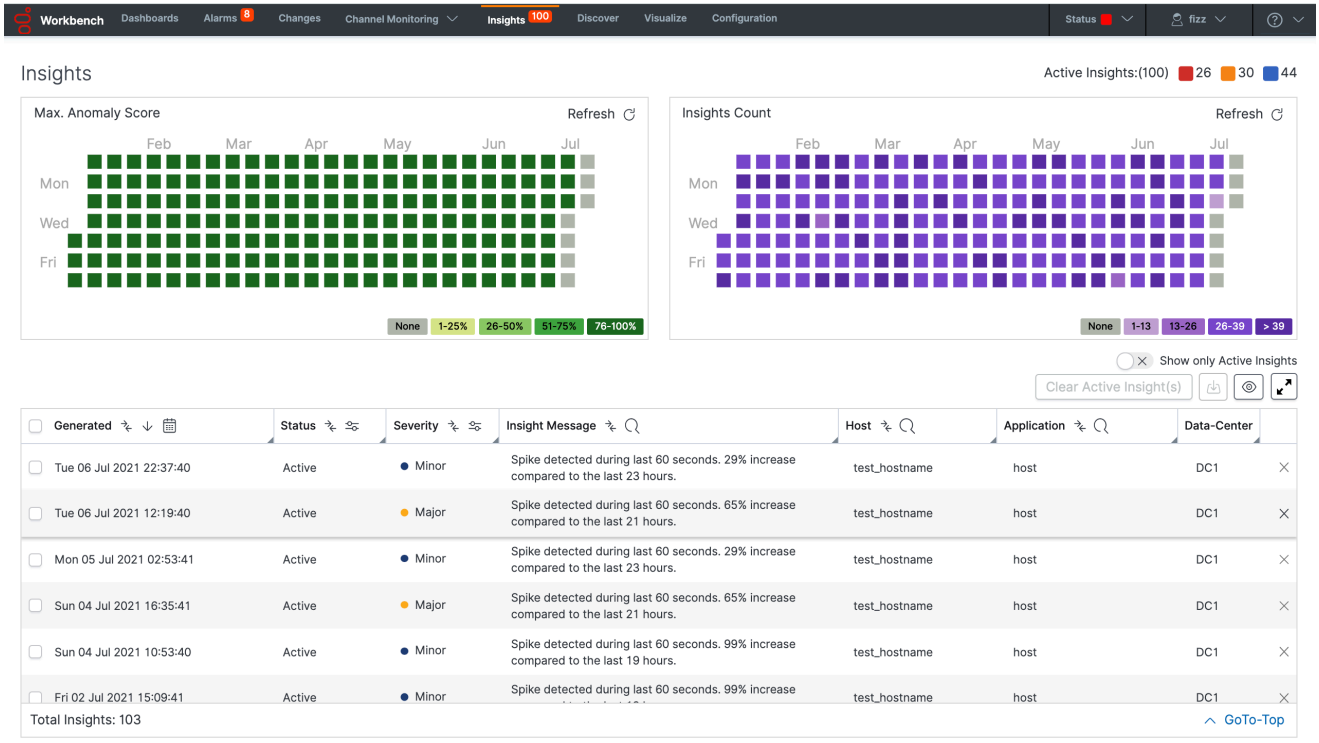
Release Notes

Details of Workbench 9 *Release Notes* can be found on the Genesys Customer Care Portal via <https://docs.genesys.com/Documentation/ST/current/RNs/WorkbenchServer>

Anomaly Detection (AD)

Workbench Anomaly Detection (AD) “Insights” will be autonomously and predictively raised, via the dedicated "Insights" Console, based on the dynamic Anomaly Detection model of the ingested metric data received from Hosts/Processes, via the Workbench Remote Agent (WAR) applications that are installed on the Genesys Application servers (i.e. sip, urs, gvp etc etc).

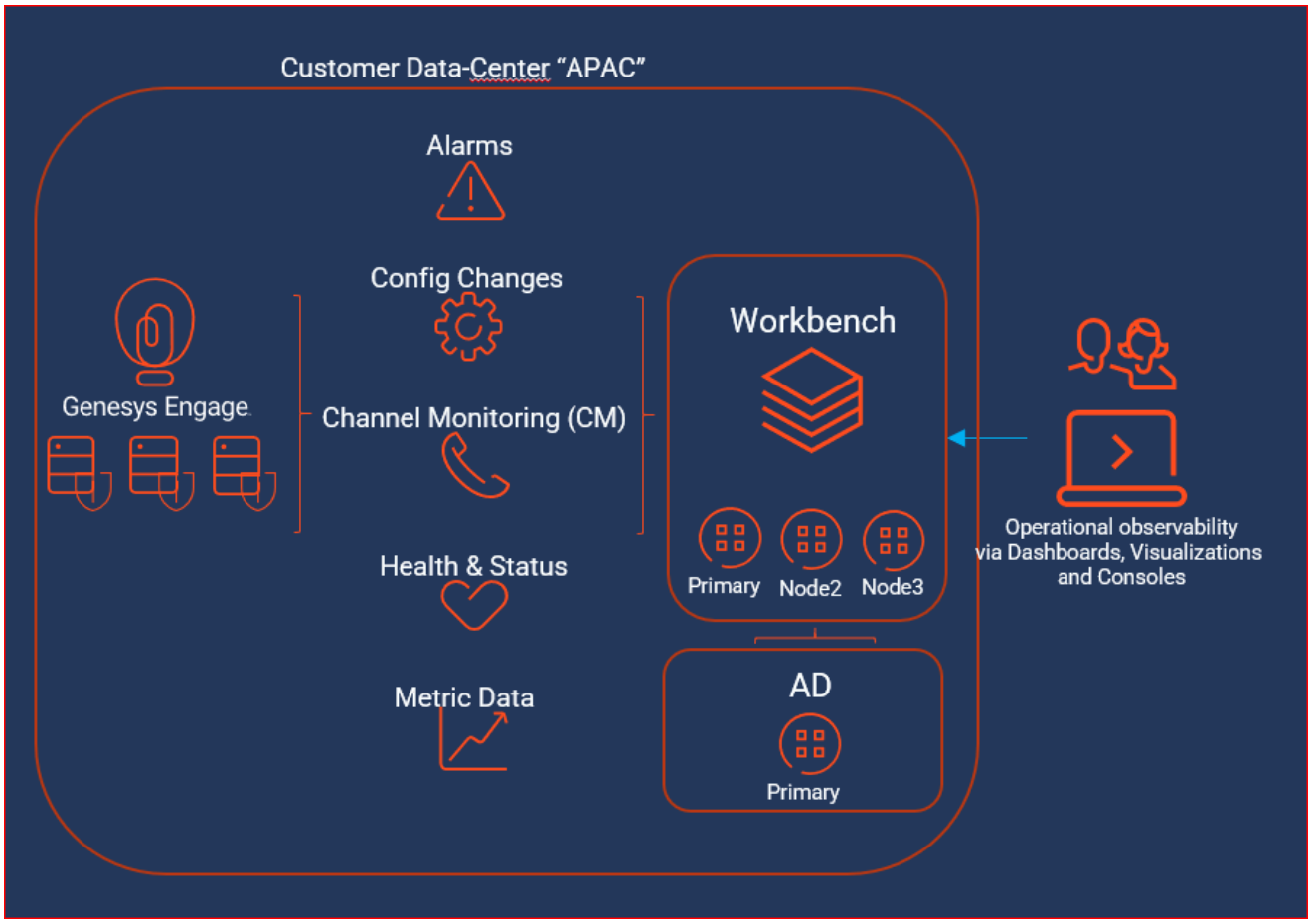
AD Insights Console



Important

- Please review Using AD for more details on using the AD feature of Workbench

Example AD Architecture



Important

- Please review AD Architecture Examples for more details on AD architectures.

Overview

Workbench Anomaly Detection (AD) is a Machine Learning (ML) feature of Workbench.

With Workbench Anomaly Detection (AD) installed, the customer is able to observe unusual, anomalous events.

Use the Workbench Anomaly Detection (AD) feature to visualize Workbench Insights in the dedicated Workbench Insights Console, these Insights will be autonomously and predictively raised based on abnormal/unusual/anomalous modelled analysis of ingested metric data (i.e. CPU/RAM/DISK/ NETWORK Metrics).

Key AD Features

- A dedicated Workbench Insights Console to view and analyze anomalies
- Workbench Anomaly Detection can proactively, autonomously and predictively detect anomalous events/issues based on Workbench ingested Metric data
- Example shipped Anomaly Detection Insights Dashboards and Visualizations providing an at-a-glance view of anomalies
- A graphical/textual "Correlation" view of Workbench Insights providing additional anomaly context
- Self-learning Machine Learning model based on the Workbench stored metric data (i.e. CPU/RAM/DISK/ NETWORK) ingested from remote hosts via Workbench Remote Agents
- Workbench Anomaly Detection is high availability capable; installing 2 or more AD Nodes/Hosts at each Data-Center enables AD HA

Important

- Workbench Anomaly Detection 9.2 is only compatible with Genesys Workbench 9.2+
- The Workbench 9.2 core components (i.e. WB IO, WB Elasticsearch, WB Kibana, WB Logstash, WB Heartbeat, WB ZooKeeper, WB Agents [for WB Hosts] and Workbench Agent Remotes [WAR's for remote Hosts]) should be installed prior to installing the Workbench Anomaly Detection (AD) 9.2 components

Important

- The Anomaly Detection components must be installed on separate hosts from the Workbench (WB) core components - i.e. do NOT install AD on the WB Hosts

Checklist

Use this section as a proactive checklist for successful Anomaly Detection (AD) planning, deployment and usage.

Item #	Description
1	Read this document thoroughly and plan your Workbench Anomaly Detection (AD) deployment carefully, before starting the Workbench AD installation.
2	Given Anomaly Detection is a feature/component of Workbench, the core Workbench features must be installed before you can install Workbench Anomaly Detection.
3	Review the Planning section to understand considerations and determine mandatory items/ actions required prior to installing Anomaly Detection - i.e. • How many Anomaly Detection (AD) Nodes/Hosts do you need in your environment? • Gain an insight into the function of the Anomaly Detection (AD) components and their respective integrations with Workbench. • Anomaly Detection (AD) requires Administrator (Windows) / Sudoer (not the *root* user) permissions for installation • Ensure the network ports utilized by Anomaly Detection are from a firewall perspective open and are not already used by other applications • Anomaly Detection (AD) uses the hostname for component configuration; therefore ensure hostname resolution between Workbench and AD Host is accurate and robust
4	As part of Planning, carefully review and determine your Anomaly Detection Sizing requirements.
5	Review Anomaly Detection FAQ's for common questions.
6	Review Anomaly Detection Best Practises for common guidance.
7	Once the Planning section is complete, proceed to Download Anomaly Detection (AD)
8	Review and complete the AD Pre-Installation Steps
9	Begin the Anomaly Detection installation, starting with the Anomaly Detection Primary Node/Host -

Item #	Description
	i.e: • AD Master Node Windows Installation • AD Master Node Linux Installation
10	If needed, continue with the Anomaly Detection Additional Node(s) installation - i.e: • AD Additional Node Windows Installation • AD Additional Node Linux Installation
11	At this stage, you now have an Anomaly Detection Primary Node or Anomaly Detection Cluster deployment up and running in your environment.
12	Review this section for details on Using AD
13	Review Anomaly Detection Troubleshooting for guidance on AD issues.
14	Review AD Options for help on Anomaly Detection configuration options/settings.
15	Review these AD Upgrade sections when migrating to a new release of Anomaly Detection.

Planning

This chapter provides general information for the planning, deployment/installation and configuration of Workbench Anomaly Detection (AD).

- AD Architecture
- AD Components
- AD Pre-Requisites
- AD Network and Security Considerations
- AD Sizing
- AD Downloading

AD Architecture

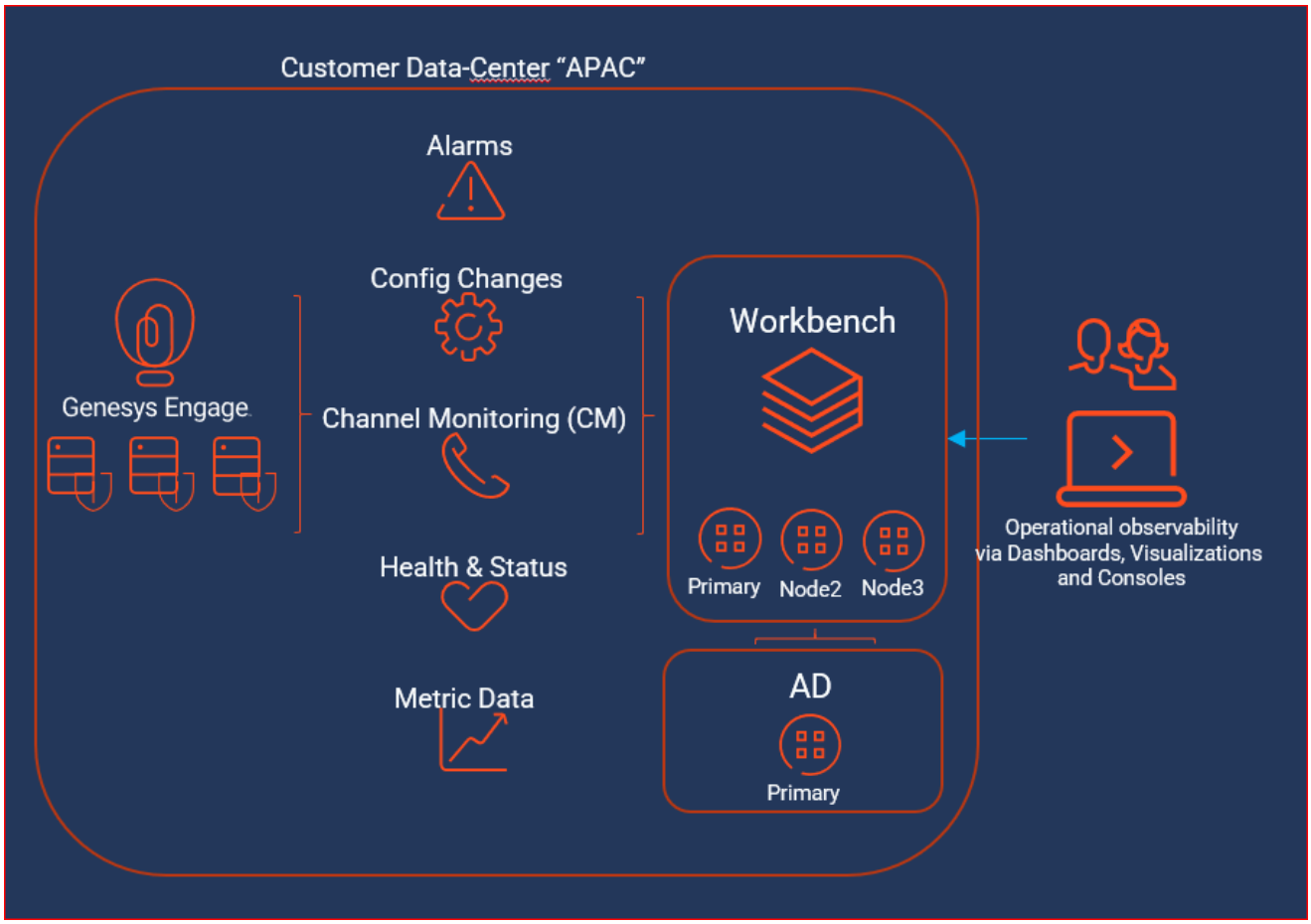
This section details example Workbench Anomaly Detection (AD) architectures; both **stand-alone** and **distributed** Anomaly Detection (AD) deployments.

> **Important**
>
> - The Anomaly Detection components must be installed on separate hosts from the Workbench (WB) core components - i.e. do NOT install AD on the WB Hosts

AD Single Node - within single Workbench Data-Center

The example architecture below provides the following:

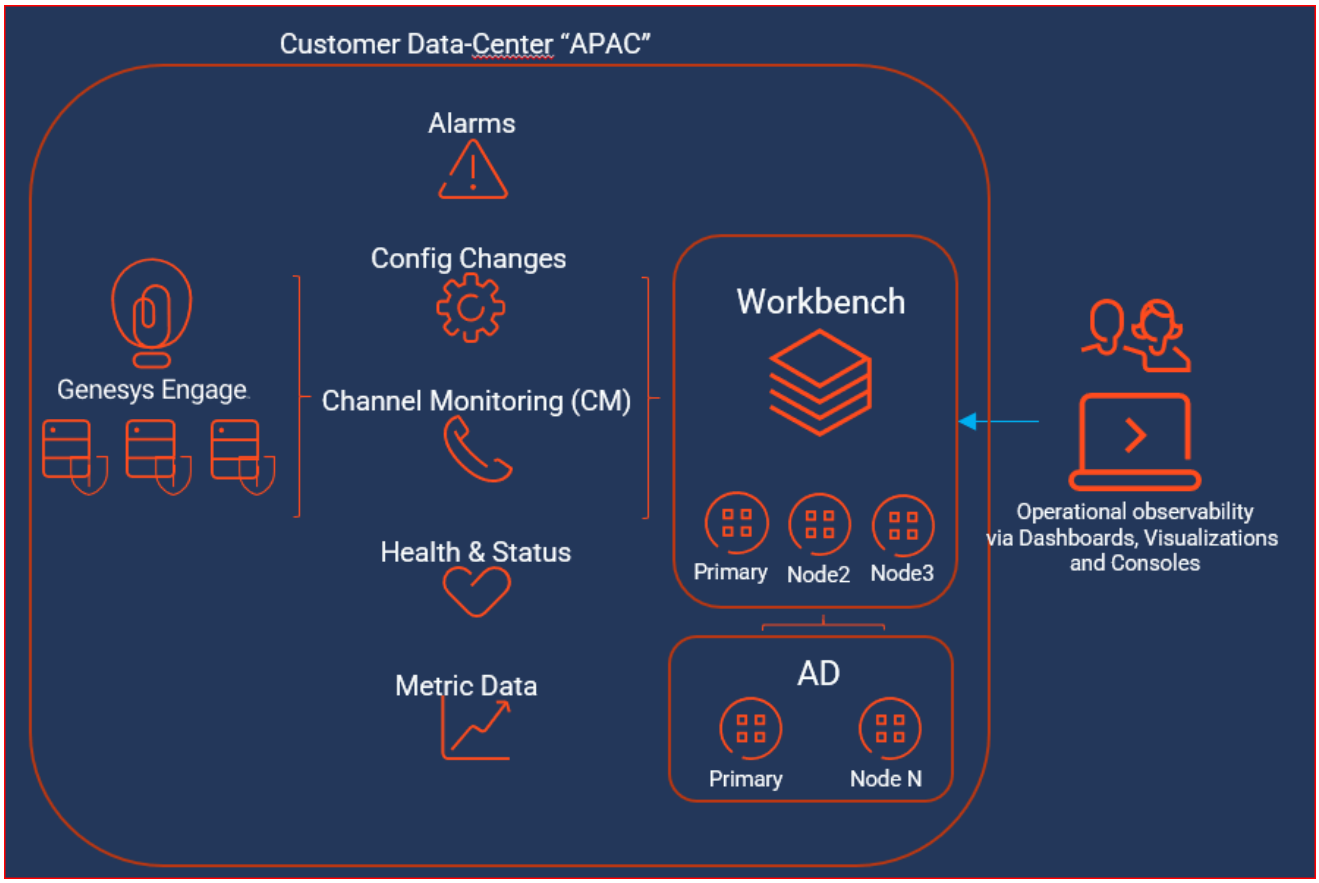
- Workbench AD is a **single** Node/Host
- Workbench AD is integrated with a **single** Workbench Data-Center/Site (i.e. APAC) deployment



AD Multi Node - within single Workbench Data-Center

The example architecture below provides the following:

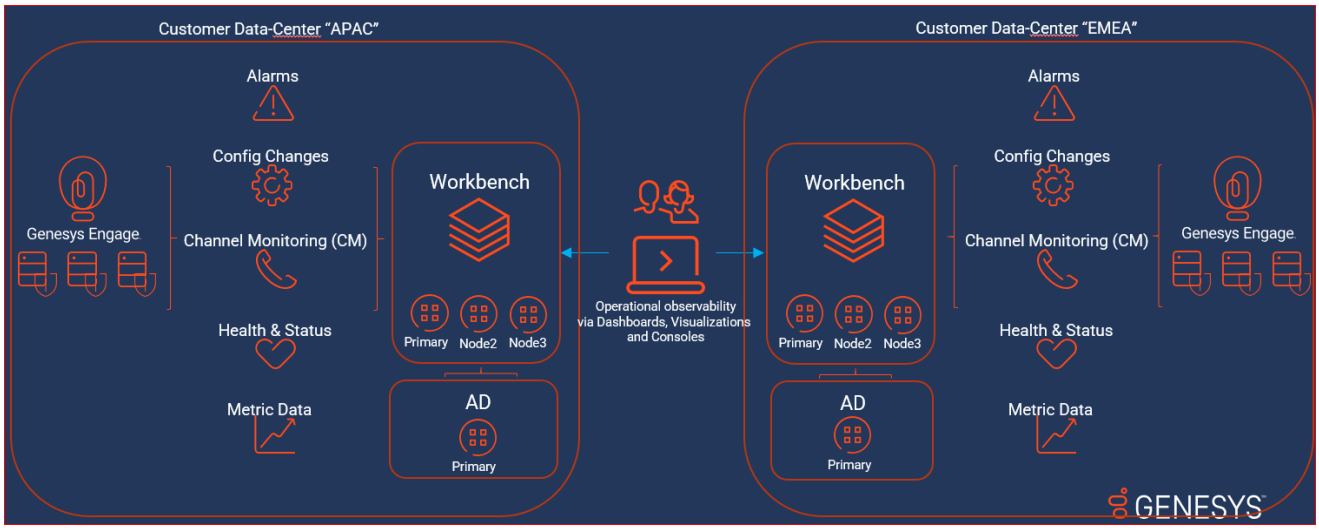
- Workbench AD is a **multi/HA** Nodes/Hosts
- Workbench AD has **Additional Nodes/Hosts** and is therefore running AD in **High Availability** mode (i.e. redundancy) and **Load Balancing** (i.e. increased scalability) mode
- Workbench AD is integrated with a **single** Workbench Data-Center/Site (i.e. APAC) deployment



AD Single Node - within multi Workbench Data-Centers

The example architecture below provides the following:

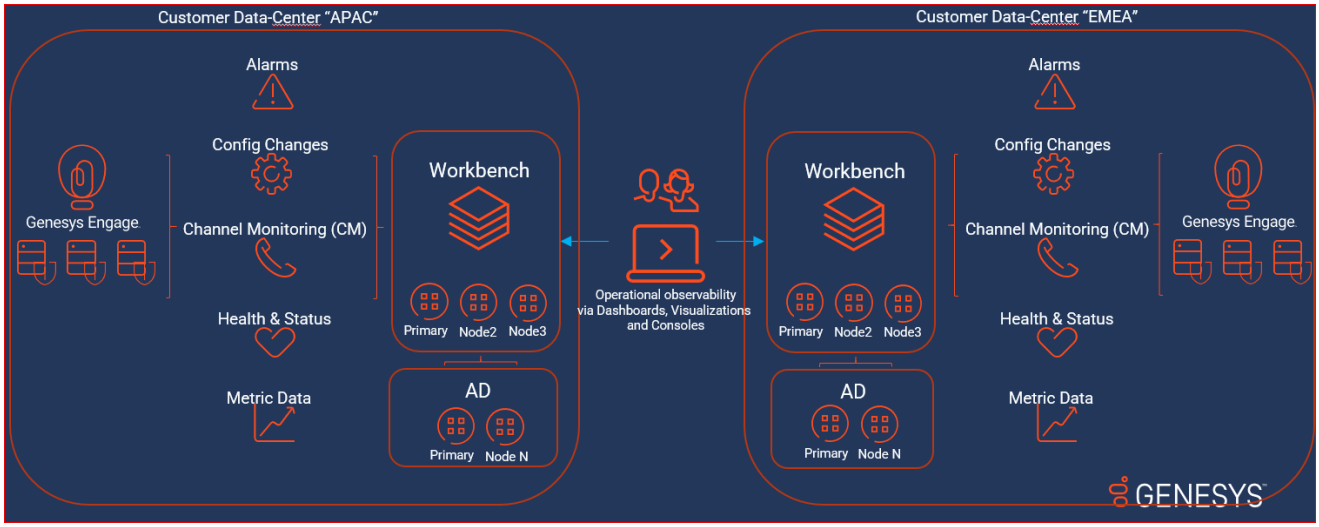
- Workbench AD is a **single** Node/Host at each Data-Center
- Workbench AD is integrated with a **multi** Workbench Data-Center/Site (i.e. APAC and EMEA) deployment
- Given the multi Data-Center integration, Workbench Insights will be visible holistically irrespective of the Workbench Data-Center the user is logged into



AD Multi Node - within multi Workbench Data-Centers

The example architecture below provides the following:

- Workbench AD is a **multi/HA** Nodes/Hosts at each Data-Center
- Workbench AD has **Additional Nodes** and is therefore running in **High Availability** mode (i.e. redundancy) and **Load Balancing** (i.e. increased scalability) mode
- Workbench AD is integrated with a **multi** Workbench Data-Center/Site (i.e. APAC and EMEA) deployment
- Given the multi Data-Center integration, Workbench Insights will be visible holistically irrespective of the Workbench Data-Center the user is logged into



AD Components

This section provides a high level summary of the Anomaly Detection (AD) components/applications.

App Manager

App Manager is responsible for initializing and monitoring each AD component, as well as scalability and high availability functions.

AD Message Processor

AD Message Processor is responsible for processing messages received from the Workbench components.

AD Streaming Consumer

AD Streaming Consumer is responsible for receiving and pre-processing messages.

AD Collector

AD Collector is responsible for local data-storage.

AD Anomaly Detector

AD Anomaly Detector is responsible for calculating the anomaly scores and generating Insights.

AD Model Management

AD Model Management is responsible for anomaly model training.

AD Message Producer

AD Message Producer is responsible for processing the results generated by AD.

AD Pre-Requisites

Anomaly Detection (AD) and Workbench (WB) Compatibility Matrix

AD Version	WB Version(s)	Compatible	Restrictions	Notes
• 9.2.000.00	• 9.2.000.xx • 9.3.000.00	Yes		

AD Host(s)/Server(s) Operating System Requirements

The Anomaly Detection components are supported on the following Operating Systems:

- Microsoft Server 2012 and 2016
- RHEL 7
- CentOS 7

Important

- The Anomaly Detection components must be installed on separate hosts from the Workbench (WB) core components - i.e. do NOT install AD on the WB Hosts

Important

- Workbench uses the Hostname for component configuration/communication
- Please ensure hostname resolution between Workbench components, including Anomaly Detection Nodes/Hosts and Engage Hosts is accurate and robust
- If the Workbench Hosts have multiple NIC's, please ensure the Hostname resolves to the desired IP Address **prior** to Workbench installation
- Genesys support for the platform versions mentioned on this page ends when the

respective vendors declare End of Support.

Network Ports - AD Hosts

Anomaly Detection (AD) uses the network ports below.

Port	Component	Comments
50000 - 51000	App Manager	Nodes and Inter-process communication
8182	AD API	Expose AD status and visualizations
9091 & 5067	Workbench Agent & Metricbeat	Status and Metrics

Important

- Ensure the Ports are reviewed, opened/unblocked and not in use by other applications **prior** to starting the AD installation
- The ports above can be edited/changed via the Workbench Configuration Console and selecting/editing the respective Workbench AD application object

Hardware Sizing Requirements

Please review the Sizing section for AD hardware requirements.

AD Network and Security Considerations

Considering Anomaly Detection (AD) is a Workbench feature/component, please follow the Workbench Networks and Security Considerations for details.

Configuring TLS

AD communicates with Workbench IO over HTTP for insert/update of Anomaly Detection Insights and Alarms.

> **Important**
>
> - TLS connection/communication between Workbench IO to Anomaly Detection is supported

Enable Workbench Anomaly Detection Host TLS

Review the details of this configuration in Workbench Configuring TLS.

Please follow these steps to enable the AD Host TLS settings:

1. Certificates need to be in a Java Key Store (.jks file) and accessible on the host by the user account running AD
2. Within Workbench UI, browse to the Configuration > Hosts section and select the AD host that TLS will be enabled on
3. Within the host object settings, navigate to the "2. Workbench TLS Communication" section
4. Populate the following options:
   - Keystore Path: path of the Java Key store on the host
   - Keystore Password: password for the key store
   - Truststore Path: path to the Java trust store
   - Truststore Password: password for the Java trust store
   - Protocol (default: TLSv1.2): TLS protocol that will be used
   - Algorithms: comma-delimited list of cipher suites that the host will use for TLS negotiation/ communication with other nodes
   - Mutual-TLS: check to enable mutual TLS
5. Click the save button to commit the changes

6. Restart the AD service for changes to take effect

AD Sizing

This section defines the Workbench Anomaly Detection hardware resources required when deploying the Workbench Anomaly Detection (AD) components.

Workbench Anomaly Detection can be deployed as a single-node/host or as a multi-node/host cluster.

The Workbench Anomaly Detection multi-node cluster deployment is available to support high-availability and/or environments that have a high number of hosts and/or low collection frequency.

AD Node/Host - Cores / Memory / Disk

The minimum hardware requirements for each AD Node/Host is:

- **8** CPU Cores
- **8** GB RAM
- **30** GB HD (free)

Required Number of AD Node(s)/Host(s) at each Workbench Data-Center

Workbench currently supports ingesting Metric data from a maximum of 100 Hosts.

Required Number of AD Nodes/Hosts	Number of Hosts sending Metric data to Workbench	Number of Metrics being sent from each Host to Workbench	Frequency of Metrics being sent from each Host to Workbench
1	100	30 (default)	60 (default)
1	100	30	30
2	100	30	10

Important

- Anomaly Detection (AD) Nodes/Hosts should be separate to Workbench Nodes/Hosts - do NOT install AD components on the WB Nodes/Hosts

AD High Availability

Deploy 2 or more AD Nodes/Hosts per Data-Center to provide AD High Availability (HA) - i.e. if 1 AD Node/Host is down Metric data will continue to be processed and Workbench Insights will be generated.

AD Downloading WB Anomaly Detection

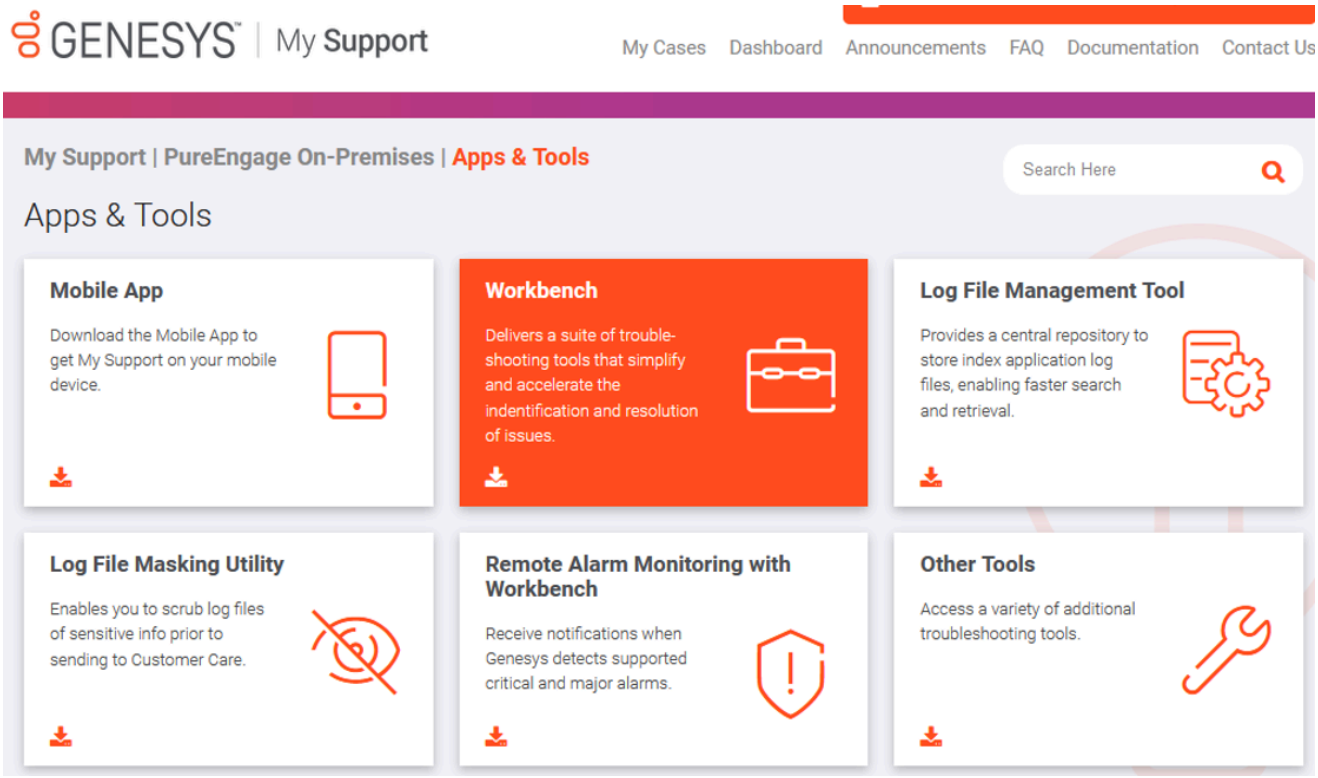
Follow these steps to download Workbench:

1. Login to My Support.
2. Click **Continue to your Dashboard** button.
3. On the *Dashboard* screen, select the **Apps and Tools** tile.
4. On the *Apps and Tools* screen, select the **Workbench** tile.
5. On the *Genesys Care Workbench* screen, click **Download Workbench AD** link.
6. On the *Terms and Conditions* screen, click the checkbox to accept the Terms and Conditions, and click **Download**.
7. On the *zip* screen, click **Download** again.

The result of the above is, depending on the target Workbench host(s) Operating System, a locally downloaded:

- **AD_9.x.xx.xx_WINDOWS.zip** file
- **AD_9.x.xxx.xx_LINUX.tar.gz** file

Please now review the **Planning** section of this document before continuing to the Deployment sections.


GENESYS | My Support
My Cases
Dashboard
Announcements
FAQ
Documentation
Contact Us
My Support | PureEngage On-Premises | Apps & Tools
Search Here
Apps & Tools
Mobile App
Download the Mobile App to get My Support on your mobile device.
Workbench
Delivers a suite of trouble-shooting tools that simplify and accelerate the indentification and resolution of issues.
Log File Management Tool
Provides a central repository to store index application log files, enabling faster search and retrieval.
Log File Masking Utility
Enables you to scrub log files of sensitive info prior to sending to Customer Care.
Remote Alarm Monitoring with Workbench
Receive notifications when Genesys detects supported critical and major alarms.
Other Tools
Access a variety of additional troubleshooting tools.

AD Deployment - New Install

This chapter provides details on the deployment of Workbench Anomaly Detection.

It contains the following sections:

- AD Pre-Installation Steps
- AD Windows Installation
  - Primary Node
  - Additional Node
- AD Linux Installation
  - Primary Node
  - Additional Node

AD Pre-Installation Steps

Important

- The Workbench core components should be installed and running **prior** to installing the Workbench Anomaly Detection (AD) components
- Please **use a non root account** with sudo permissions for all commands when installing Workbench AD on Linux
  - Do NOT use the Linux <ROOT> account to install Workbench Anomaly Detection (AD)
- Anomaly Detection (AD) uses the Hostname for component configuration/ communication
  - please ensure hostname resolution between the Workbench and Anomaly Detection (AD) Hosts is robust
- If the Anomaly Detection (AD) Host has multiple NIC's
  - please ensure the Hostname resolves to the desired IP Address prior to Anomaly Detection (AD) installation

Warning

- The Anomaly Detection 9.2.000.10 components do not support an upgrade capability - please either:
  - a) remain running AD 9.2.000.00 but follow the Workbench Agent 9.2.000.00 log4j vulnerability mitigation steps here: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/KnownIssuesandLimitations

or

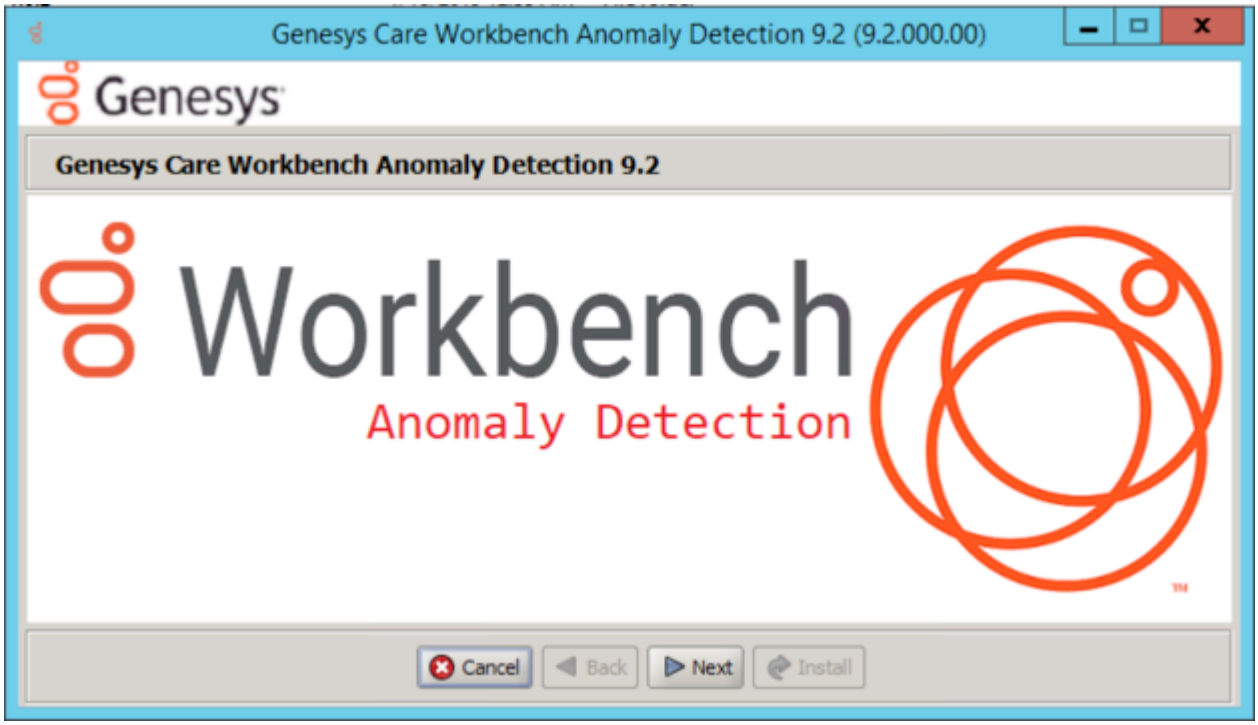
- b) un-install AD 9.2.000.00 and re-install the Anomaly Detection 9.2.000.10 components

AD Windows Install - Primary Node

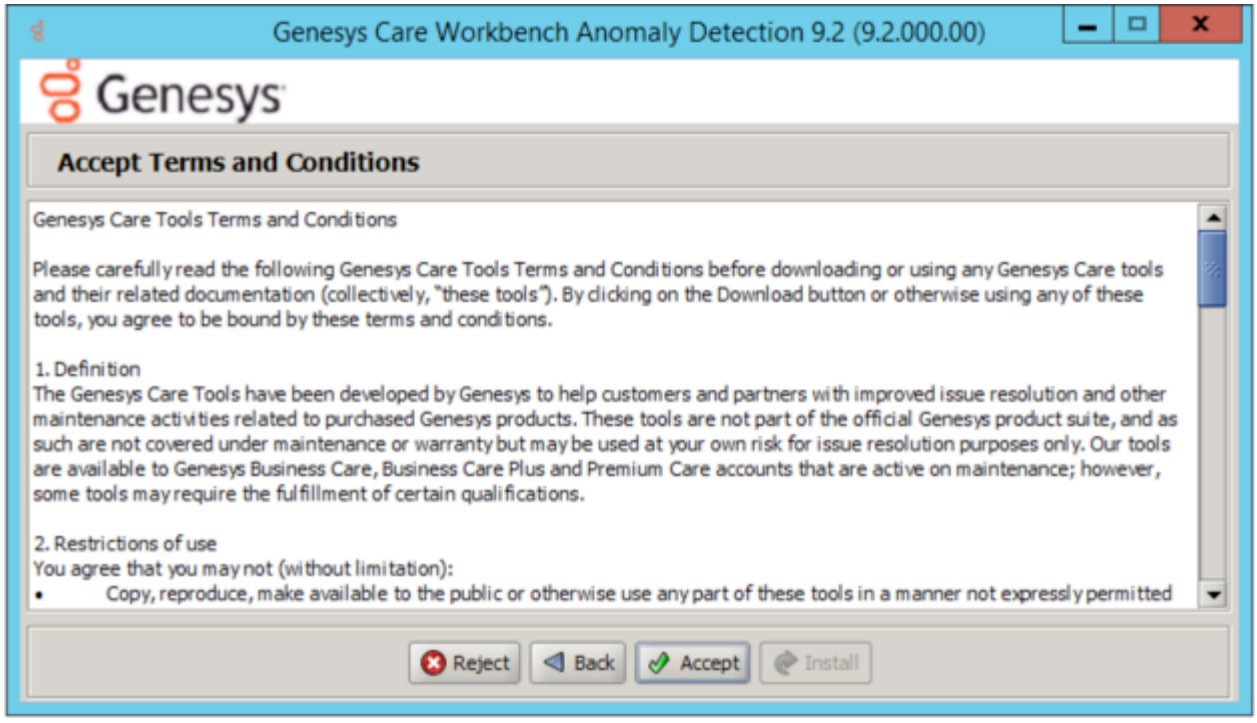
Review this link for details on downloading Workbench AD: Downloading Anomaly Detection (AD).

Please use the following steps to install Workbench AD **9.x.xxx.xx** on Windows:

1. Extract the downloaded **AD_9.x.xxx.xx_WINDOWS.zip** compressed zip file.
2. Navigate into the **AD_9.x.xxx.xx_WINDOWS/ip/windows** folder.
3. Extract the **AD_9.x.xxx.xx_Installer_Windows.zip** compressed zip file.
4. Open a command prompt **As Administrator** and run **install.bat**.
5. Click **Next** on the **Genesys Care Workbench Anomaly Detection 9.x** screen to start the Workbench AD installation.

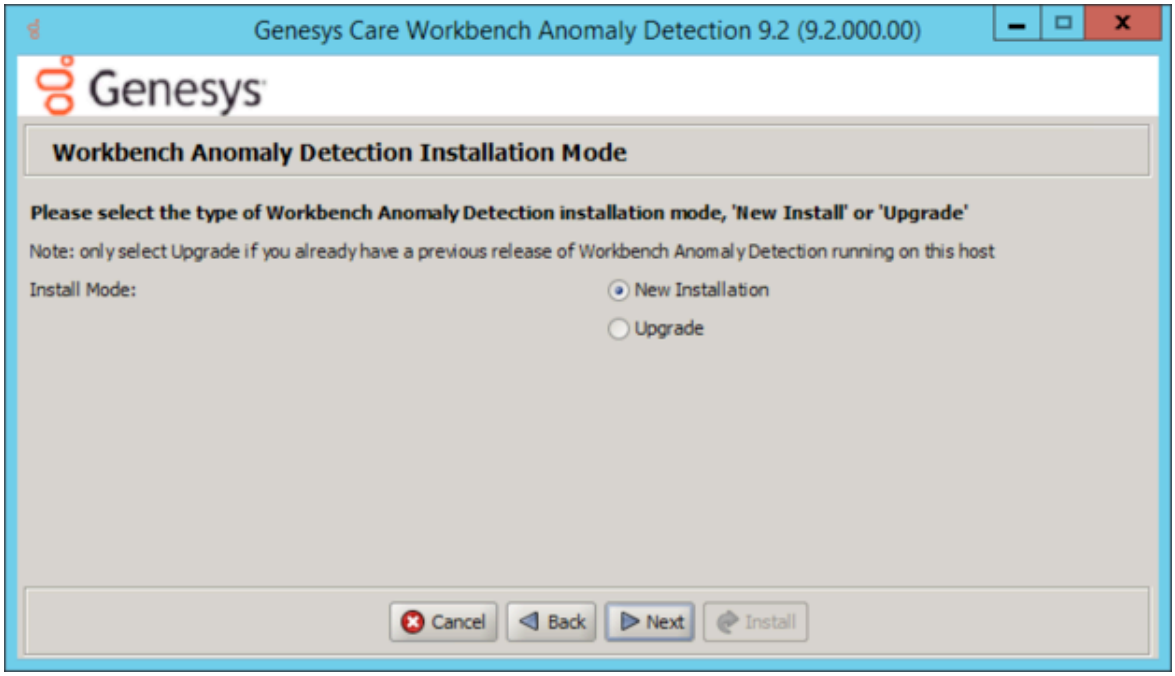


6. Review and if in agreement, click **Accept** to the **Genesys Terms and Conditions** to continue.



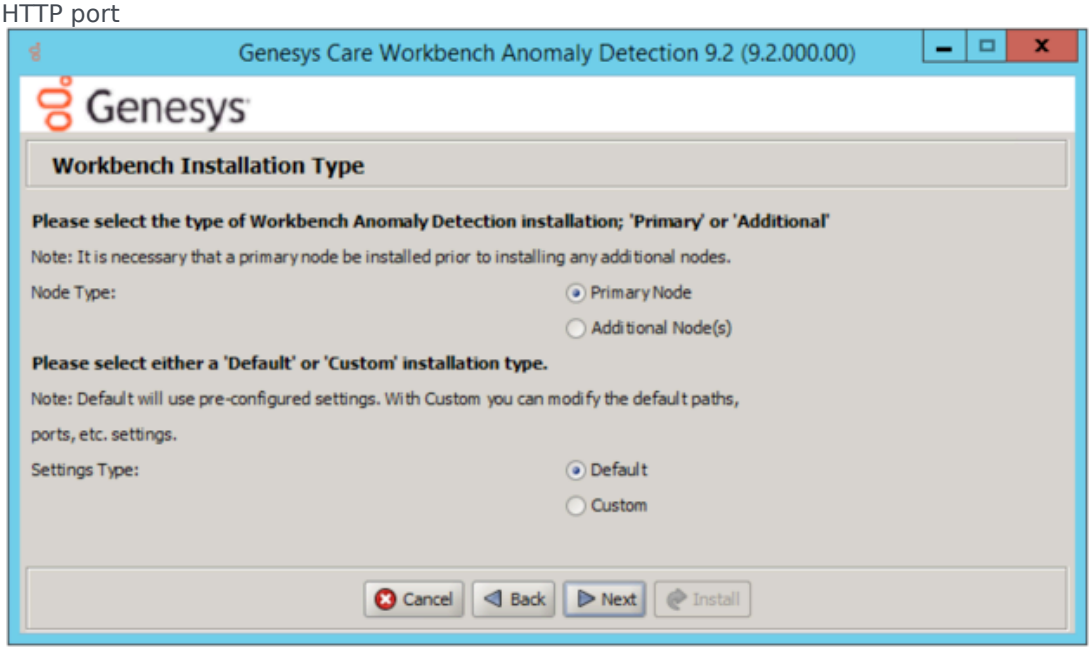
7. Select **New Installation** on the Installation Mode screen
   - There are 2 Installation Modes:
     - **New Installation** - no Workbench Anomaly Detection components are yet running on this host/node
     - **Upgrade** - you already have Workbench Anomaly Detection running on this host/node and wish to upgrade

> ### Warning
> *AD currently has no upgrade capability
> *Therefore select **New Installation** and not Upgrade during the AD 9.x.xxx.xx installation

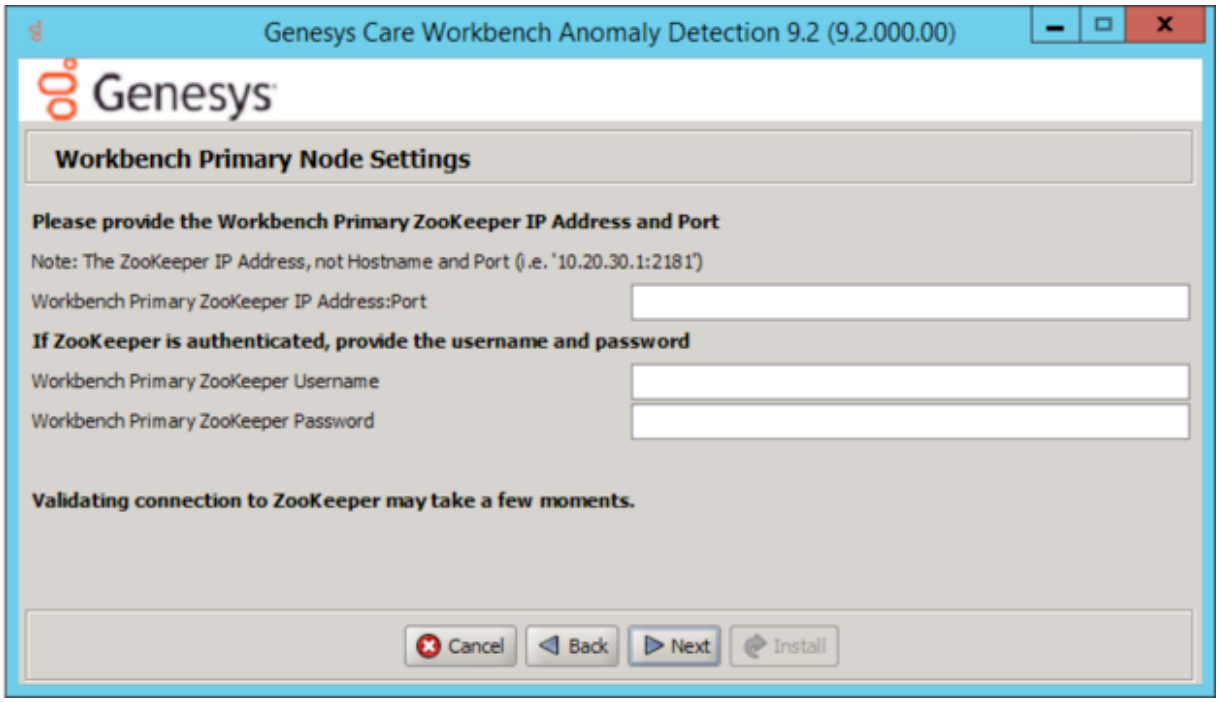


8. Select the **Workbench Anomaly Detection Installation Type:**
    1. Select the type of **Workbench Anomaly Detection Installation:**
        - **Primary:** master Anomaly Detection Node
        - **Additional:** additional Anomaly Detection Node used for distributing load. It is necessary that a primary node be installed prior to installing any additional nodes.
    2. Default or Custom Installation Type:
        - **Default** - the respective Workbench AD **Default** settings will be used.
            - Default settings being installation paths, ports, etc.
        - **Custom** - or, if required, you can change the default settings by selecting a **Custom** install.
            - For Workbench Anomaly Detection:
                - Binary files location
                - Configuration files location
                - Data files location
                - Log files location
                - Socket port
                - Incoming data port from Logstash
                - HTTP AD API port
            - For Workbench Metricbeat:
                - Binary files location
                - Data files location

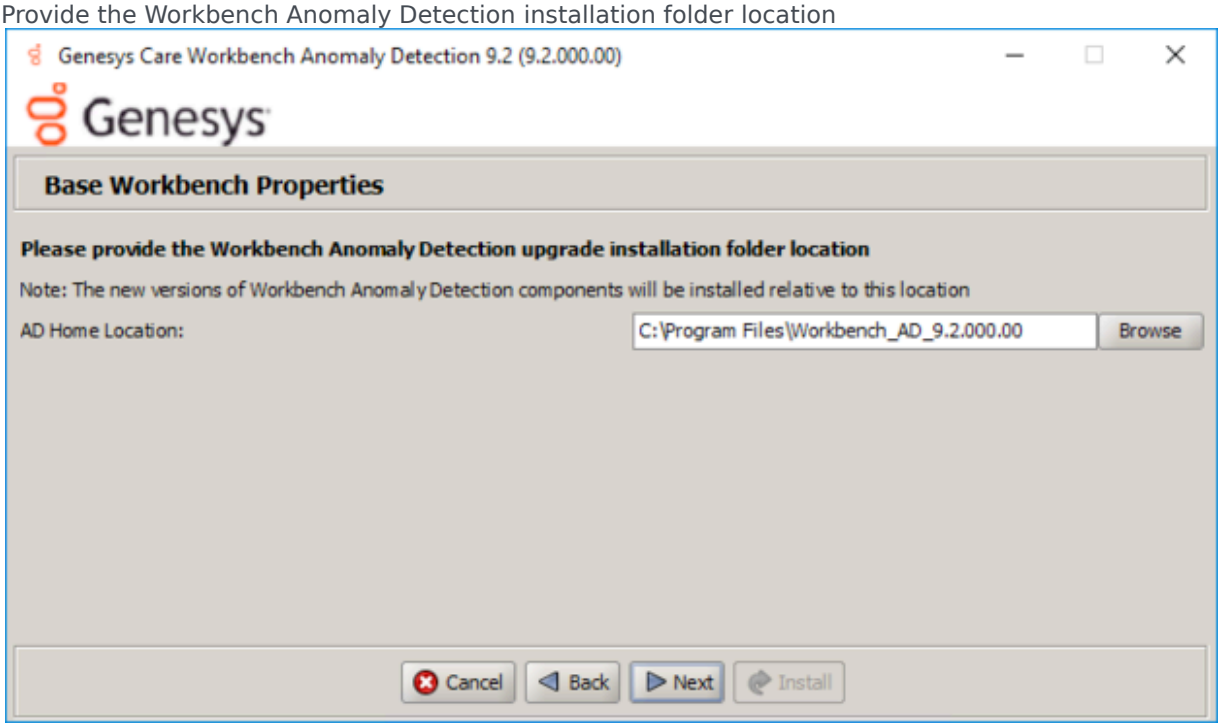
    - Log files location
    - HTTP port
- For Workbench Agent:
    - Binary files location
    - Log files location
    - HTTP port



9. Provide the Workbench **Primary Zookeeper IP Address and Port**
    - If Zookeeper is authenticated, provide username and password



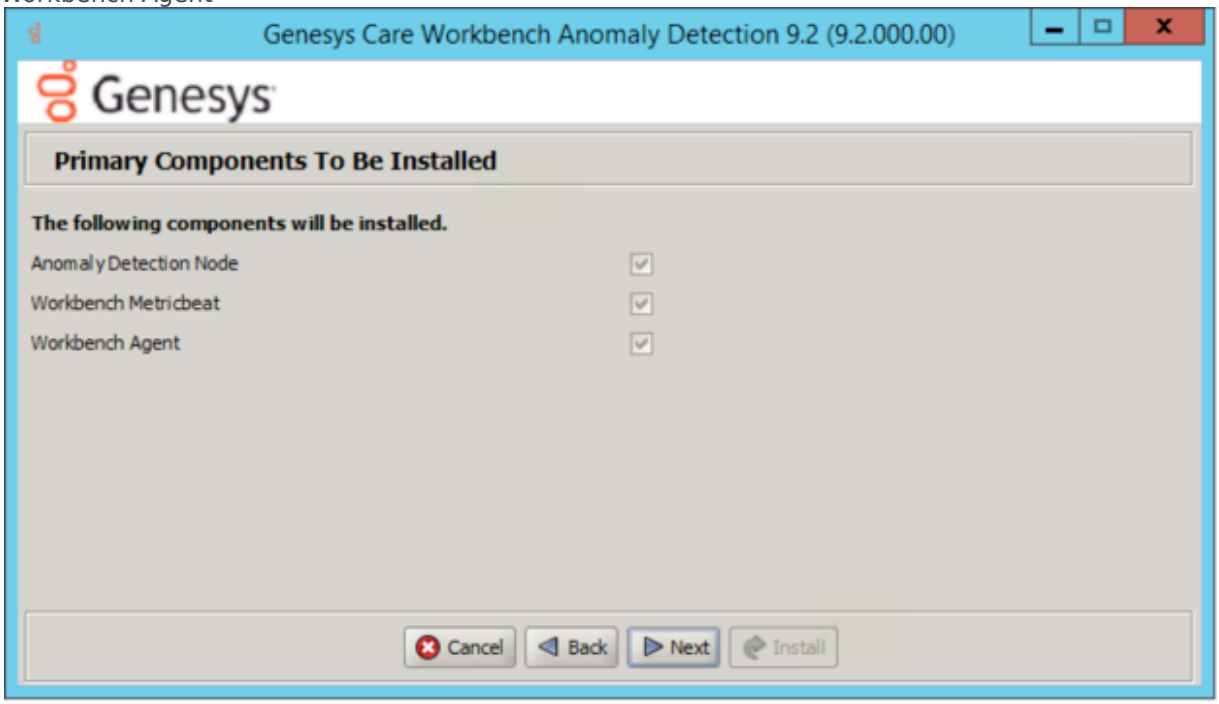
10. **Base Workbench Properties**:
    - Provide the Workbench Anomaly Detection installation folder location



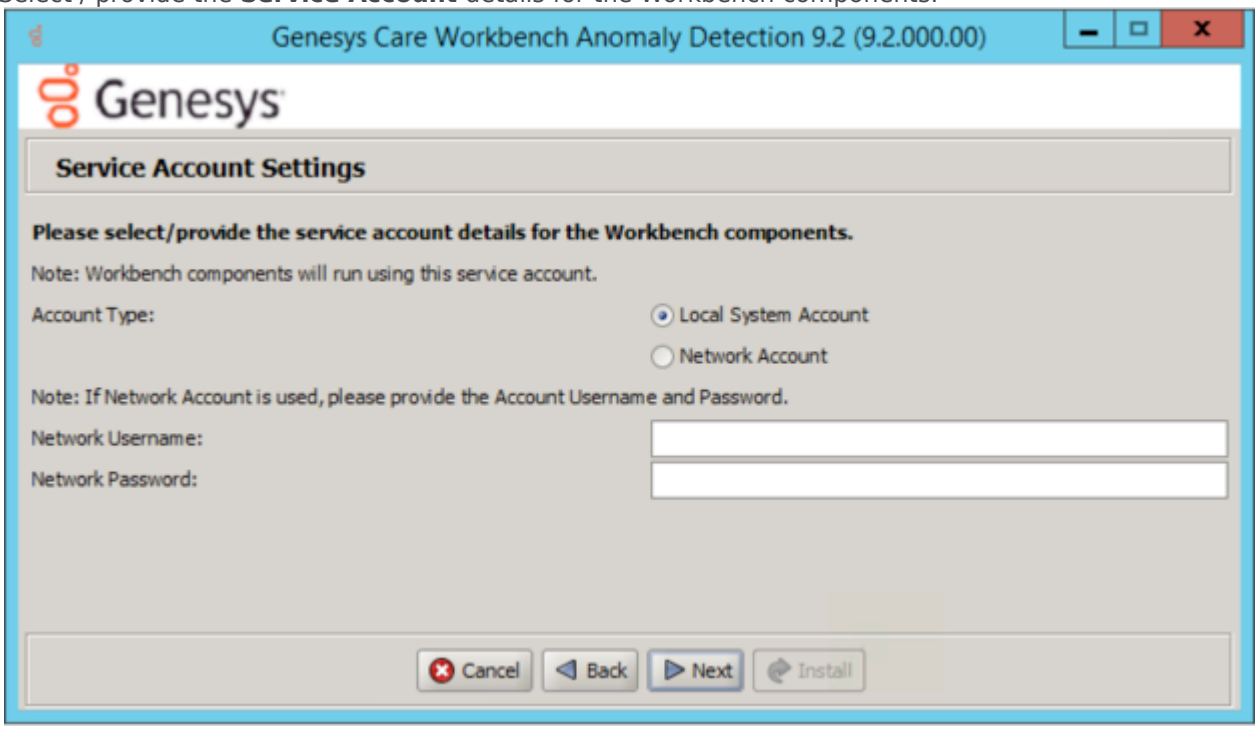
    - AD Hostname: This Hostname will be utilized by the Workbench solution components.

11. **Primary Components to be Installed**
    Information on which Workbench components are being installed on this host/node

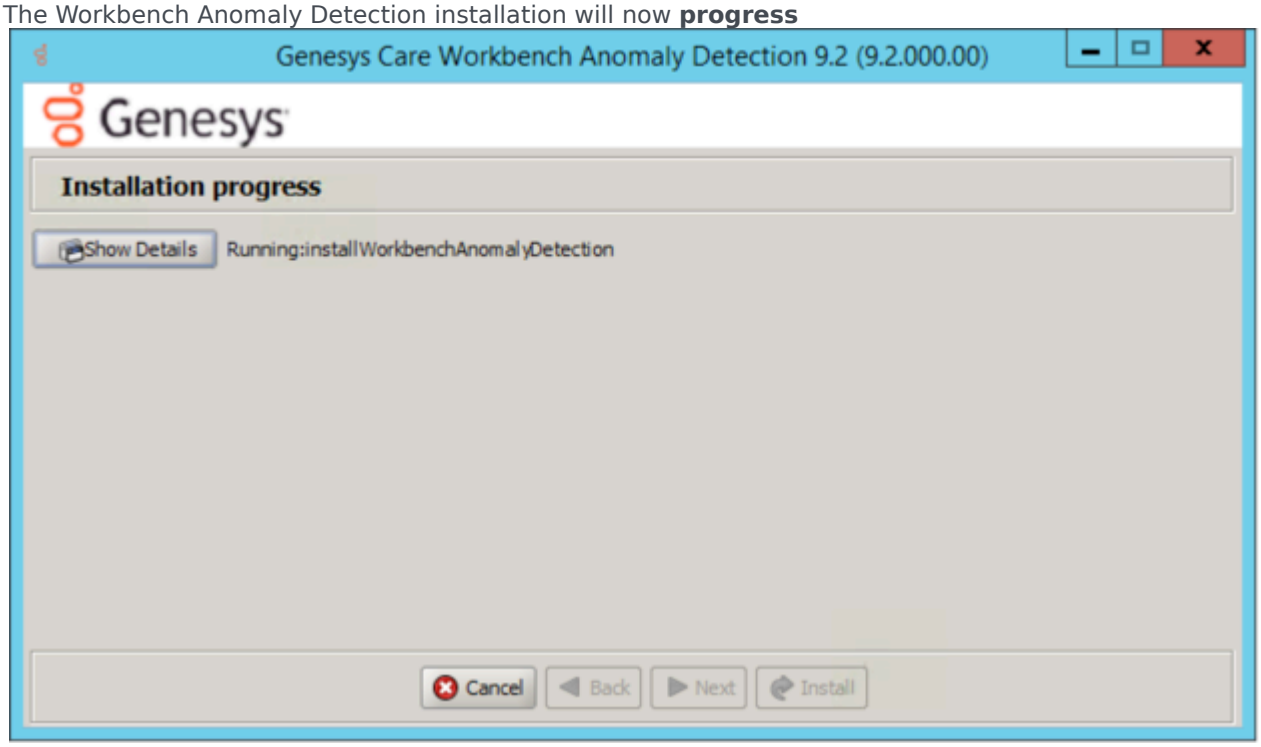
- Anomaly Detection Node
- Workbench Metricbeat
- Workbench Agent



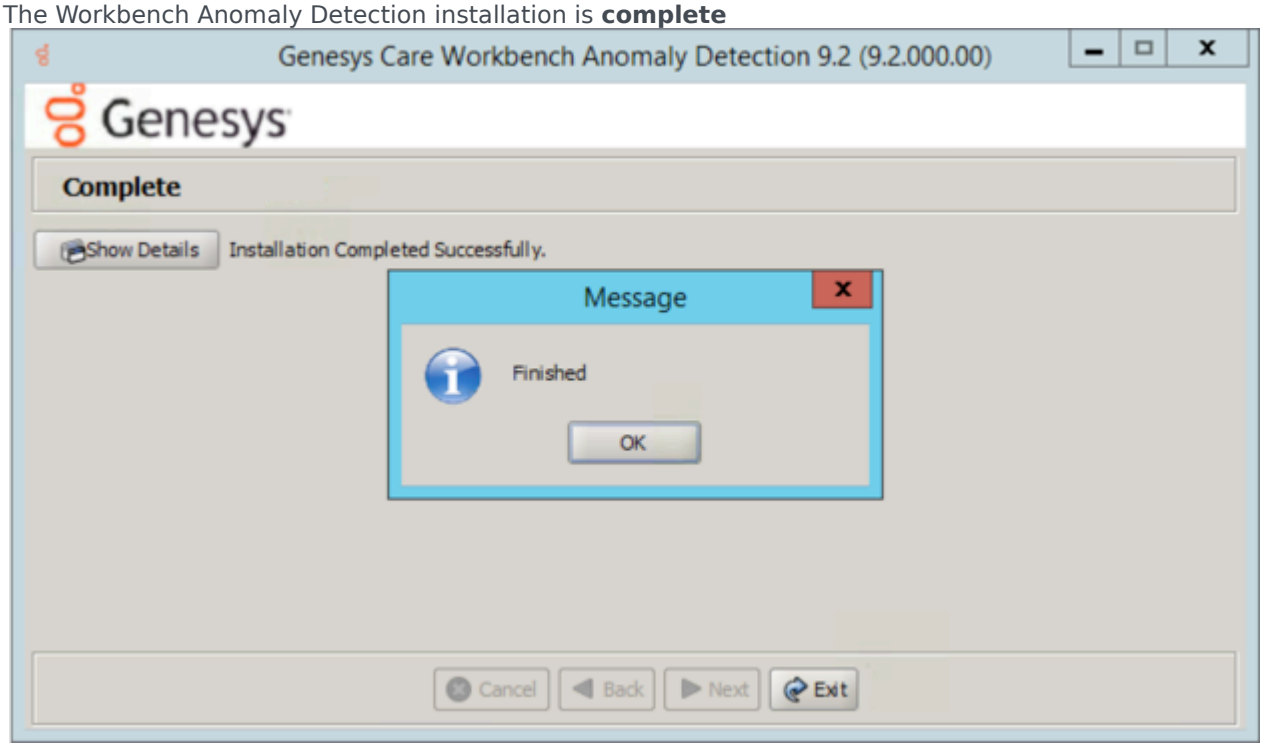
12. Select / provide the **Service Account** details for the Workbench components:



13. The Workbench Anomaly Detection installation will now **progress**



14. The Workbench Anomaly Detection installation is **complete**



Click **OK** and **Exit** to close the installation dialogs.

Post Installation Steps

1. Validate if the AD Primary components services are running:
    1. WB Anomaly Detection Node: **WB_AnomalyDetection_9.x.xxx.xx**
    2. WB Metricbeat: **WB_Metricbeat_9.x.xxx.xx**
    3. WB Agent: **WB_Agent_9.x.xxx.xx**
2. Validate if the new AD host appears in Workbench Applications as is presented in AD Configuration.
3. Follow the steps in Post Installation Configuration if needed.
4. If you are installing AD at first time, follow the guidelines given in Using AD to learn how to use Workbench Anomaly Detection Insights and its features.

Warning

- Post AD installation there is a 3 day training period before Insights are raised; during this time the Insights Console will display "No Insights Found!"

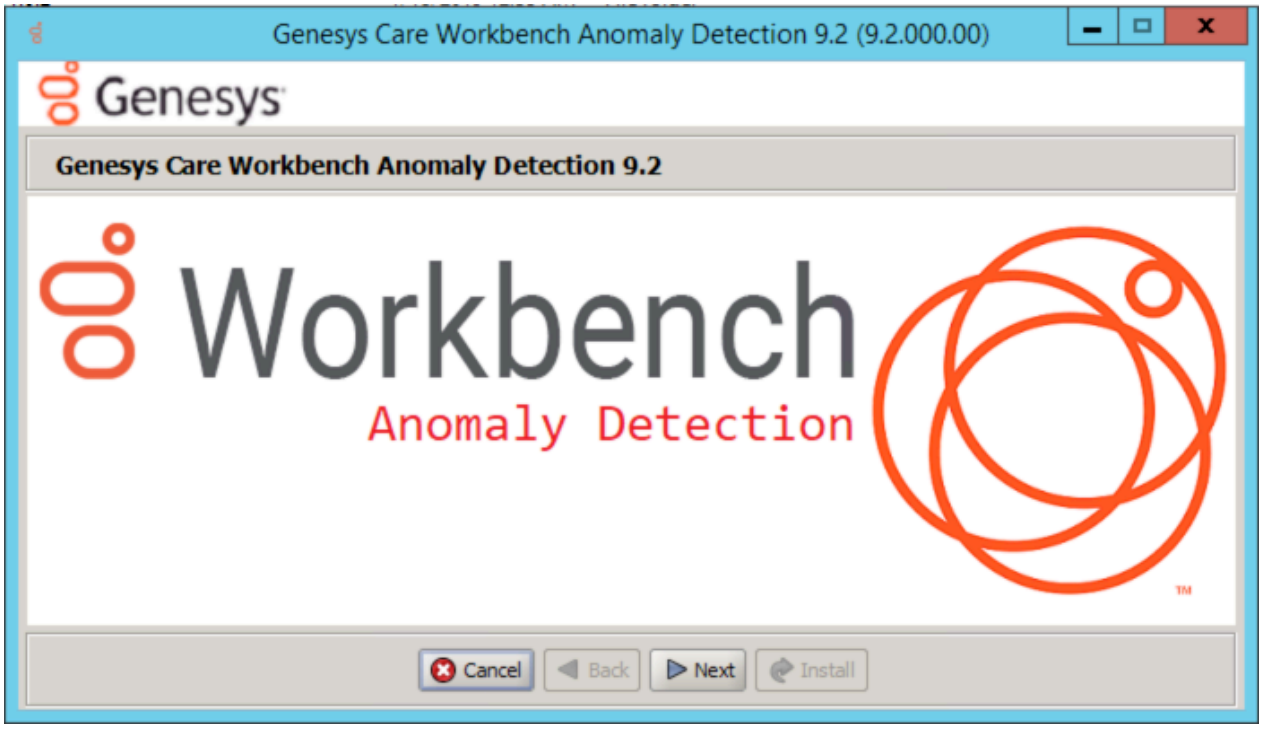
AD Windows Install - Additional Node

Review this link for details on downloading Workbench AD: Downloading Anomaly Detection (AD).

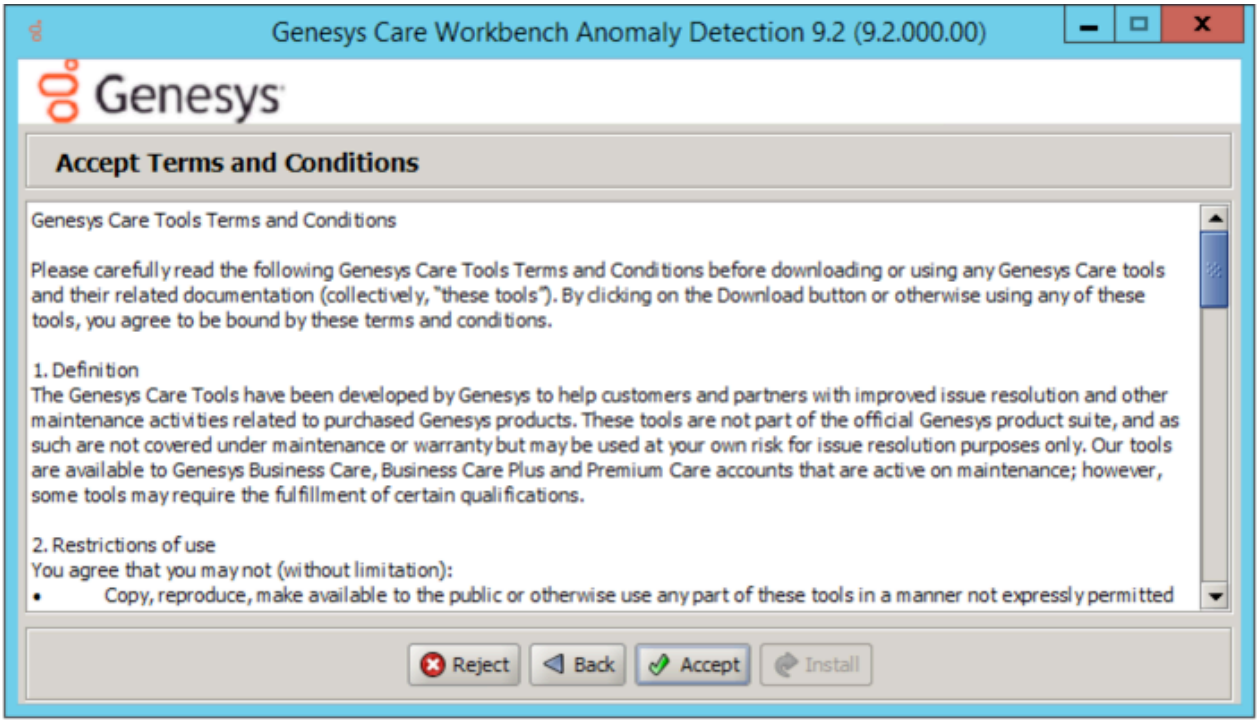
> **Important**
>
> - Ensure you have an installed and running AD Primary Node before installing any AD Additional Nodes

Please use the following steps to install Workbench AD **9.x.xxx.xx** on Windows:

1. Extract the downloaded **AD_9.x.xxx.xx_WINDOWS.zip** compressed zip file.
2. Navigate into the **AD_9.x.xxx.xx_WINDOWS/ip/windows** folder.
3. Extract the **AD_9.x.xxx.xx_Installer_Windows.zip** compressed zip file.
4. Open a command prompt **As Administrator** and run **install.bat**.
5. Click **Next** on the **Genesys Care Workbench Anomaly Detection 9.x** screen to start the Workbench AD installation.

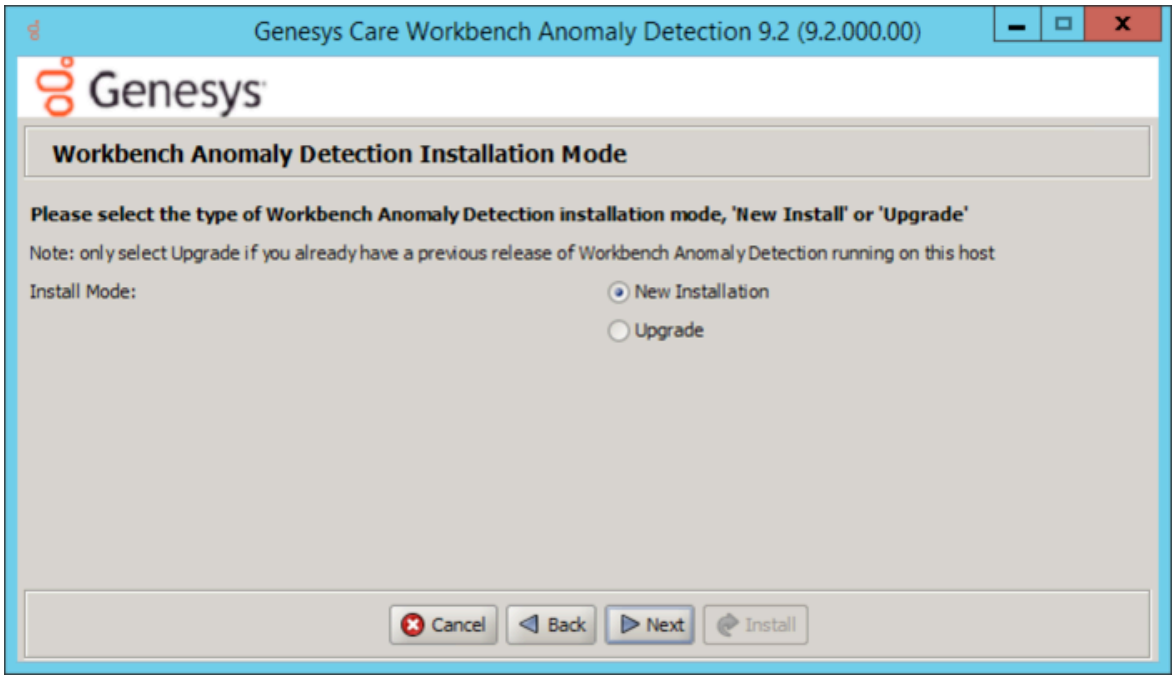


6. Review and if in agreement, click **Accept** to the **Genesys Terms and Conditions** to continue.



7. Select **New Installation** on the Installation Mode screen
   - There are 2 Installation Modes:
     - **New Installation** - no Workbench Anomaly Detection components are yet running on this host/node
     - **Upgrade** - you already have Workbench Anomaly Detection running on this host/node and wish to upgrade

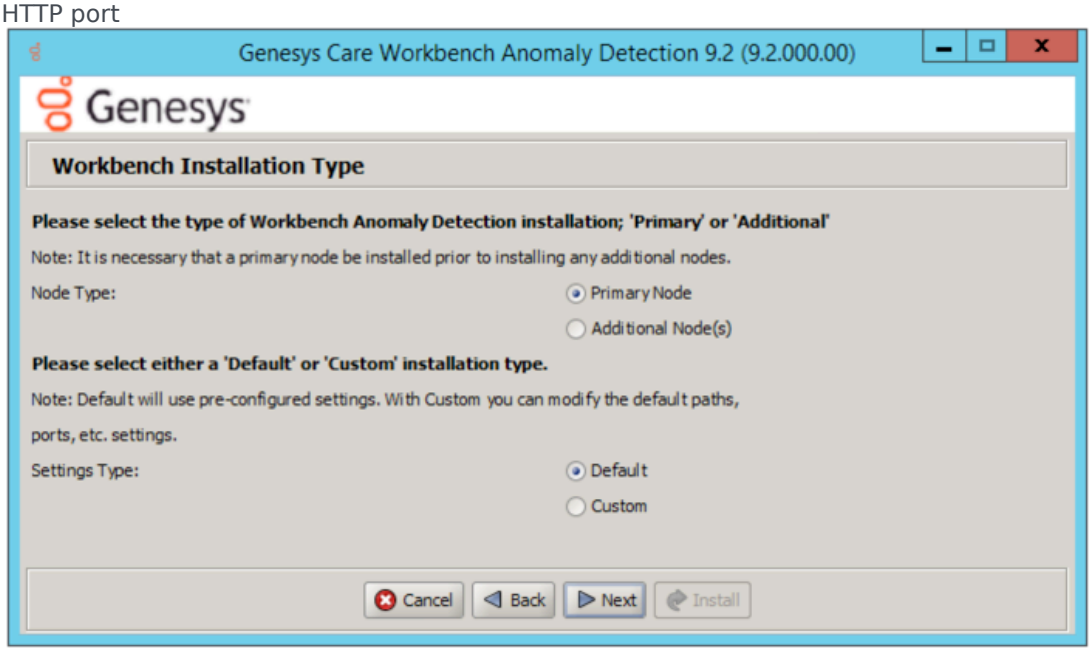
> ### Warning
> *AD currently does not support upgrade capability
> *Therefore select **New Installation** and not Upgrade during the AD 9.x.xxx.xx installation



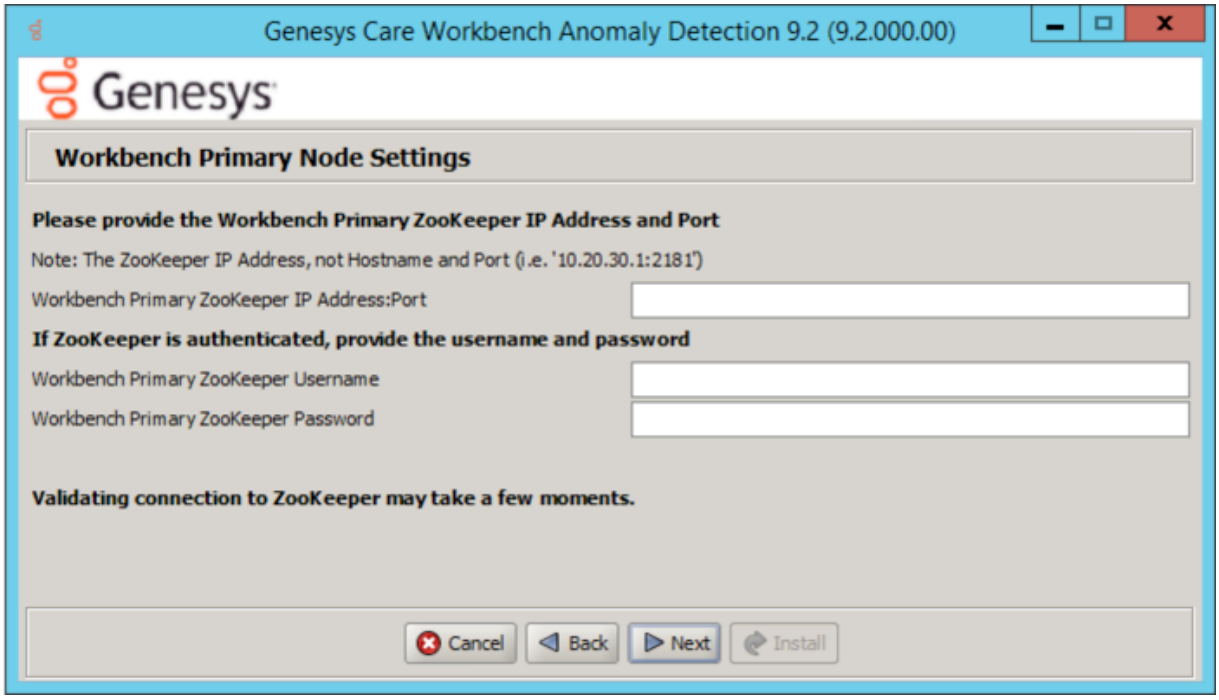
8. Select the **Workbench Anomaly Detection Installation Type:**
    1. Select the type of **Workbench Anomaly Detection Installation:**
        - **Primary** Anomaly Detection Node
        - **Additional:** Anomaly Detection Node used for distributing load. It is necessary that a primary node be installed prior to installing any additional nodes.
    2. Default or Custom Installation Type:
        - **Default** - the respective Workbench AD **Default** settings will be used.
            - default settings being paths, ports, etc.
        - **Custom** - or, if required, you can change the default settings by selecting a **Custom** install. In Custom mode, the following parameters are required:
            - For Workbench Anomaly Detection:
                - Binary files location
                - Configuration files location
                - Data files location
                - Log files location
                - Socket port
                - Incoming data port from Logstash
                - HTTP AD API port
            - For Workbench Metricbeat:
                - Binary files location

- Data files location
- Log files location
- HTTP port

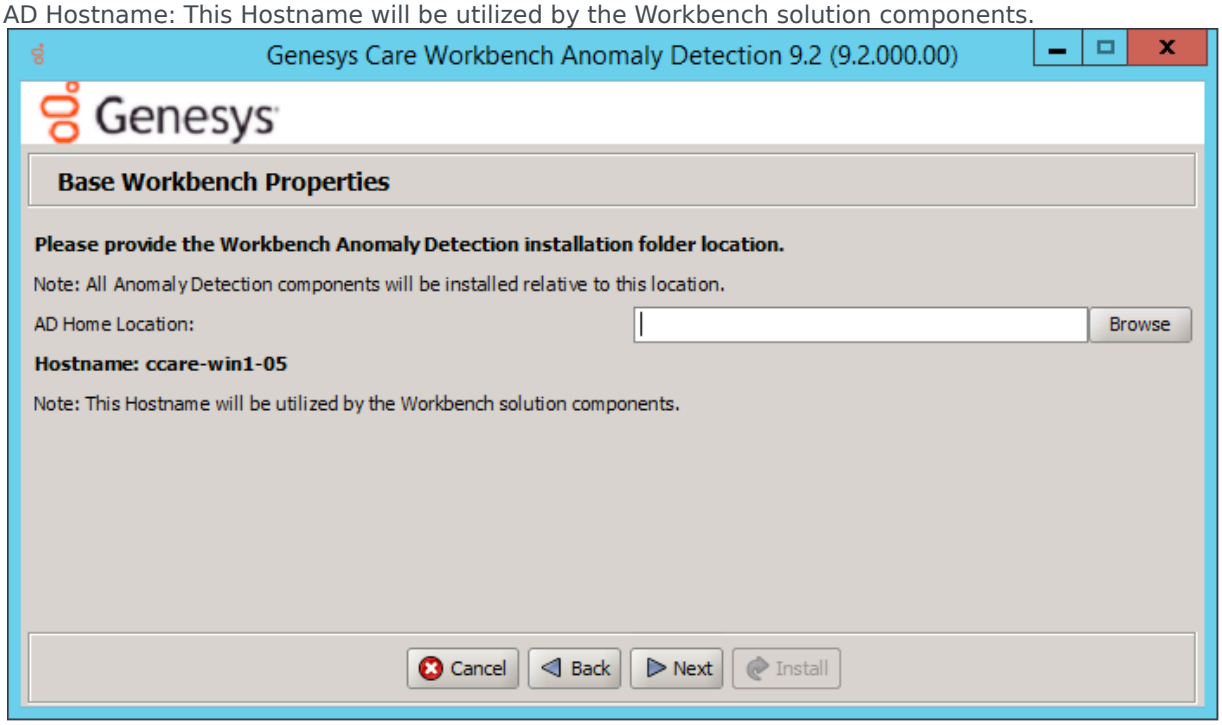
- For Workbench Agent:
  - Binary files location
  - Log files location
  - HTTP port



9. Continue with the next steps for both: **Primary or Additional Node Installation.**
10. Provide the Workbench **Primary Zookeeper IP Address and Port**
    1. If Zookeeper is authenticated, provide username and password

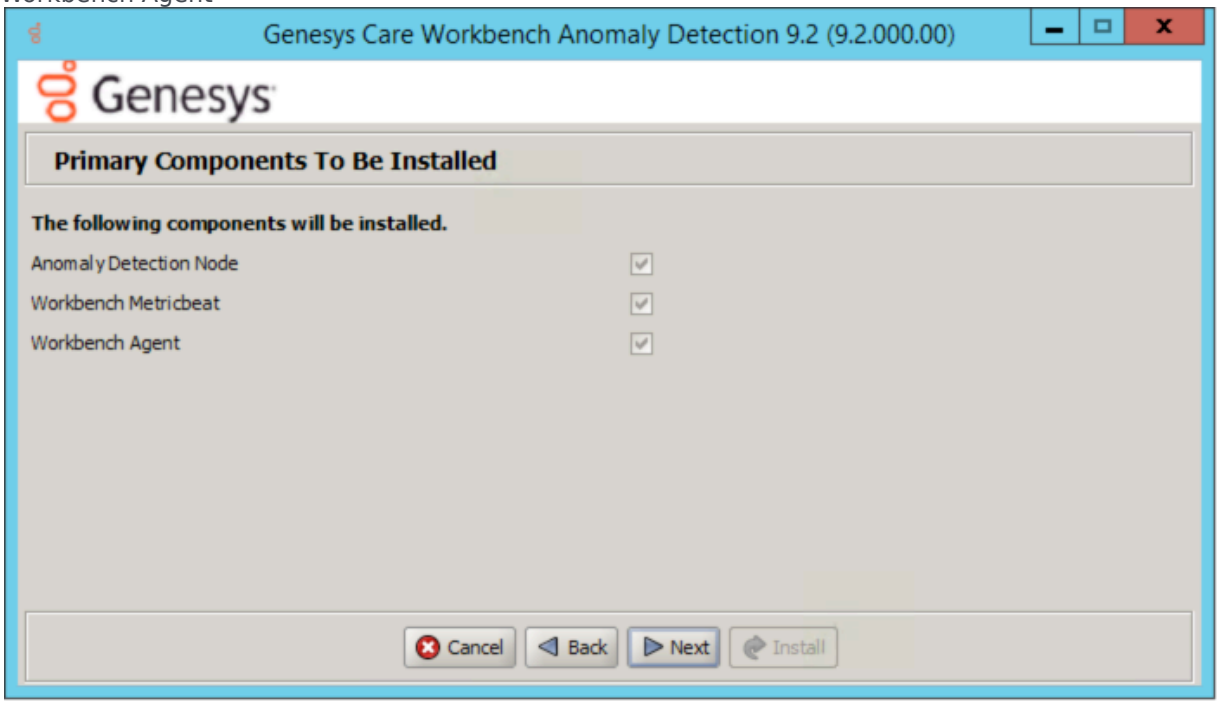


11. Base Workbench Properties:
    - Provide the Workbench Anomaly Detection installation folder location
    - AD Hostname: This Hostname will be utilized by the Workbench solution components.

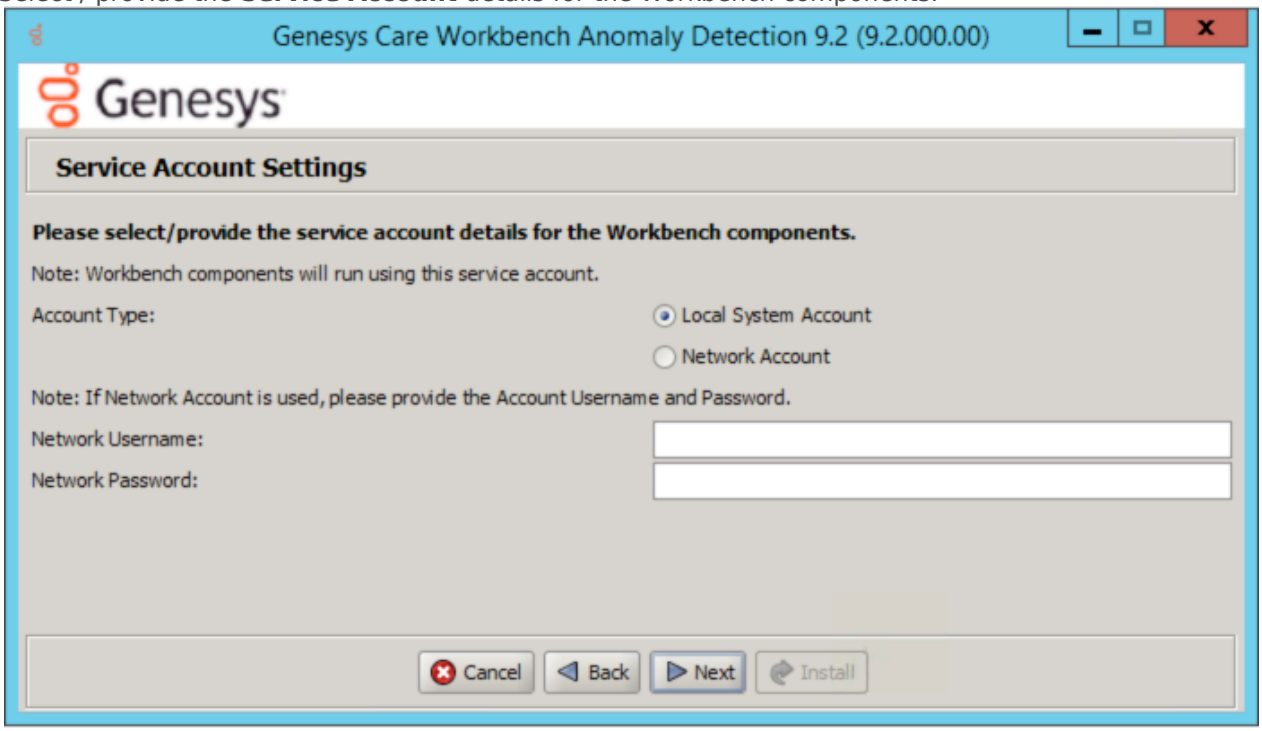


12. Primary components to be installed: Information on which Workbench components are being installed on this host/node

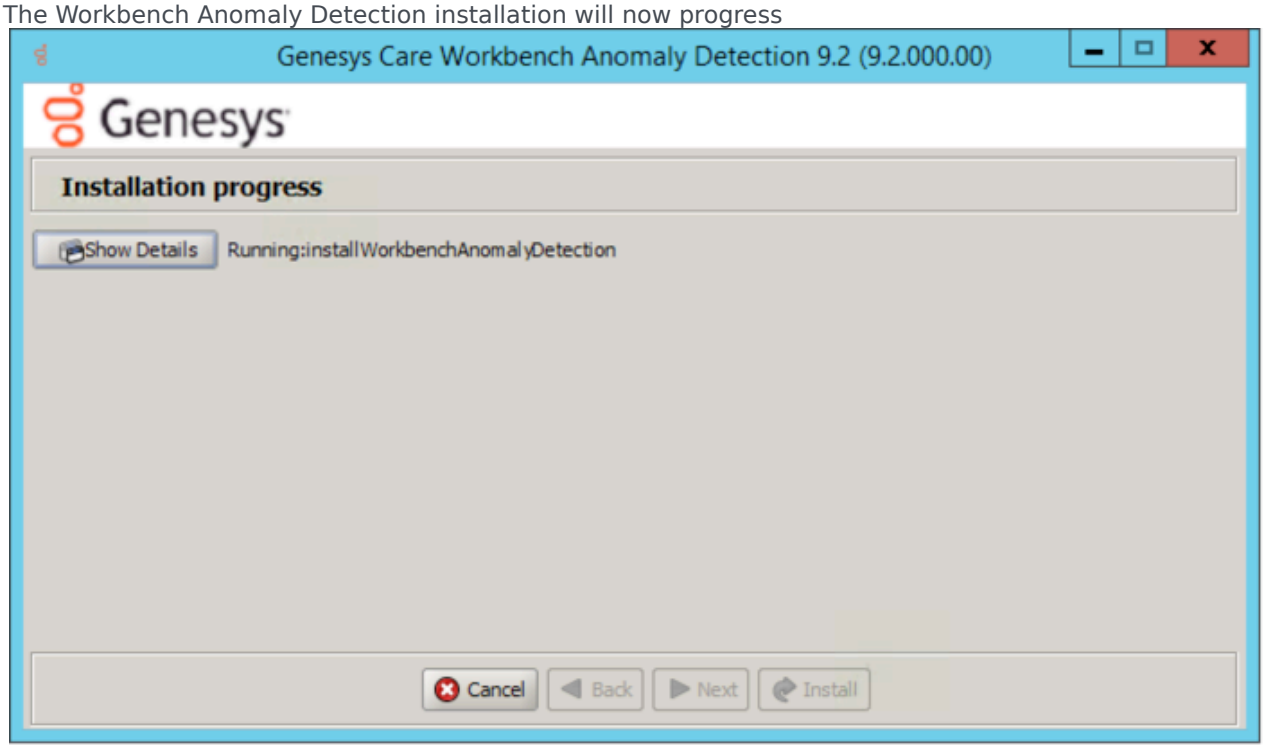
- Anomaly Detection Node
- Workbench Metricbeat
- Workbench Agent



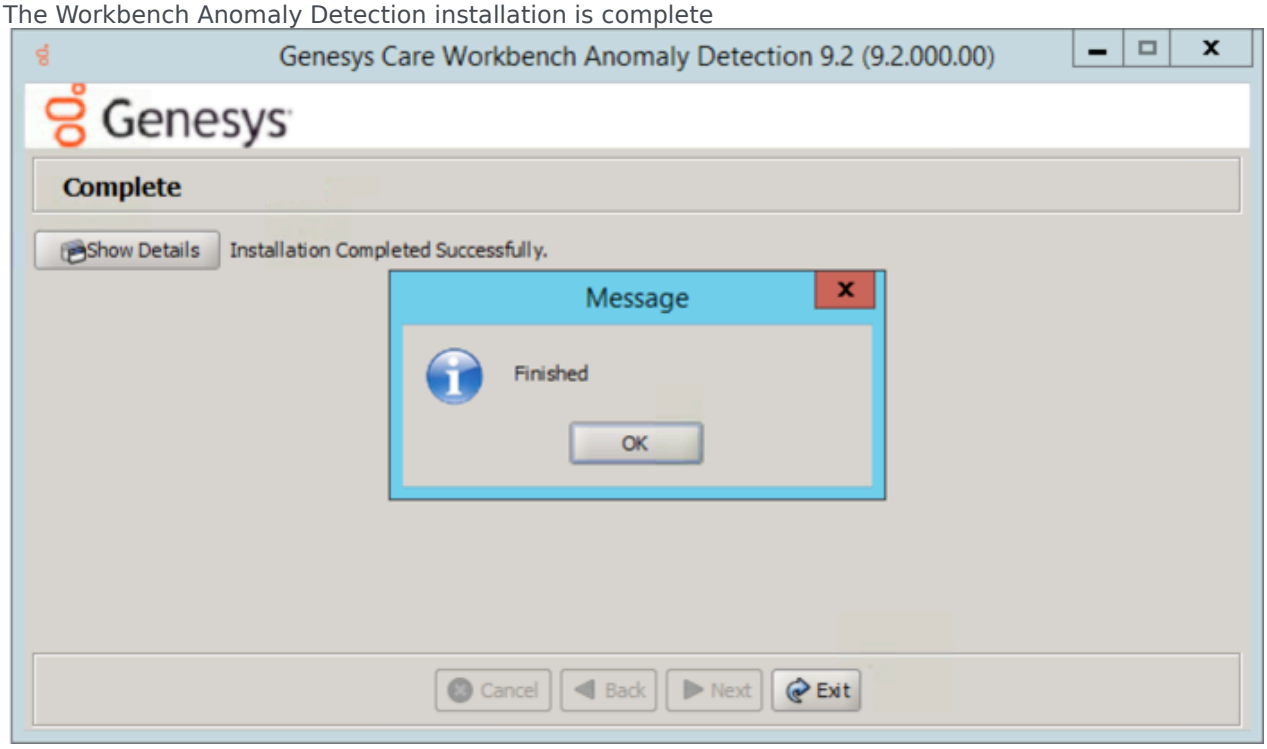
13. Select / provide the **Service Account** details for the Workbench components:



14. The Workbench Anomaly Detection installation will now progress



15. The Workbench Anomaly Detection installation is complete



Post Installation Steps

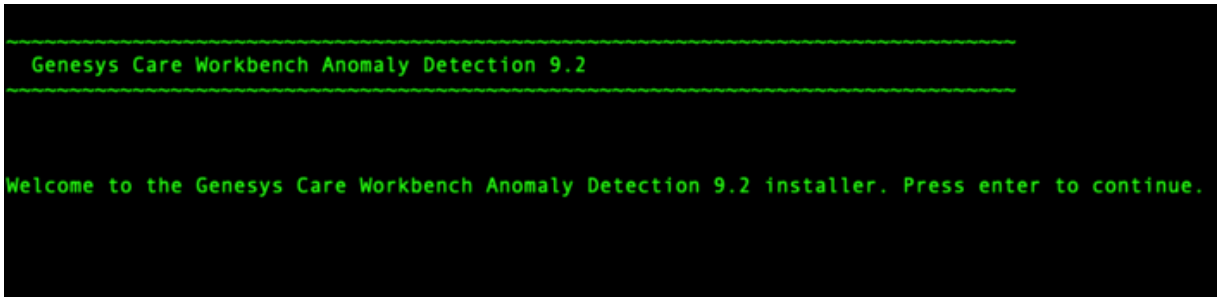
1. Validate if the AD primary components services are running:
    1. WB Anomaly Detection Node: **WB_AnomalyDetection_9.x.xxx.xx**
    2. WB Metricbeat: **WB_Metricbeat_9.x.xxx.xx**
    3. WB Agent: **WB_Agent_9.x.xxx.xx**
2. Validate if the new AD host appears in Workbench Applications as is presented in AD Configuration.
3. Follow the steps in Post Installation Configuration if needed.
4. If you are installing AD at first time, follow the guidelines given in Using AD to learn how to use Workbench Anomaly Detection Insights and its features.

AD Linux Install - Primary Node

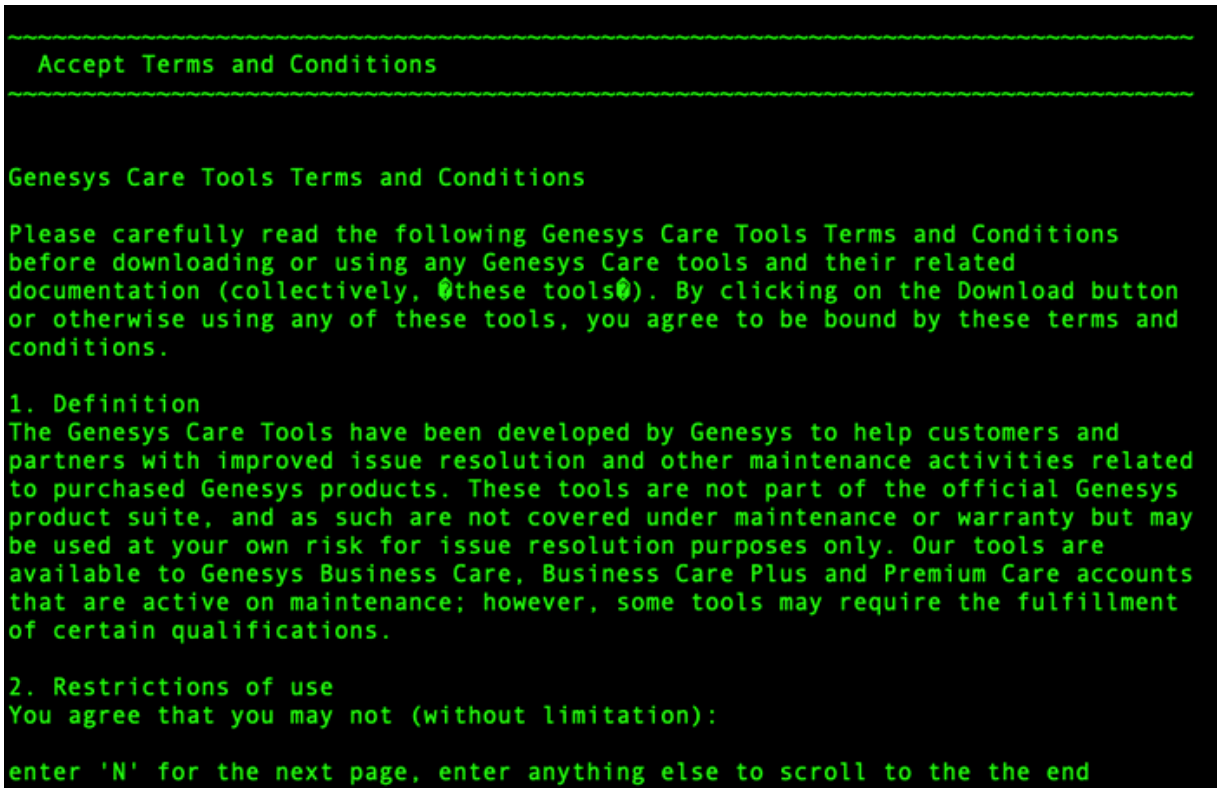
Review this link for details on downloading Workbench AD: Downloading Anomaly Detection (AD).

Please use the following steps to install Workbench AD **9.x.xxx.xx** on Linux:

1. Create a working directory (i.e. ~/tmp) adding the **AD_9.x.xxx.xx_LINUX.tar.gz** file
2. Run **tar zxf AD_9.x.xxx.xx_LINUX.tar.gz** to extract the downloaded *AD_Installer_Linux.tar.gz* compressed file.
3. Navigate into the **ip\linux** folder
4. Run **tar zxf AD_9.x.xxx.xx_Installer_Linux.tar.gz** to extract AD Installer content; the following files should be extracted:
    1. install.sh
    2. jdk-11.0.2/
    3. lib/
    4. AD_9.x.xxx.xx_Installer.jar
5. Run **./install.sh** (DO NOT prefix *./install.sh* with *sudo*)
6. Genesys Care Workbench Anomaly Detection - Installation
    - Press **Enter** on the **Genesys Care Workbench Anomaly Detection 9.x** screen to start the AD installation.

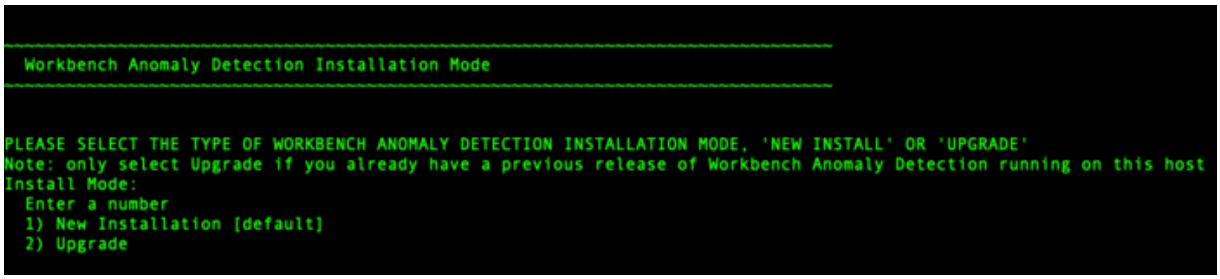


7. Genesys Workbench license agreement.
    - Press **Enter** to view the Genesys Workbench license agreement
8. Review license agreement
    - Enter **N** for the next page, or press anything else to scroll to the end of the Terms and Conditions

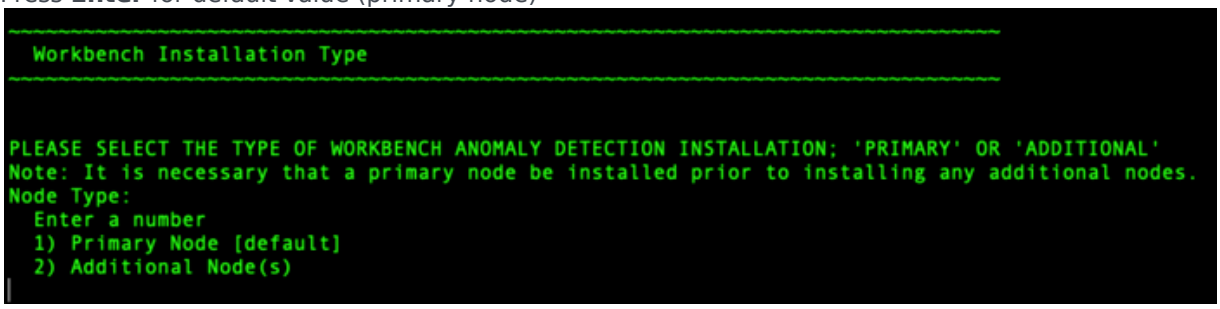


9. Genesys Workbench **Terms and Conditions**
    - If you agree to the Genesys Workbench Terms and Conditions, press **Enter** (default=Y) or enter **Y** to continue.
10. Workbench Installation Mode:
    - There are 2 Installation Modes:
        - **New Installation** - no Workbench Anomaly Detection components are yet running on this host/node
        - **Upgrade** - you already have Workbench Anomaly Detection running on this host/node and wish to upgrade
    - Press **Enter** for default value (new installation)

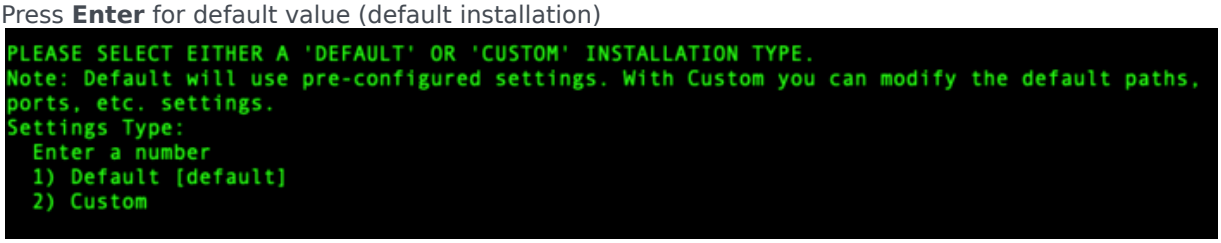
> ### Warning
> *AD currently does not support upgrade capability
> *Therefore select **New Installation** and not Upgrade during the AD 9.x.xxx.xx installation



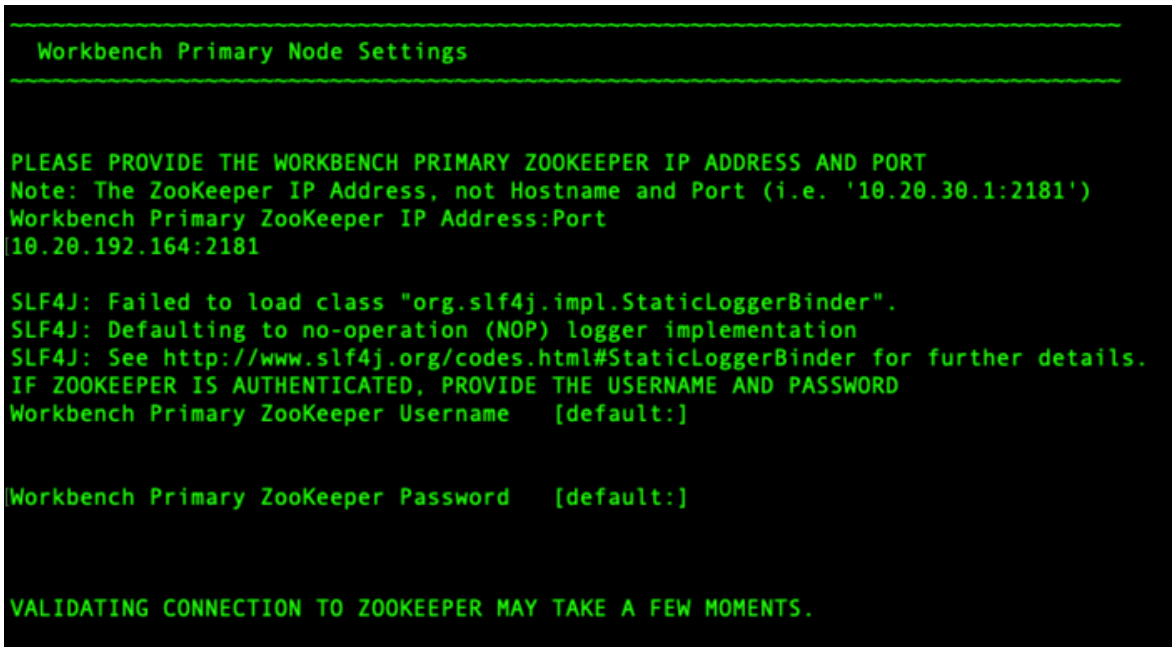
11. Workbench AD **Installation Type**
    - There are 2 Installation Types:
        - **Primary** - Anomaly Detection Node
        - **Additional** - Anomaly Detection Node used for distributing load. You already have Workbench Anomaly Detection Primary Node running in other host.
    - Press **Enter** for default value (primary node)



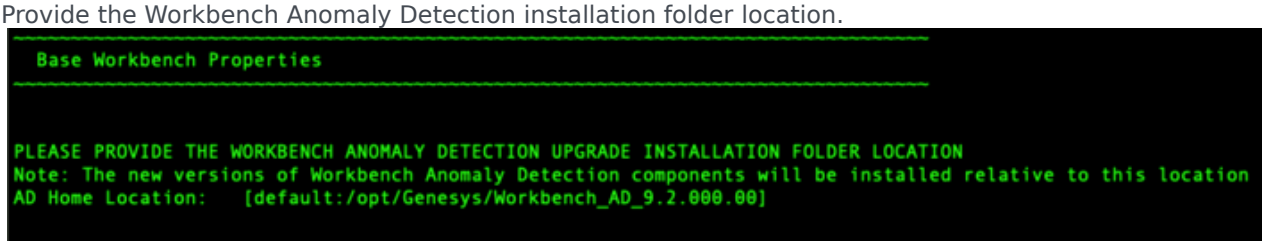
12. **DEFAULT** or **CUSTOM** installation
    - Install Workbench AD with Default or Custom settings:
        - **Default** - the respective Workbench AD **Default** settings will be used.
            - Default settings being installation paths, ports, etc.
        - **Custom** - or, if required, you can change the default settings by selecting a **Custom** install.
    - Press **Enter** for default value (default installation)



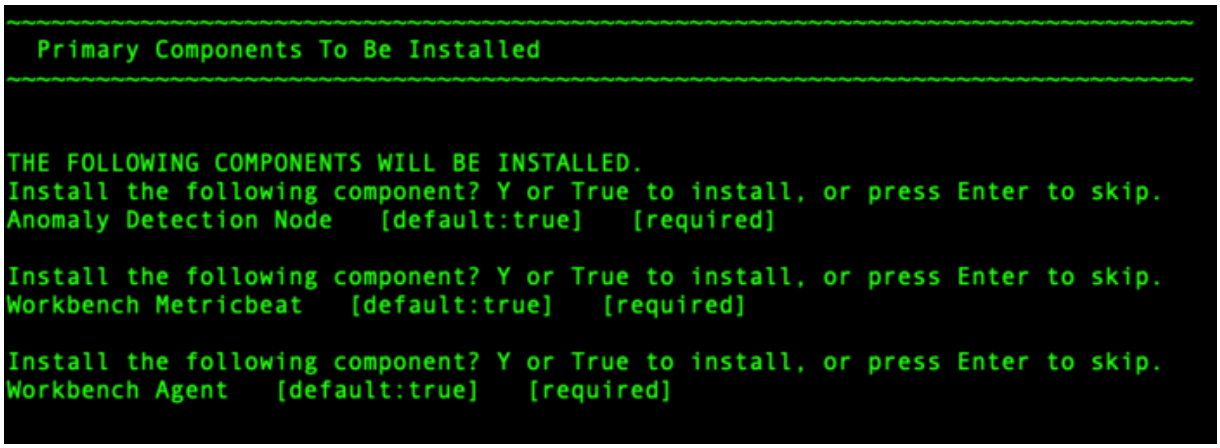
13. Provide the Workbench **Primary Zookeeper IP Address and Port**.
    - If Zookeeper is authenticated, provide username and password.
        - Simply press Enter for username/password if ZooKeeper authentication is disabled



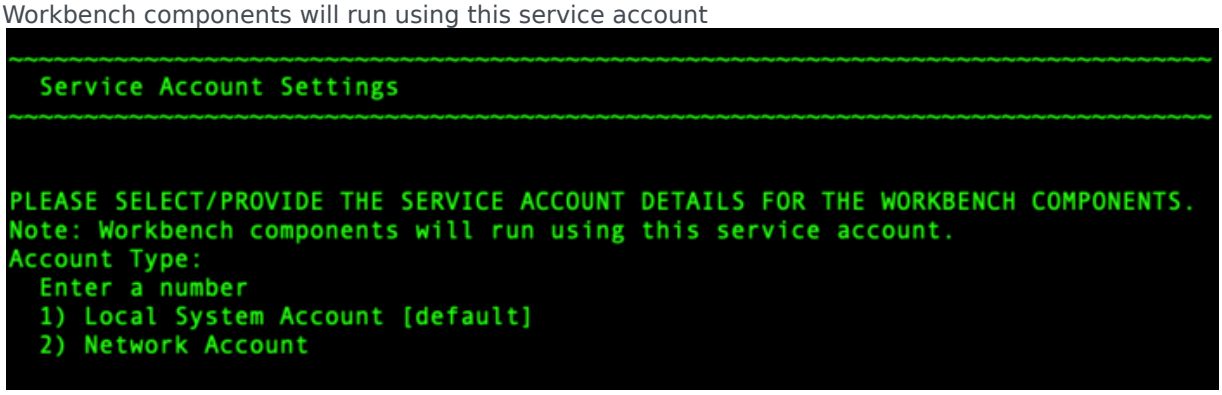
14. Provide the Workbench Anomaly Detection installation folder location.



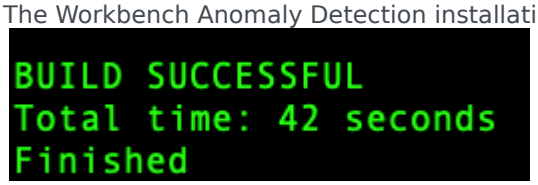
15. AD Hostname:
    - This Hostname will be utilized by the Workbench solution components.
16. Primary components to be installed: Information on which Workbench components are being installed on this host/node
    - Anomaly Detection Node
    - Workbench Metricbeat
    - Workbench Agent



17. Select / provide the **Service Account** details for the Workbench components:
    - Workbench components will run using this service account



18. The Workbench Anomaly Detection installation will now progress
19. The Workbench Anomaly Detection installation is complete



Post Installation Steps

1. Validate (i.e. service --status-all | grep WB) if the AD Primary component Services are running:
    1. WB Anomaly Detection Node: **WB_AnomalyDetection_9.x.xxx.xx**
    2. WB Metricbeat: **WB_Metricbeat_9.x.xxx.xx**
    3. WB Agent: **WB_Agent_9.x.xxx.xx**
2. Validate if the new AD host appears in Workbench/Configuration/Hosts as is presented in AD

Configuration.

3. Follow the steps in Post Installation Configuration if needed.
4. If you are installing AD at first time, follow the guidelines given in Using AD to learn how to use the Workbench Anomaly Detection Insights features.

Warning

- Post AD installation there is a 3 day training period before Insights are raised; during this time the Insights Console will display "No Insights Found!"

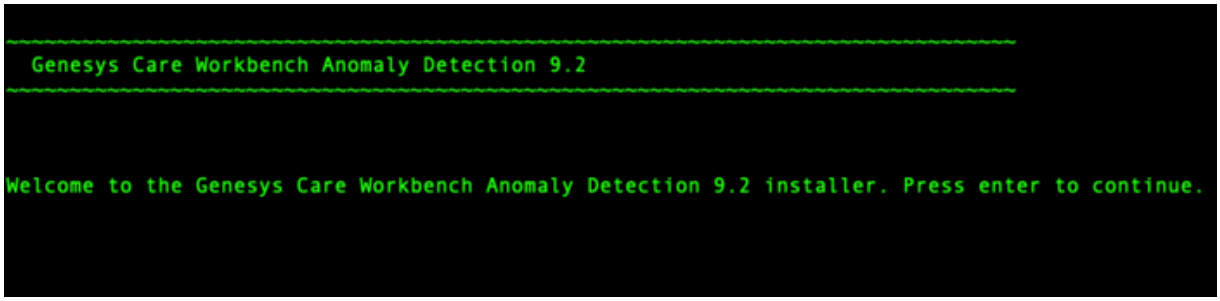
AD Linux Install - Additional Node

Review this link for details on downloading Workbench AD: Downloading Anomaly Detection (AD).

> **Important**
>
> - Ensure you have an installed and running AD Primary Node before installing any AD Additional Nodes

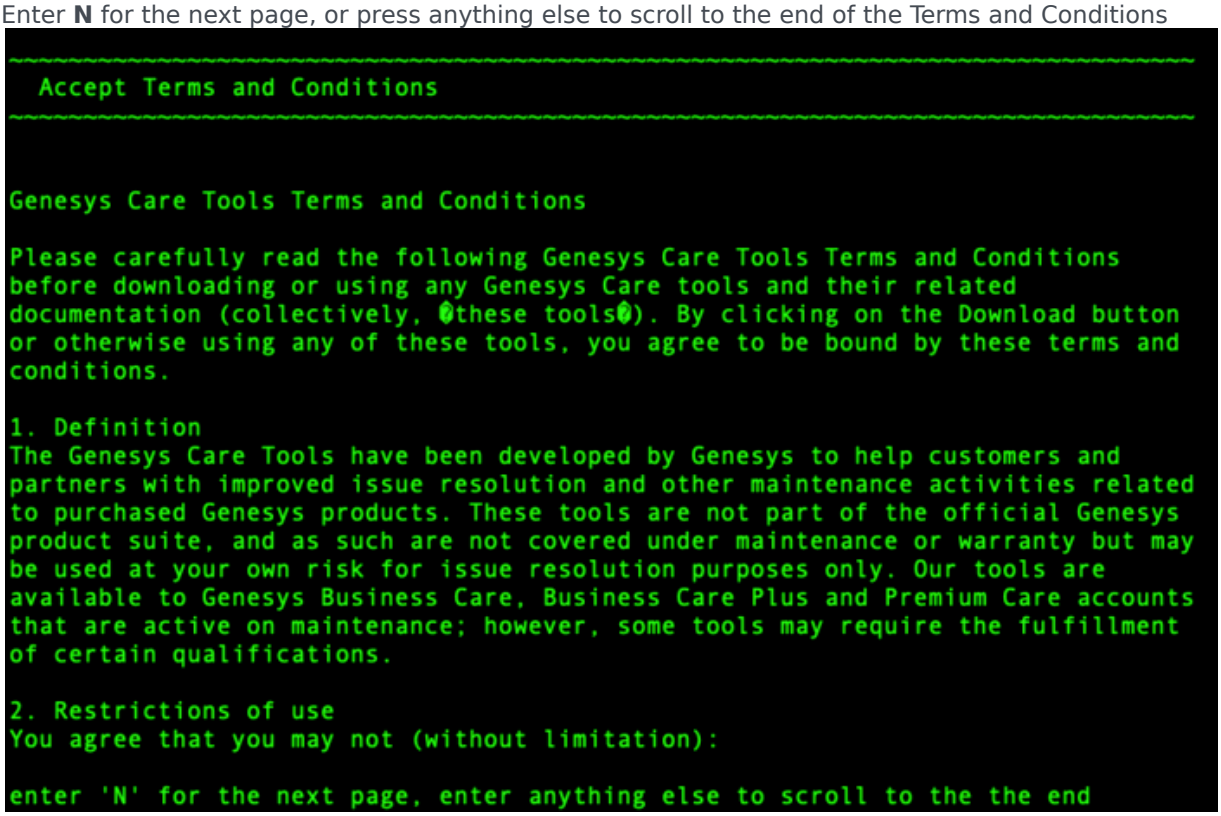
Please use the following steps to install Workbench AD **9.x.xxx.xx** on Linux:

1. Create a working directory (i.e. ~/tmp) adding the **AD_9.x.xxx.xx_LINUX.tar.gz** file
2. Run **tar zxf AD_9.x.xxx.xx_LINUX.tar.gz** to extract the downloaded *AD_Installer_Linux.tar.gz* compressed file.
3. Navigate into the **ip\linux** folder
4. Run **tar zxf AD_9.x.xxx.xx_Installer_Linux.tar.gz** to extract AD Installer content; the following files should be extracted:
    1. install.sh
    2. jdk-11.0.2/
    3. lib/
    4. AD_9.x.xxx.xx_Installer.jar
5. Run **./install.sh** (DO NOT prefix *./install.sh* with *sudo*)
6. Genesys Care Workbench Anomaly Detection - Installation
    - Press **Enter** on the **Genesys Care Workbench Anomaly Detection 9.x** screen to start the AD installation.

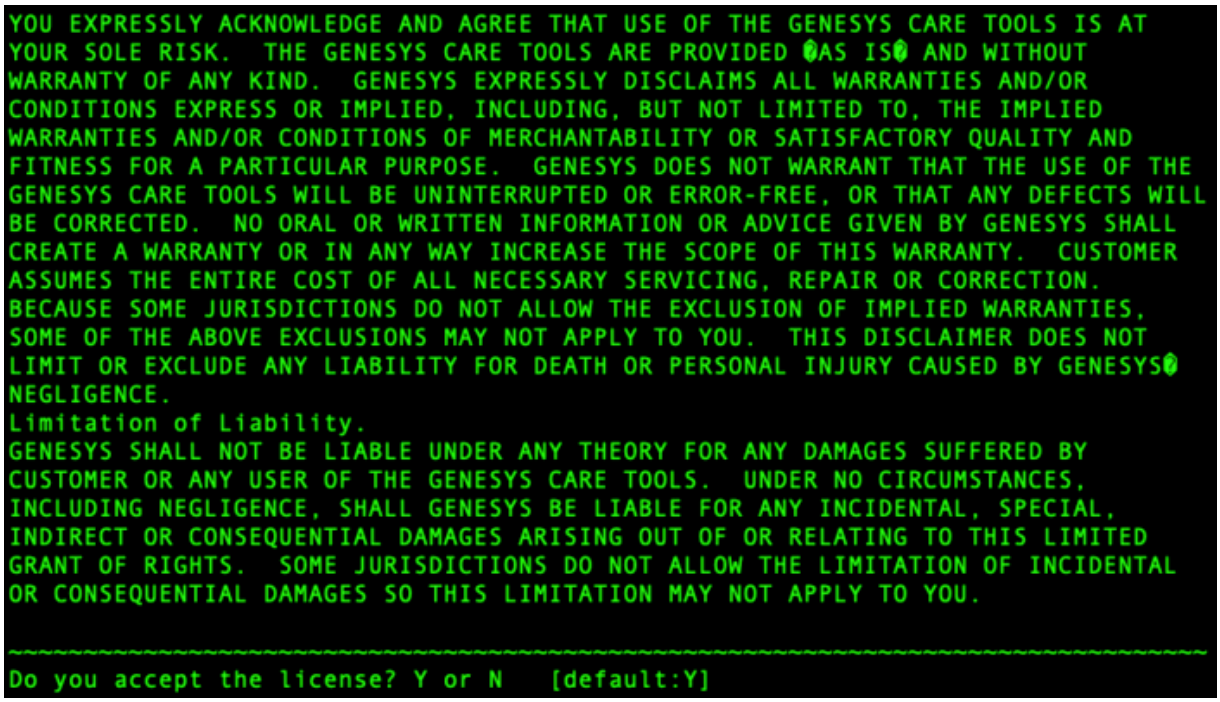


7. Genesys Workbench **License Agreement**
    - Press **Enter** to view the Genesys Workbench License Agreement
8. Review license agreement

- Enter **N** for the next page, or press anything else to scroll to the end of the Terms and Conditions

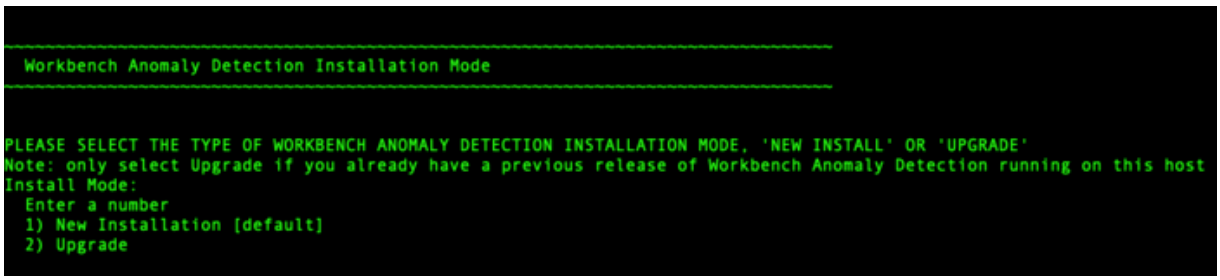


9. Genesys Workbench **Terms and Conditions**
   - If you agree to the Genesys Workbench Terms and Conditions, press **Enter** (default=Y) or enter **Y** to continue.



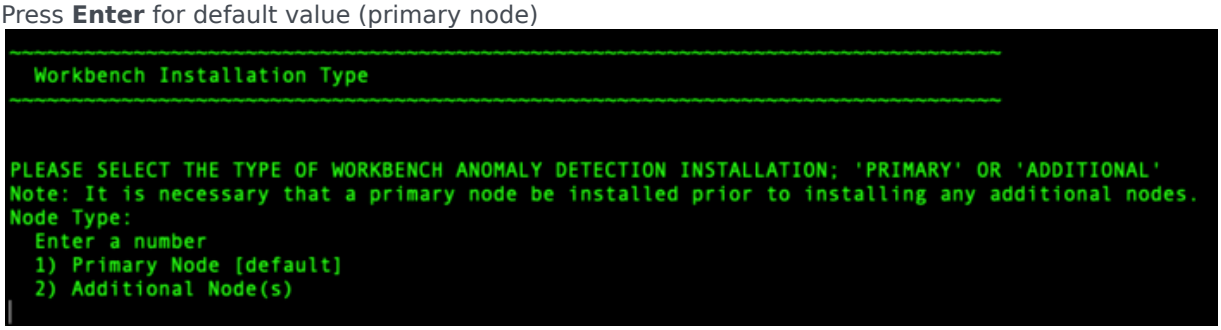
10. Workbench **Installation Mode**:
    - There are 2 Installation Modes:
      - **New Installation** - no Workbench Anomaly Detection components are yet running on this host/node
      - **Upgrade** - you already have Workbench Anomaly Detection running on this host/node and wish to upgrade
    - Press **Enter** for default value (new installation)

> **Warning**
> *AD currently does not support upgrade capability
> *Therefore select **New Installation** and not Upgrade during the AD 9.x.xxx.xx installation



11. Workbench AD **Installation Type**

- There are 2 Installation Types:
  - **Primary Node** - master Anomaly Detection Node
  - **Additional Node** - additional Anomaly Detection Node used for distributing load. You already have Workbench Anomaly Detection Primary Node running in other host.
- Press **Enter** for default value (primary node)



12. Continue with the next steps for both: **Primary or Additional** Node Installation.
13. **DEFAULT** or **CUSTOM** installationInstall Workbench AD with Default or Custom settings:
    - **Default** - the respective Workbench AD **Default** settings will be used.
      - default settings being paths, ports, etc.
    - **Custom** - or, if required, you can change the default settings by selecting a **Custom** install. In Custom mode, the following parameters are required:
      - For Workbench Anomaly Detection:
        - Binary files location
        - Configuration files location
        - Data files location
        - Log files location
        - Socket port
        - Incoming data port from Logstash
        - HTTP AD API port
      - For Workbench Metricbeat:
        - Binary files location
        - Data files location
        - Log files location
        - HTTP port
      - For Workbench Agent:
        - Binary files location
        - Log files location
        - HTTP port

```
PLEASE SELECT EITHER A 'DEFAULT' OR 'CUSTOM' INSTALLATION TYPE.
Note: Default will use pre-configured settings. With Custom you can modify the default paths,
ports, etc. settings.
Settings Type:
  Enter a number
  1) Default [default]
  2) Custom
```

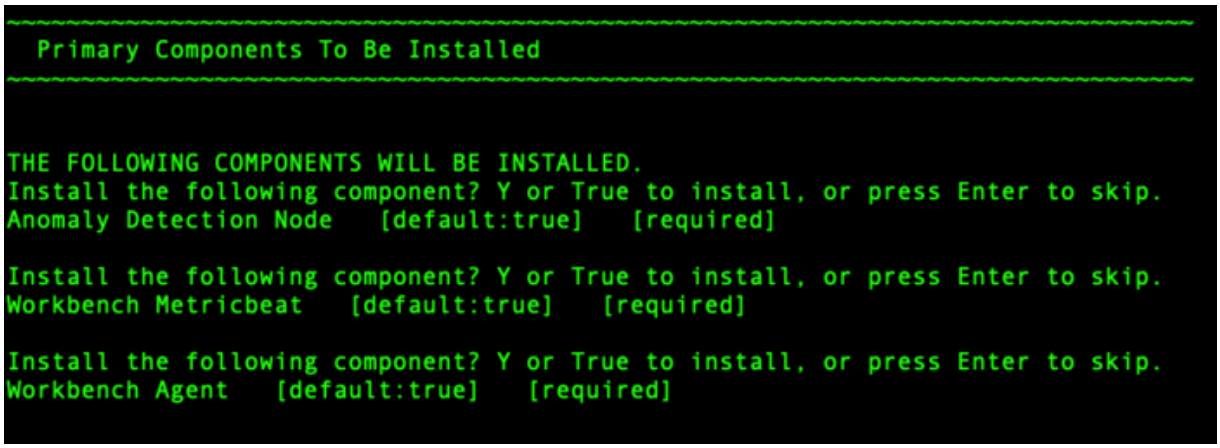
14. Provide the Workbench **Primary Zookeeper IP Address and Port**.
    - If Zookeeper is authenticated, provide username and password
      - Simply press Enter for username/password if ZooKeeper authentication is disabled

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Workbench Primary Node Settings
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE PROVIDE THE WORKBENCH PRIMARY ZOOKEEPER IP ADDRESS AND PORT
Note: The ZooKeeper IP Address, not Hostname and Port (i.e. '10.20.30.1:2181')
Workbench Primary ZooKeeper IP Address:Port    [default:]


IF ZOOKEEPER IS AUTHENTICATED, PROVIDE THE USERNAME AND PASSWORD
Workbench Primary ZooKeeper Username    [default:]


Workbench Primary ZooKeeper Password


SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.

VALIDATING CONNECTION TO ZOOKEEPER MAY TAKE A FEW MOMENTS.
```

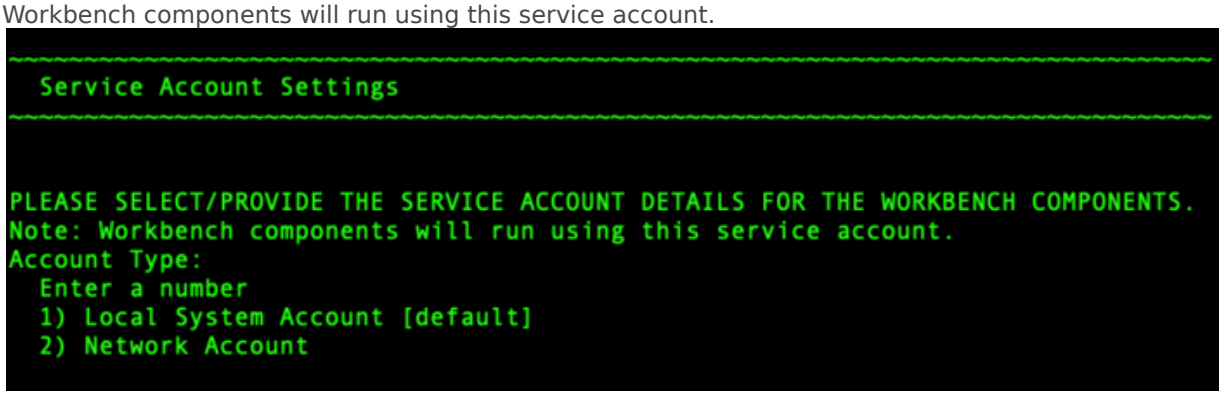
15. Provide the Workbench Anomaly Detection installation folder location:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  Base Workbench Properties
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


PLEASE PROVIDE THE WORKBENCH ANOMALY DETECTION INSTALLATION FOLDER LOCATION.
Note: All Anomaly Detection components will be installed relative to this location.
AD Home Location:    [default:/usr/local/Workbench_9.2.000.00]
```

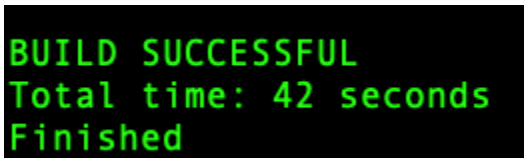
16. AD Hostname:AD Hostname:
    - This Hostname will be utilized by the Workbench solution components.
17. Primary components to be installed: Information on which Workbench components are being installed on this host/node
    - Anomaly Detection Node
    - Workbench Metricbeat
    - Workbench Agent



18. Select / provide the **Service Account** details for the Workbench components:
    - Workbench components will run using this service account.



19. The Workbench Anomaly Detection installation will now progress
20. The Workbench Anomaly Detection installation is complete



Post Installation Steps

1. Validate (i.e. service --status-all | grep WB) if the AD Additional component Services are running:
    1. WB Anomaly Detection Node: **WB_AnomalyDetection_9.x.xxx.xx**
    2. WB Metricbeat: **WB_Metricbeat_9.x.xxx.xx**
    3. WB Agent: **WB_Agent_9.x.xxx.xx**
2. Validate if the new AD host appears in Workbench/Configuration/Hosts as is presented in AD Configuration.

3. Follow the steps in Post Installation Configuration if needed.
4. If you are installing AD at first time, follow the guidelines given in Using AD to learn how to use the Workbench Anomaly Detection Insights features.

AD Post Installation Configuration

Genesys recommended post Anomaly Detection (AD) installation steps:

> **Important**
>
> - The Workbench Anomaly Detection installation uses the Ant Installer component, if during the AD installation a Network Account install is selected, the Ant Installer prints the username and password details to the "ant.install.log" file. Genesys therefore recommends, post installation, at a minimum the "ant.install.log" file be manually edited and the password be masked/deleted.

For all other configuration options, please refer to the section Anomaly Detection Configuration Options

AD Data-Center Synchronization

Important

- All AD related data including anomalies, events, notifications are available across all Workbench Data-Centers and follow the same principle as standard data synchronization in Workbench.
- To ensure all data is properly synchronized across Workbench Data-Centers please follow the steps outlined in Workbench Data-Center Sync
- Once the Workbench Data-Centers are sync'd/linked, existing data will be synchronized and any new data will be replicated to all Workbench Data-Centers.
- If AD is currently installed in one or more Data-Center(s) and an AD node it being added to an additional data-center for the first time, it is recommended to close all existing insights in the environment to ensure syncing consistently across the data-centers.

AD Deployment Upgrade

Important

- The Anomaly Detection 9.2.000.10 components do not support an upgrade capability - please either:
  - a) remain running AD 9.2.000.00 but follow the Workbench Agent 9.2.000.00 log4j vulnerability mitigation steps here: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/KnownIssuesandLimitations

or

- b) un-install AD 9.2.000.00 and re-install the Anomaly Detection 9.2.000.10 components

AD Pre-Upgrade Steps

Important

- The Anomaly Detection 9.2.000.10 components do not support an upgrade capability - please either:
  - a) remain running AD 9.2.000.00 but follow the Workbench Agent 9.2.000.00 log4j vulnerability mitigation steps here: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/KnownIssuesandLimitations

or

- b) un-install AD 9.2.000.00 and re-install the Anomaly Detection 9.2.000.10 components

AD Windows Upgrade - Primary and Additional Node

Important

- The Anomaly Detection 9.2.000.10 components do not support an upgrade capability - please either:
  - a) remain running AD 9.2.000.00 but follow the Workbench Agent 9.2.000.00 log4j vulnerability mitigation steps here: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/KnownIssuesandLimitations

or

- b) un-install AD 9.2.000.00 and re-install the Anomaly Detection 9.2.000.10 components

AD Linux Upgrade - Primary and Additional Node

Important

- The Anomaly Detection 9.2.000.10 components do not support an upgrade capability - please either:
  - a) remain running AD 9.2.000.00 but follow the Workbench Agent 9.2.000.00 log4j vulnerability mitigation steps here: https://docs.genesys.com/Documentation/ST/latest/WorkbenchUG/KnownIssuesandLimitations

or

- b) un-install AD 9.2.000.00 and re-install the Anomaly Detection 9.2.000.10 components

Using AD

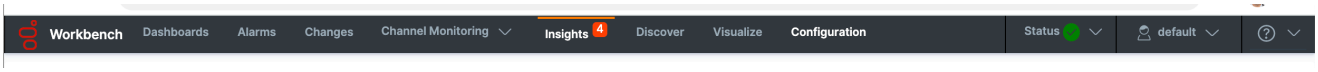
This Anomaly Detection (AD) Insights section contains information on the use and configuration of Workbench Anomaly Detection Insights and its features thereof.

This section provides the following information:

- AD Navigation Bar
- AD Insights Console
- AD Dashboards
- AD Visualizations
- AD Configuration

AD Navigation Bar

The Workbench top navigation bar provides the below highlighted "Insights" menu item for the Anomaly Detection feature, click this Insights link for the Anomaly Detection Insights Console.



Note: The  Insights menu badge displays the overall active Insights count for an holistic (i.e. the cumulative count for all Workbench Data-Centers) view.

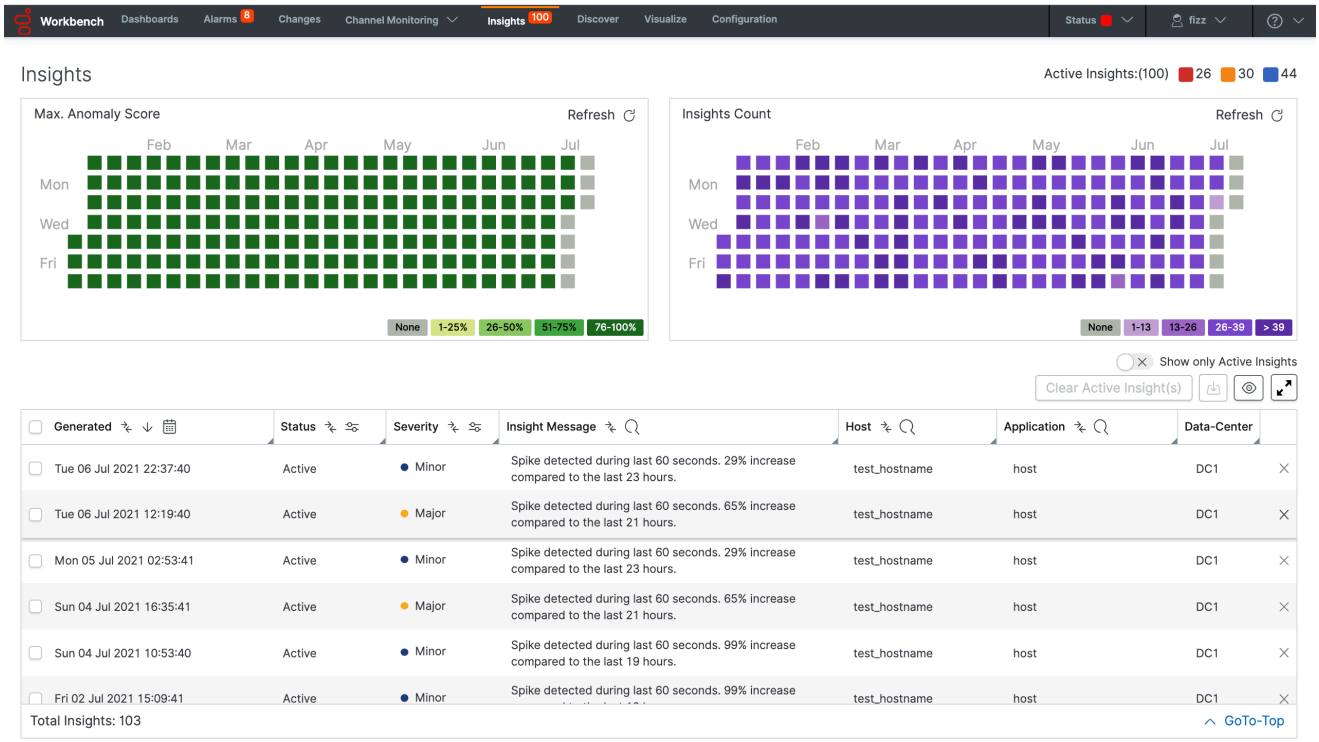
AD Insights Console

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.

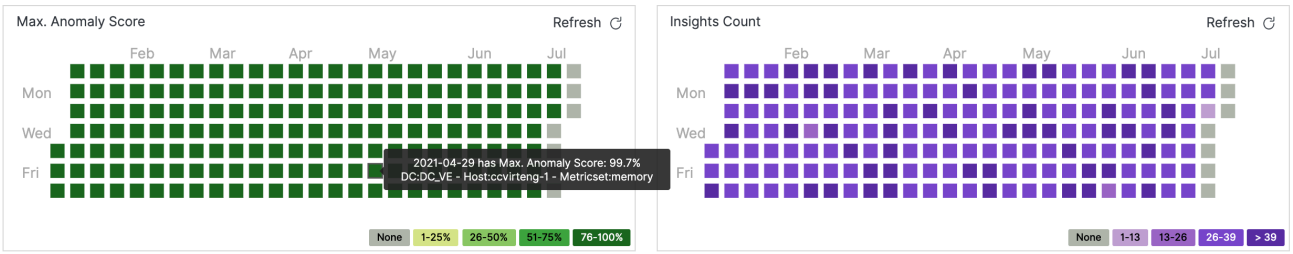


Statistics Summary

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.

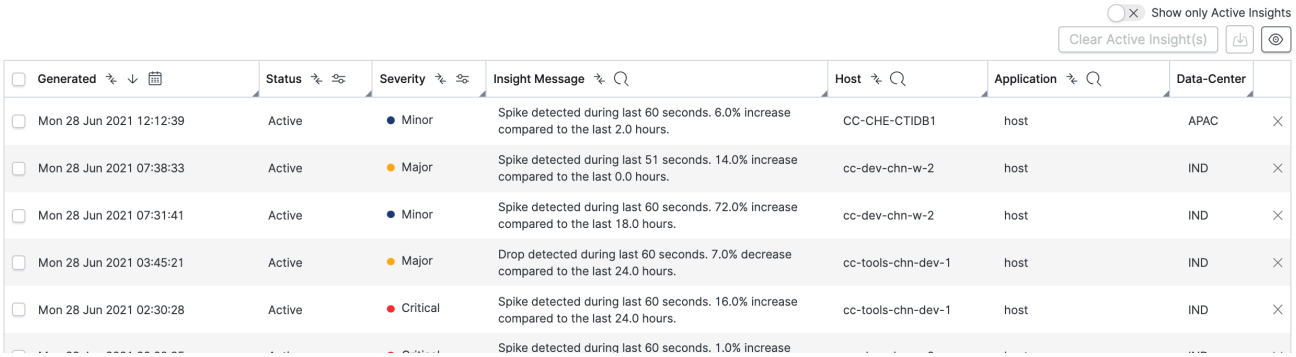
Each square shows the date and the number of Insights detected that day; the ranges are calculated based on the maximum value detected during the last 6 months.

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%.



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

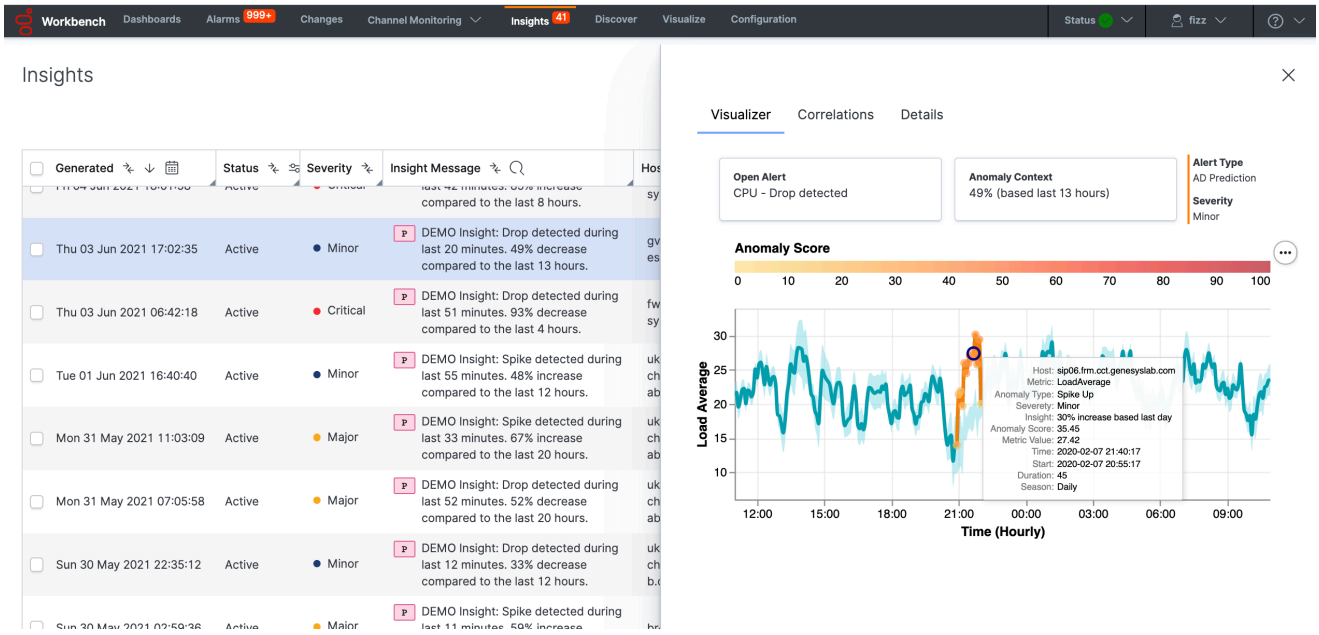
- Show Only Active Insights: a toggle filter to show only the active Insights

- 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.



Visualizer

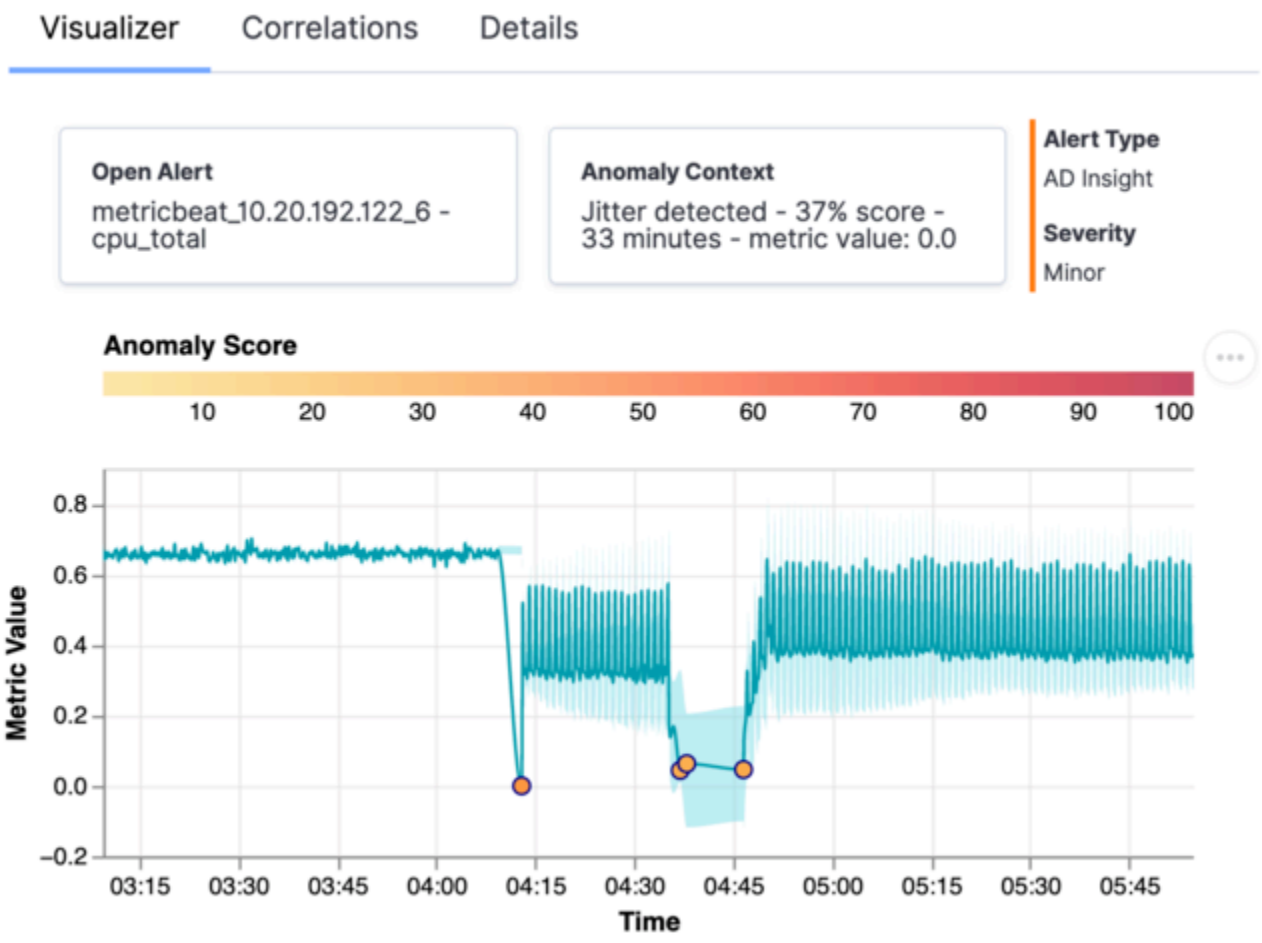
Display Insights context in graphical view. Main Sections:

- 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.

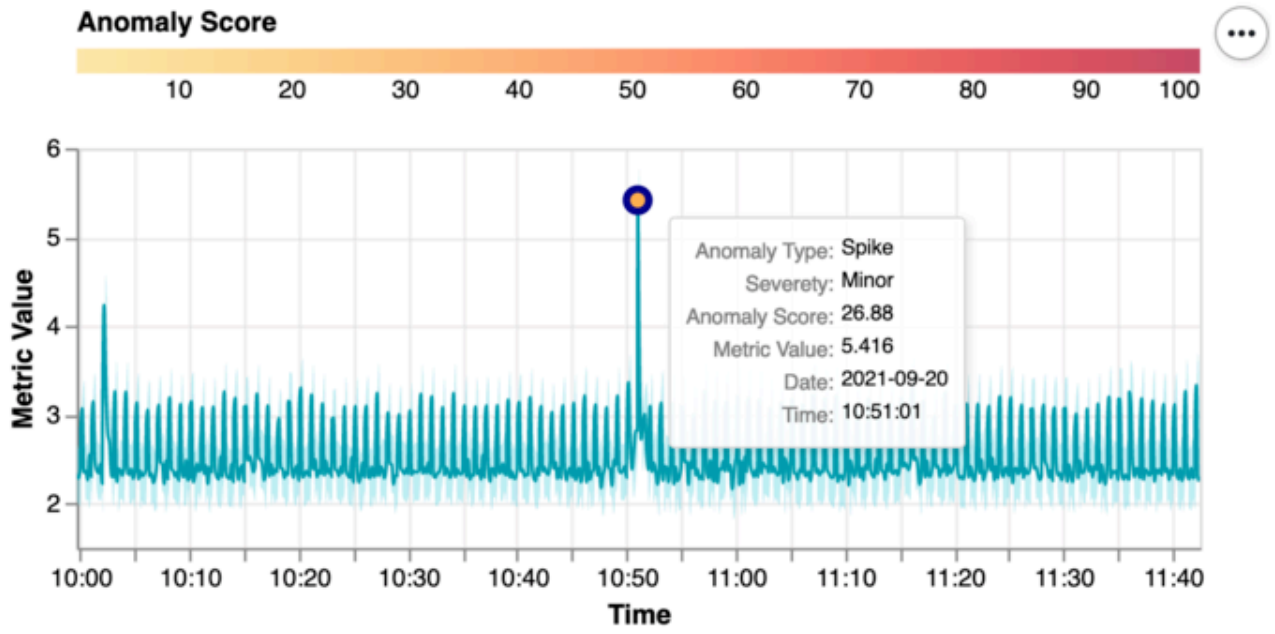
- Insight duration is defined as the time between the first and last anomaly point in the same hour; when this time is smaller than 15 minutes it will be displayed in seconds.

- 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

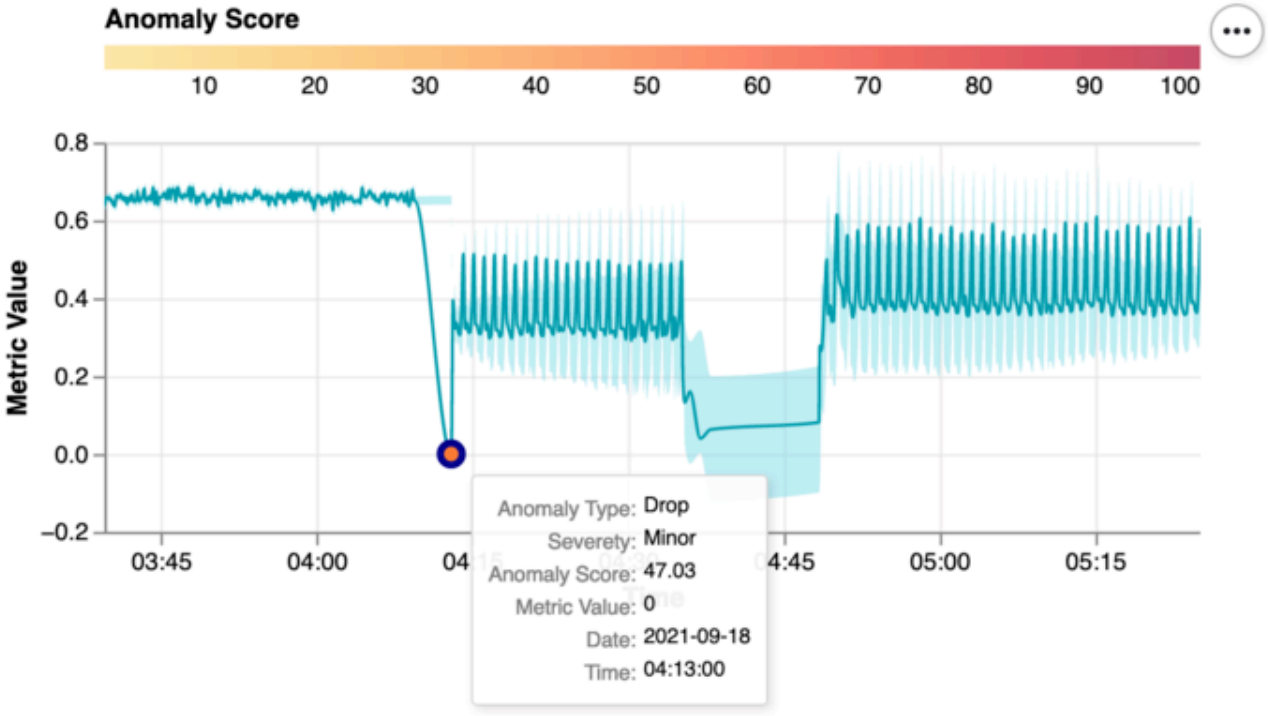


AD is able to detect four types of anomalies:

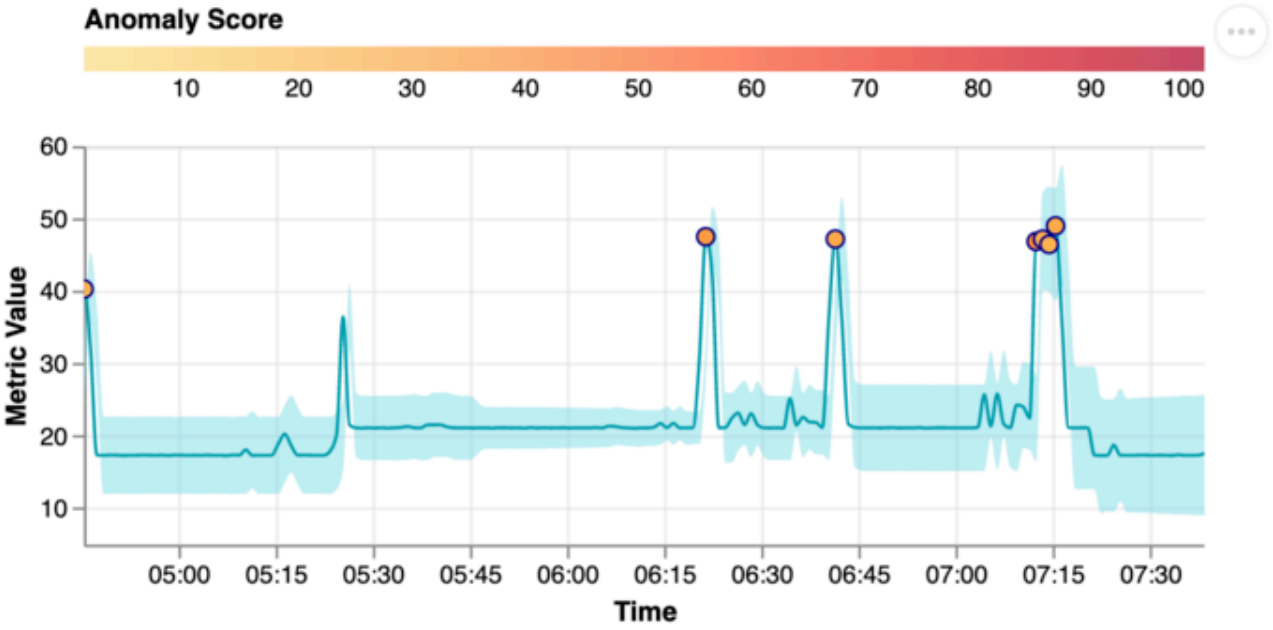
- Spike: is considered as an acute increase in the metric value followed by an immediate return to the underlying level.



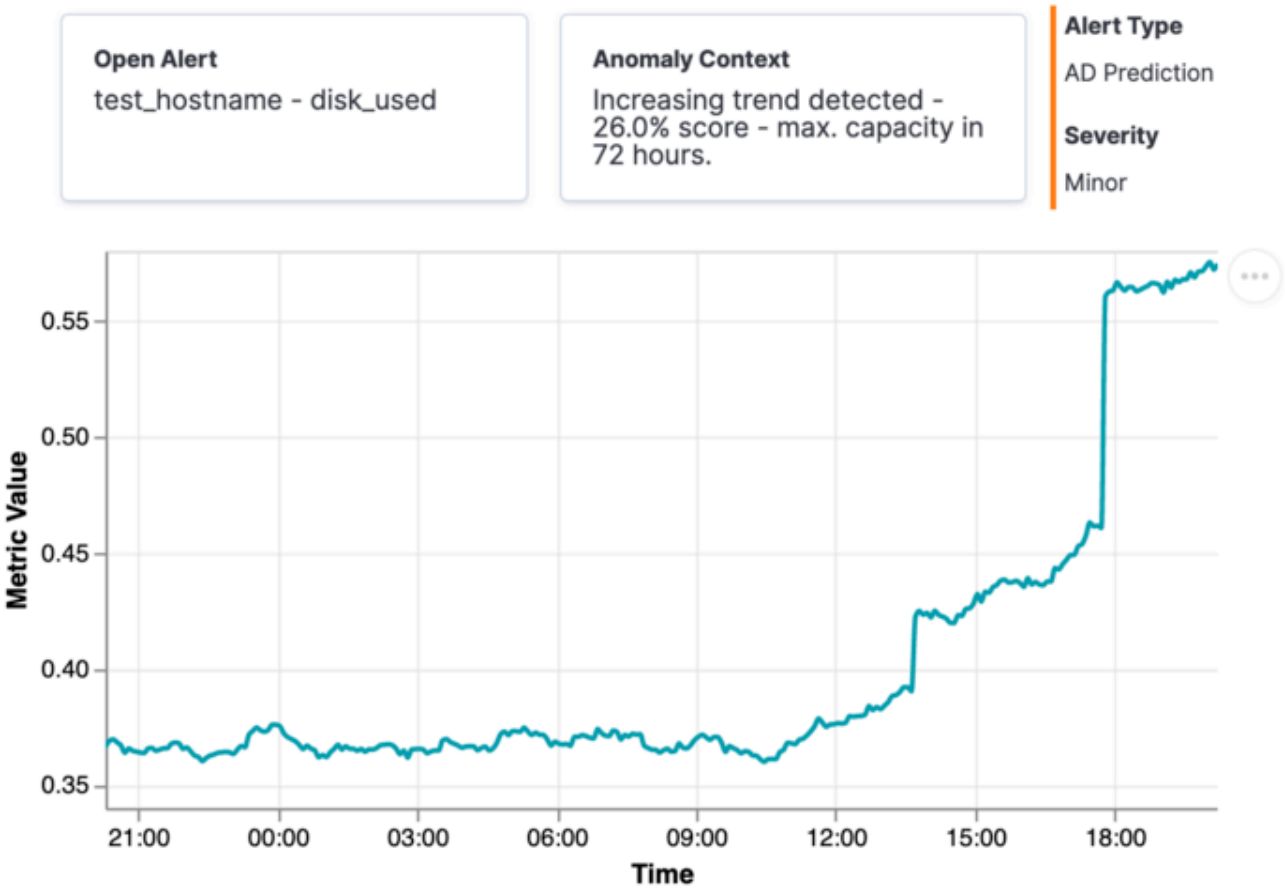
- Drop:is considered as an acute decrease in the metric value followed by an immediate return to the underlying level.



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



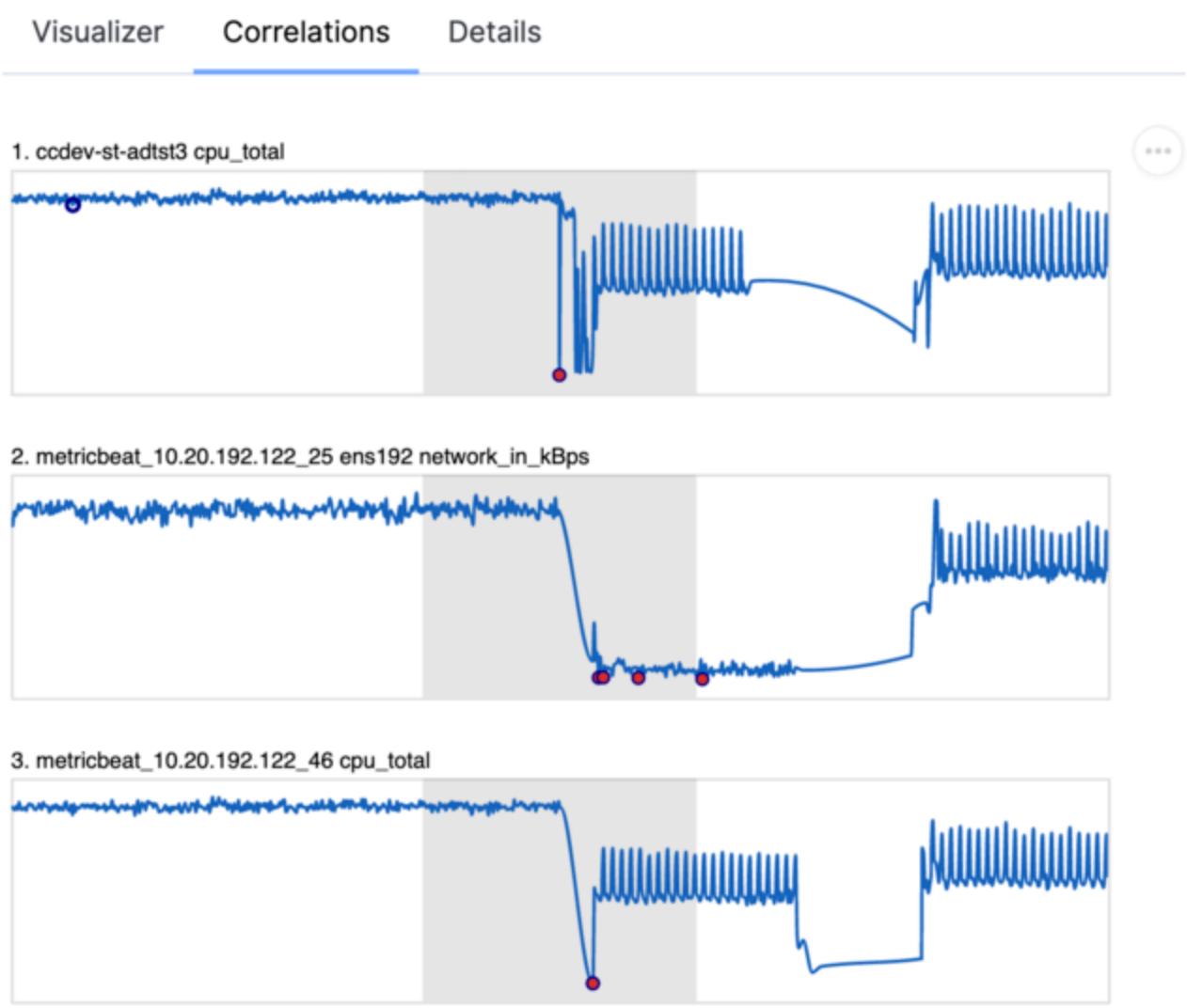
- Trend Prediction: Insights generated based on hourly trend predictions.
  - A new insight is generated when high values are (> 95%) predicted in the next hours [0 - 72 hours]
  - Score give an indication of the metric rate of change.
  - Because these insights are based on predictions, these don't 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.

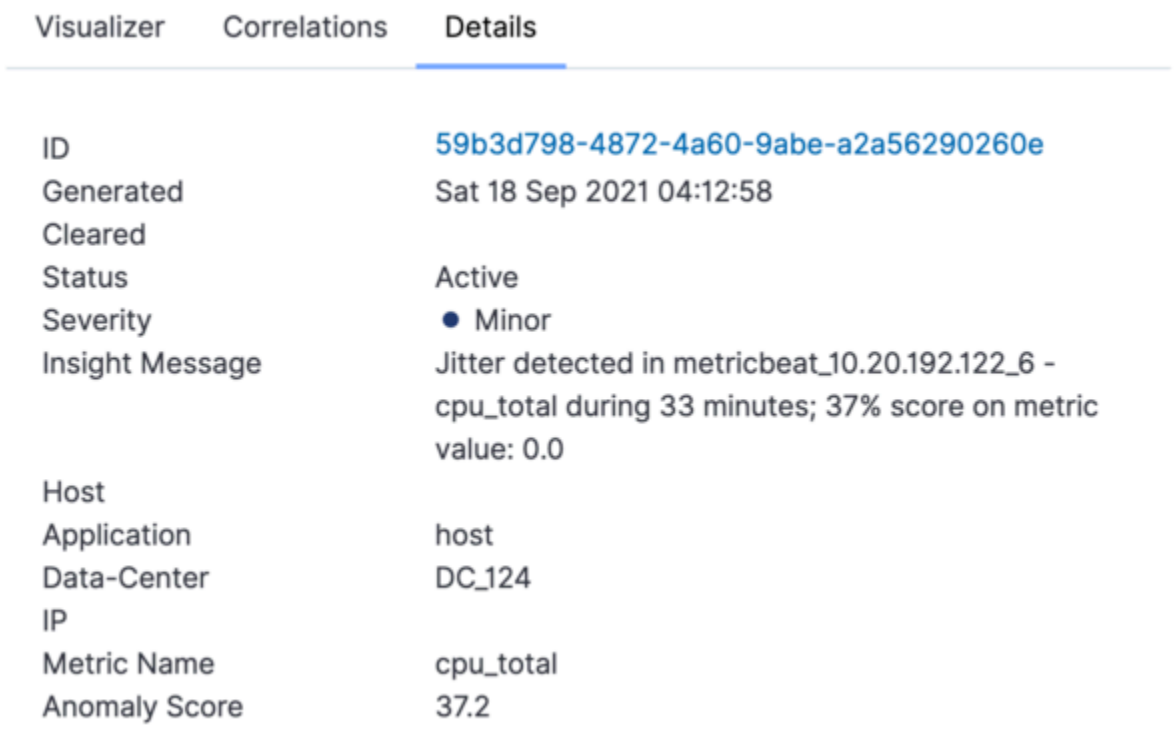


Details

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

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



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.

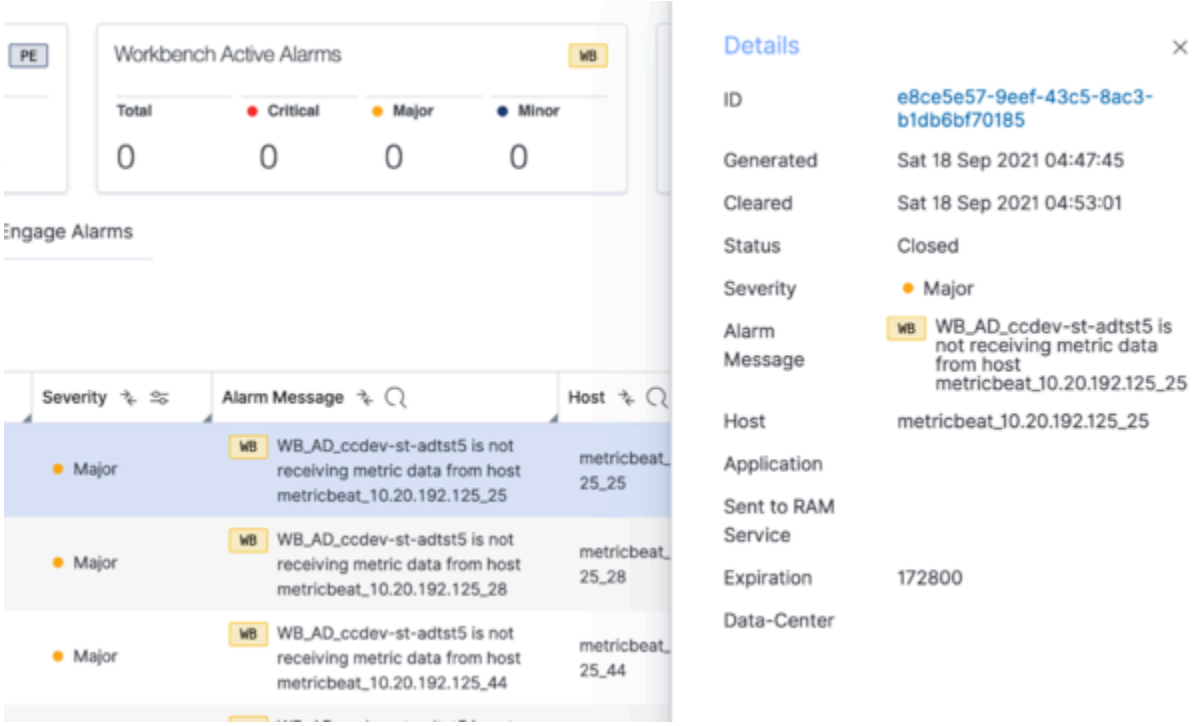
- Severity: Critical
- Structure: {ad_appname} is not receiving metric data from Logstash
- Suggested Actions: validate if Logstash is receiving data from Metricbeats or all Metricbeats are down.

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.

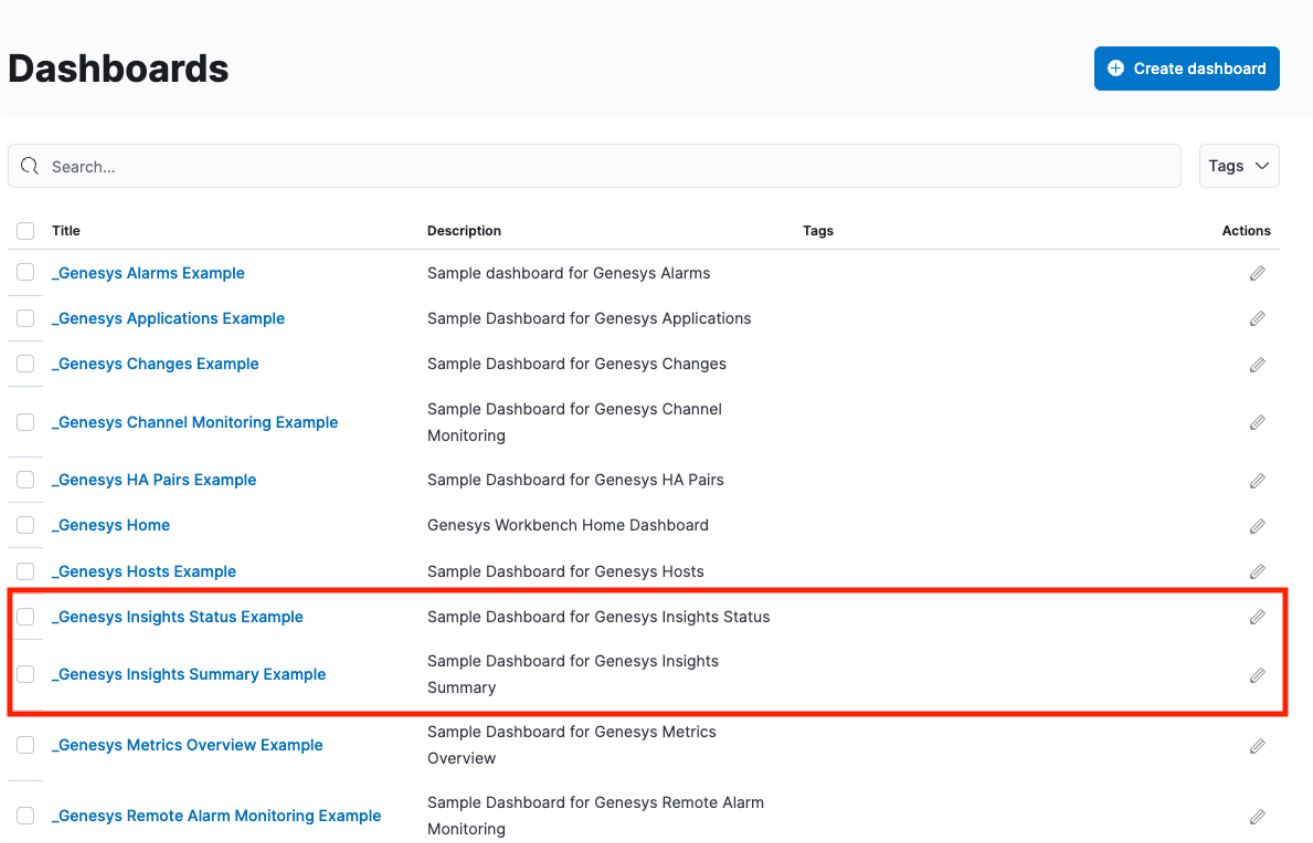
- Severity: Critical
- Structure: AD Node {ad_node_name} is down
- Suggested Actions: validate if that specific host is down.



AD Dashboards

Installing the Workbench Anomaly Detection feature enables two additional example Dashboards in Workbench.

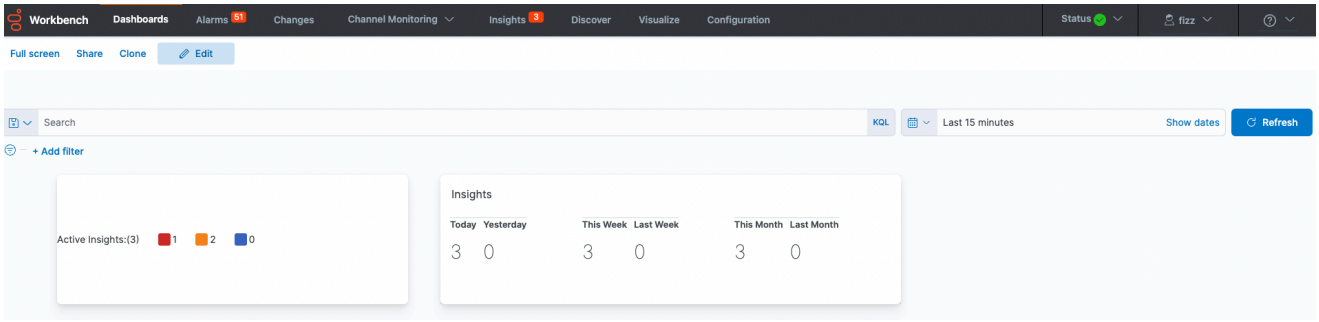
These example Dashboards provide an at-a-glance view of **AD Insights Summary** and **AD Component Status** details.



_Genesys Insights Summary Example Dashboard

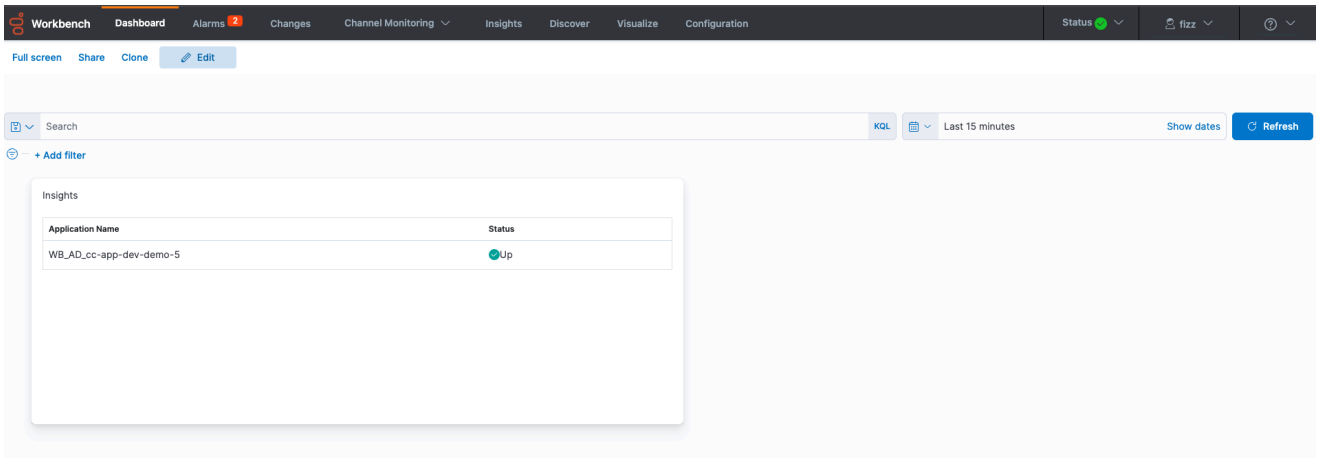
This example dashboard includes the following real-time Visualizations:

- _Genesys_Insights_Summary - a view of Active *Critical*, *Major* and *Minor* Insights
- _Genesys_#_of_Insights_Summary - a view of Insights raised *Today/Yesterday*, *This Week/Last Week* and *This Month/Last Month*



_Genesys_Insights_Status Example Dashboard

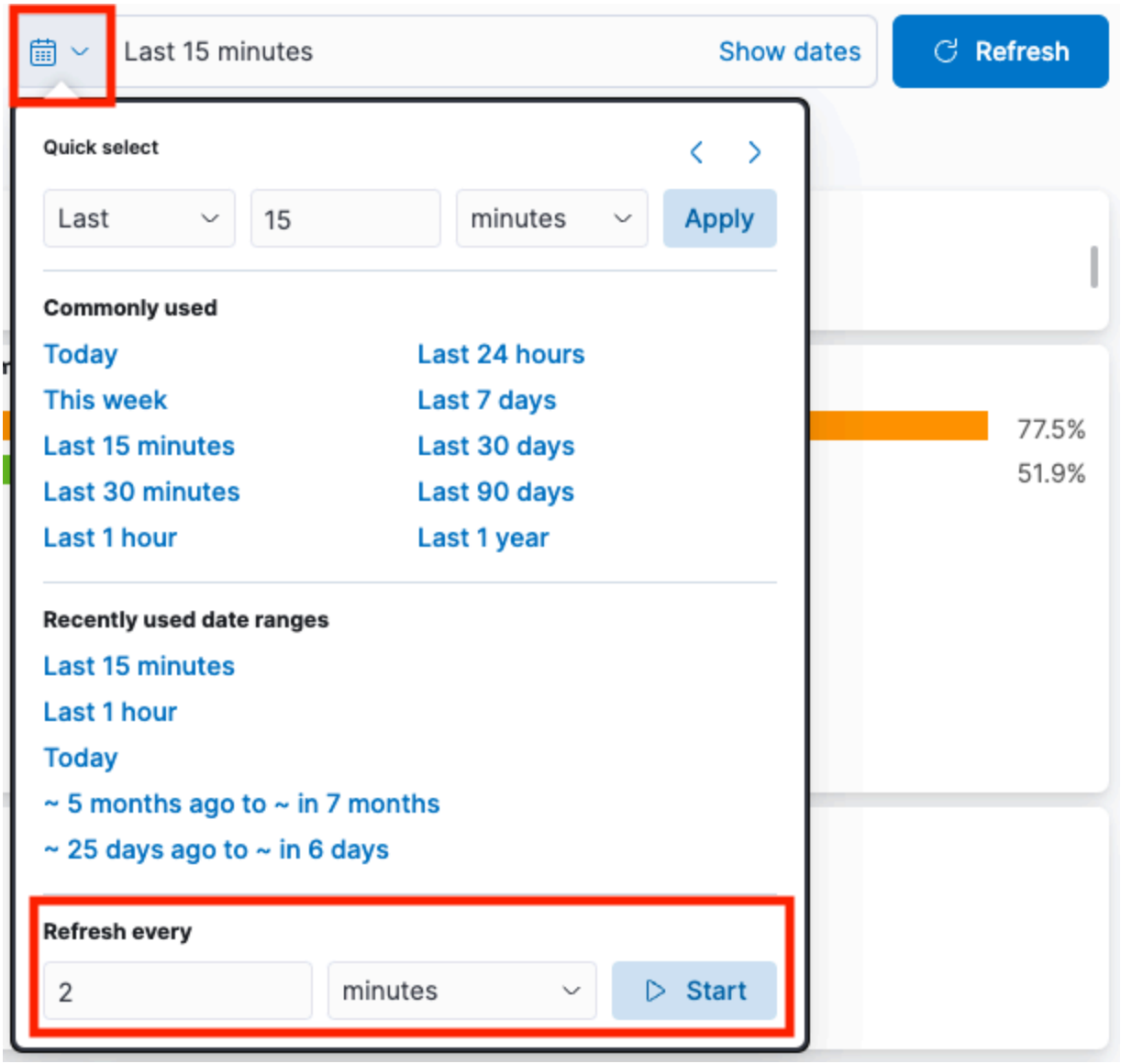
This example dashboard includes an AD Insights component *Status* Visualization to show the real-time status of the AD component(s).



Considerations

Important

- From WB 9.3+ the Dashboards/Visualizations do not update by default in real-time
- Use the 'Quick Select' feature below to 'Start' auto Refresh functionality of Dashboards/ Visualizations



Important

- For Workbench 9.2 to 9.3 upgrades, existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
- The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
- As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/ message will be displayed
- Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

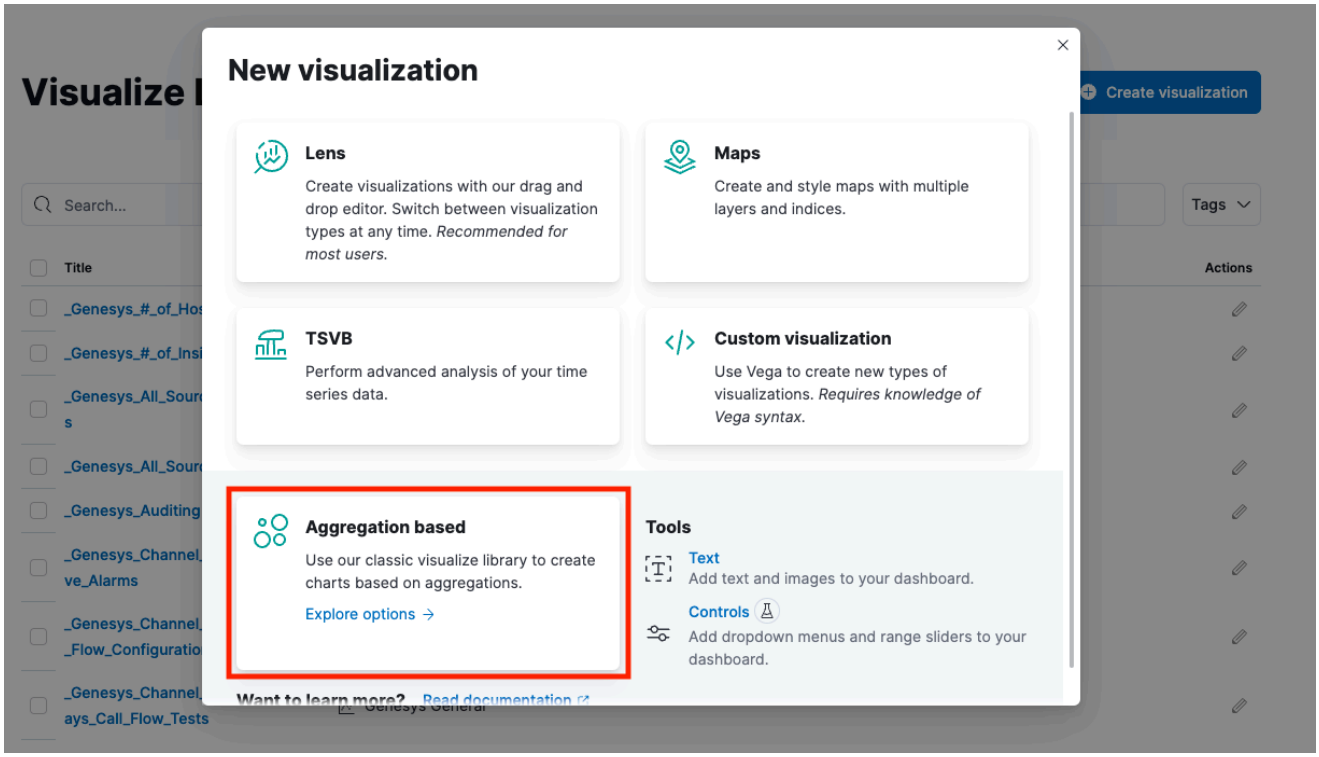
Important

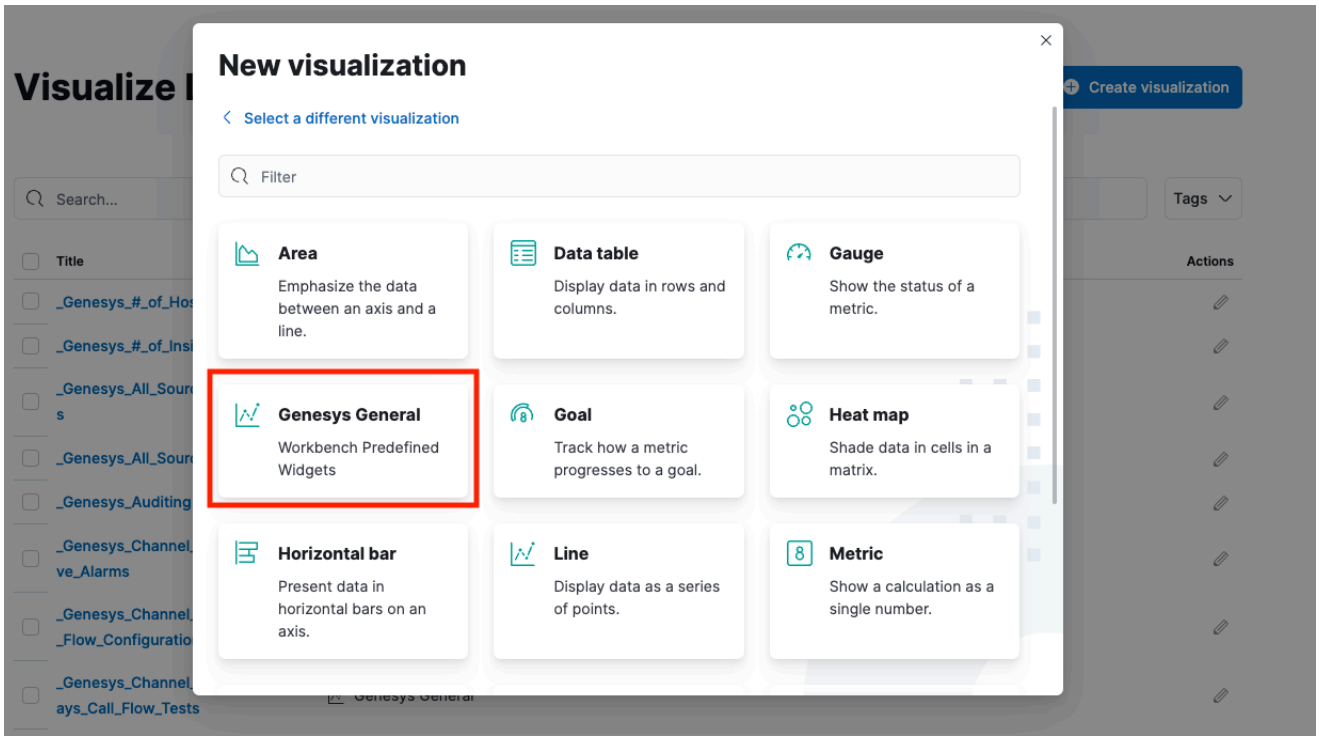
- For detailed documentation about creating/customize your own Dashboards, please review the Dashboards section

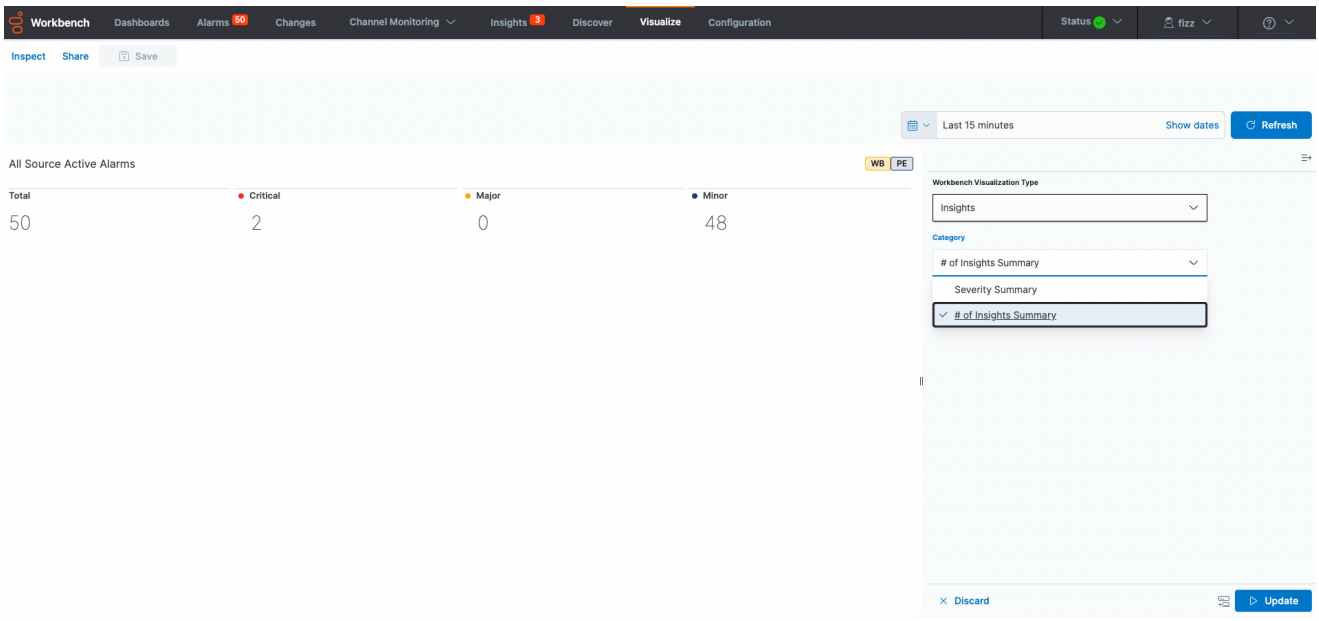
AD Visualizations

The AD Insights feature enables the following additional real-time Visualizations under **Genesys General** Type.

- _Genesys_#_of_Insights_Summary
- _Genesys_Insight_Summary
- _Genesys_Insights_Status

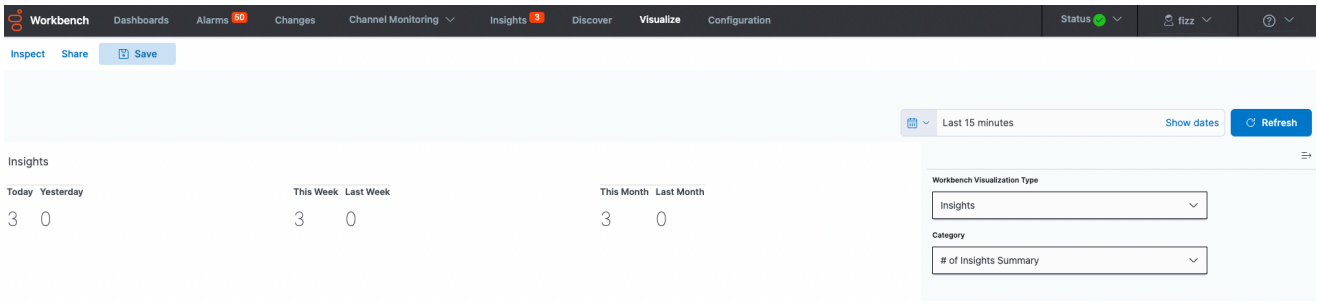






Genesys#_of_Insights_Summary Visualization

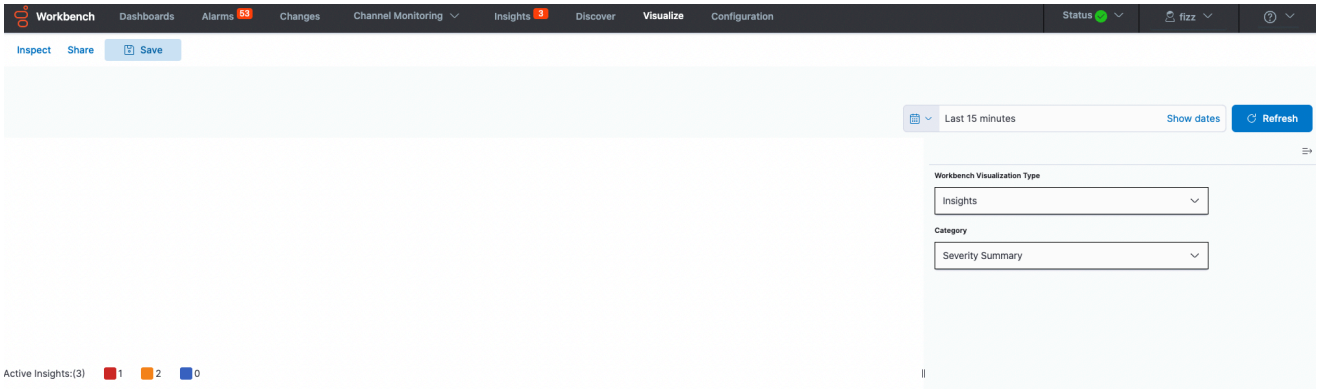
This Vizualization displays the real-time **Statistical Summary** of detected Insights/Anomalies; in a *Today*, *Yesterday*, *This Week*, *Last Week*, and *This Month* and *Last Month* format.



_Genesys_Insight_Summary Visualization

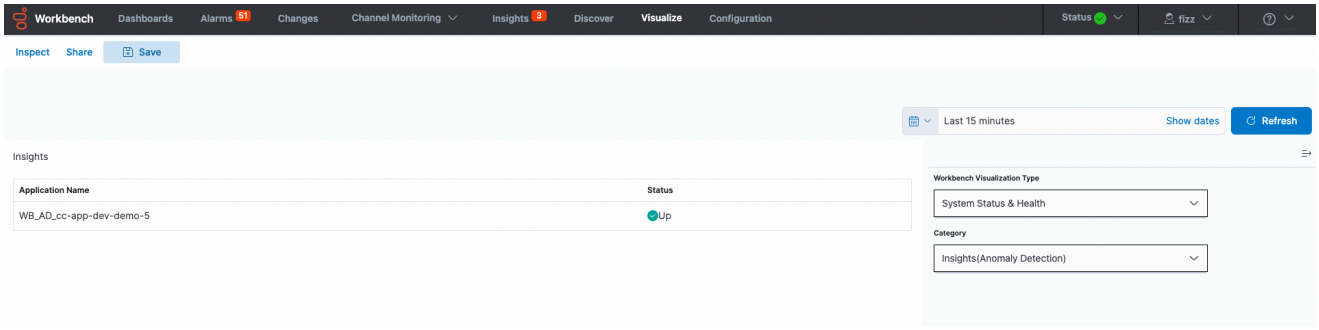
This real-time Visualization displays **Active Insights/Anomalies Summary** details; in a *Critical*, *Major*, *Minor* format.

Note: - Critical, - Major, - Minor



_Genesys_Insights_Status Visualization

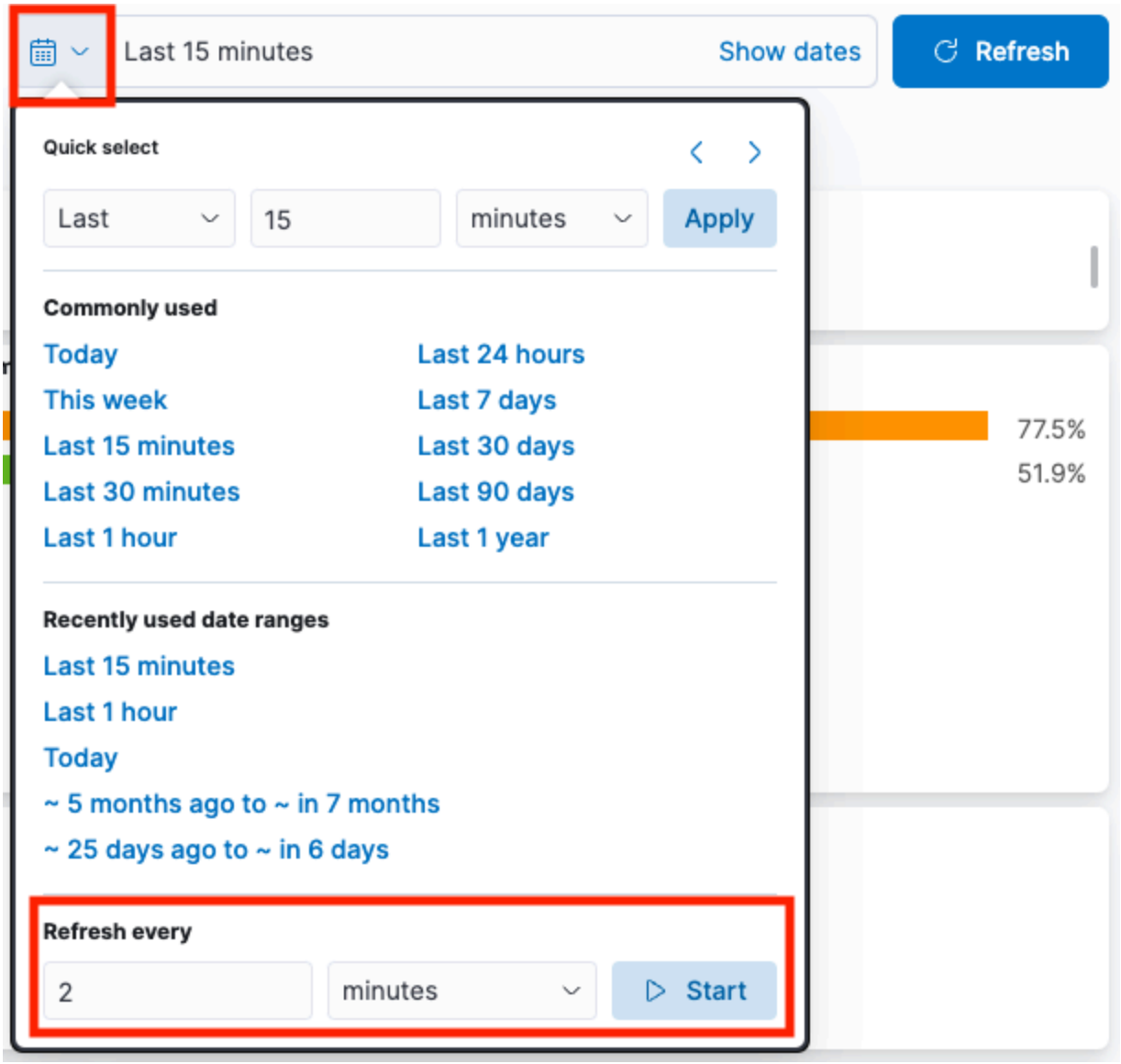
This real-time Visualization displays **Active Status** (i.e. Up/Down) of the AD components/ applications.



Considerations

Important

- From WB 9.3+ the Dashboards/Visualizations do not update by default in real-time
- Use the 'Quick Select' feature below to 'Start' auto Refresh functionality of Dashboards/ Visualizations



Important

- For Workbench 9.2 to 9.3 upgrades, existing Dashboards/Visualizations will be migrated with a "_9.2" suffix
- The migrated "_9.2" Dashboards/Visualizations will not be functional given the changes from Kibana 7.1 to 7.17
- As such, when opening the migrated "_9.2" Dashboards/Visualizations, a Warning icon/ message will be displayed
- Even though the migrated "_9.2" Dashboards/Visualizations are not functional and

display a Warning, the logic for migrating is to provide context for previously created Dashboards/Visualizations

Important

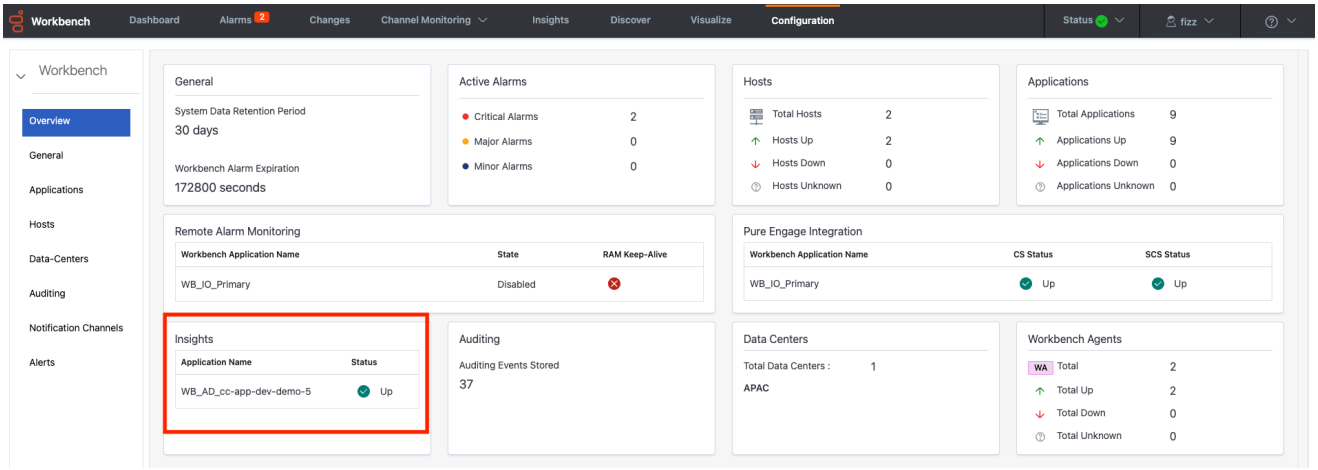
- For further comprehensive guidance on creating your own Vizualizations, please review the Visualizations section

AD Configuration

The Workbench Configuration Console enables the user to manage AD component(s) configurations and view their respective status.

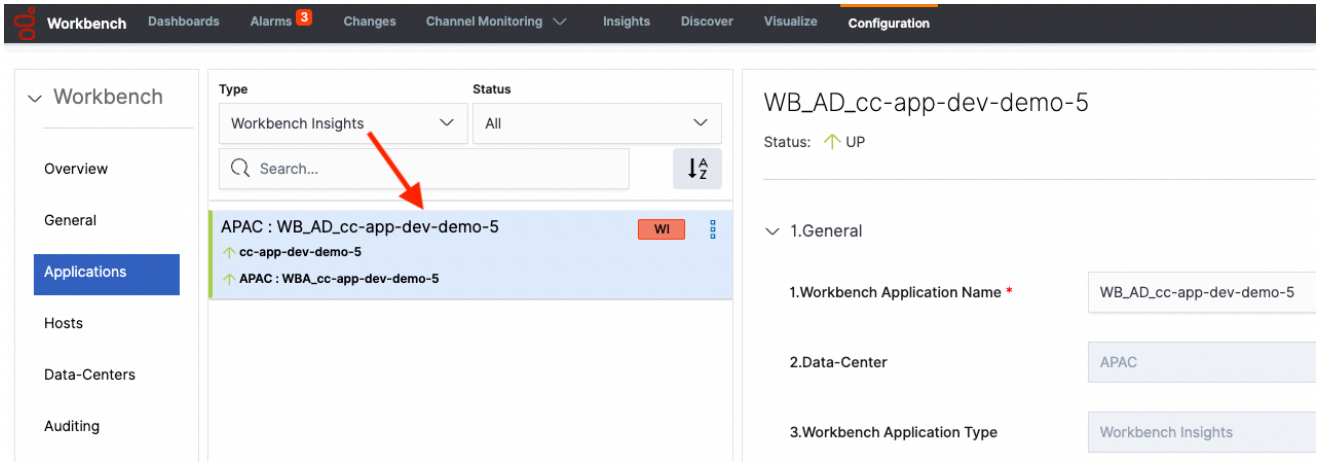
Configuration / Overview

The "Configuration / Overview" submenu section has an additional **Insights** based Visualization to view all installed AD Insight application statuses.



Configuration / Applications

An additional "Workbench Insights" filter has been added to Applications to filter based on AD Insight applications.



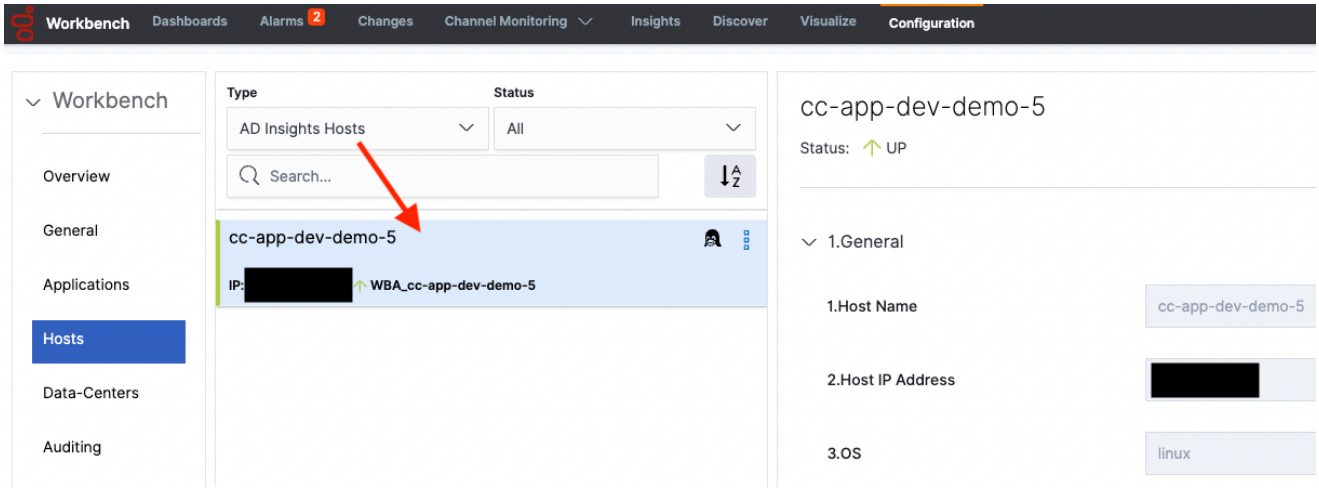
Note: The WI badge indicates the Workbench Insights Application Type.

> **Important**
>
> - For more information about each configuration option details, please review the AD Settings section

Configuration / Hosts

Post installing the AD feature, the **Configuration / Hosts** section will now display AD Host(s) where AD applications are installed

An "AD Insights Hosts" filter has been added to the Type dropdown to filter by AD Hosts only.



Important

- For details on Workbench configuration, please review the Workbench Configuration section.

Uninstalling AD

This section details the steps required to uninstall Workbench Anomaly Detection and all associated components.

Important

- Please note, this process will **permanently remove** any AD (and associated) Services and all files including data, logs, etc.
- If any data in the AD installation folder is required for archival purposes, please ensure it is saved at a separate location prior to running the AD uninstallation script(s).
- The process will leave the original configuration file generated for the settings used to install AD, which can be shared with Genesys Customer Care, if related to an installation issue.
- The complete process requires removing the AD application/host objects and configurations from Workbench as per instructions in the section "Removing Application Files from Windows Operating System" and "Removing Application Files from Linux Operating System", followed by removing the AD files as per instructions in the sections "Removing Application Objects through UI".

Removing AD Application files from Windows Operating Systems

The following steps will allow you to **uninstall** AD in **Windows**.

1. Browse to the AD home installation folder (e.g., "C:\Program Files\Workbench_AD_9.x.xxx.xx")
2. Open a Command/Powershell Console as an **Administrator** from this location (ensure the current directory in the prompt is the one identified in step 1).
3. Execute the **uninstall.bat** file.
4. **Remove any remaining files/folders** from and including the AD home installation folder.
5. This completes the AD Windows uninstallation process.

Removing AD Application files from Linux Operating Systems

The following steps will allow you to **uninstall** AD on **Linux**.

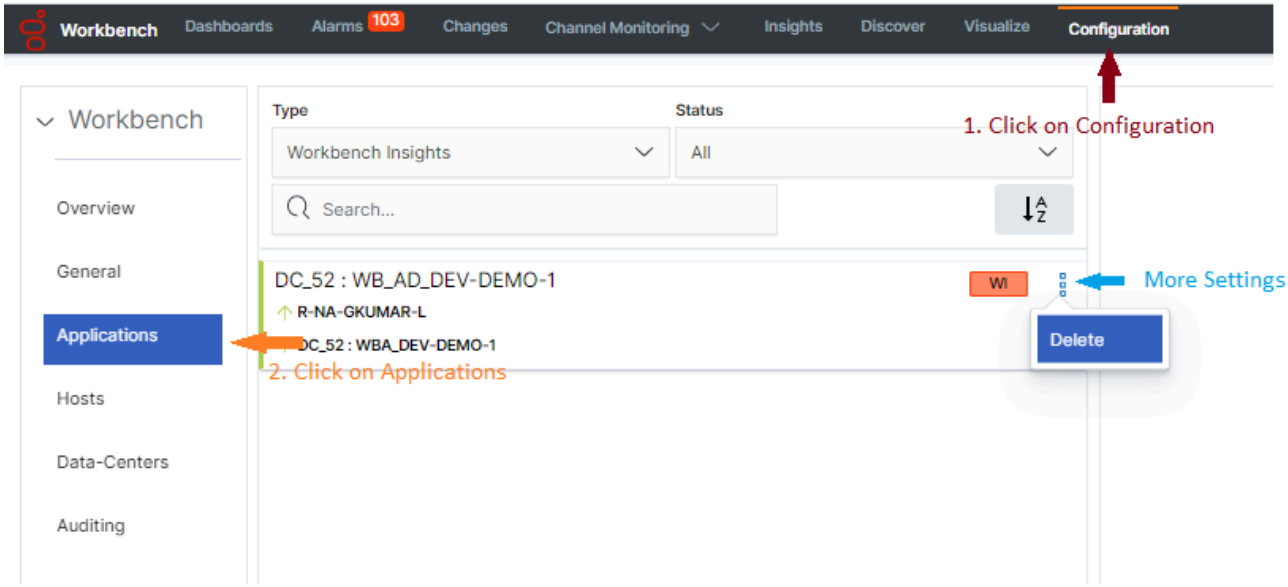
1. Using a Linux Terminal, **cd** (change directory) to the AD home installation folder (e.g., /opt/Genesys/Workbench_AD_9.x.xxx.xx)

2. Execute **./uninstall.sh** as a user (not root) with **Administrator** permissions.
3. **Remove any remaining files/folders** from and including the AD home installation folder.
4. This completes the AD Linux uninstallation process.

Remove AD Application Objects

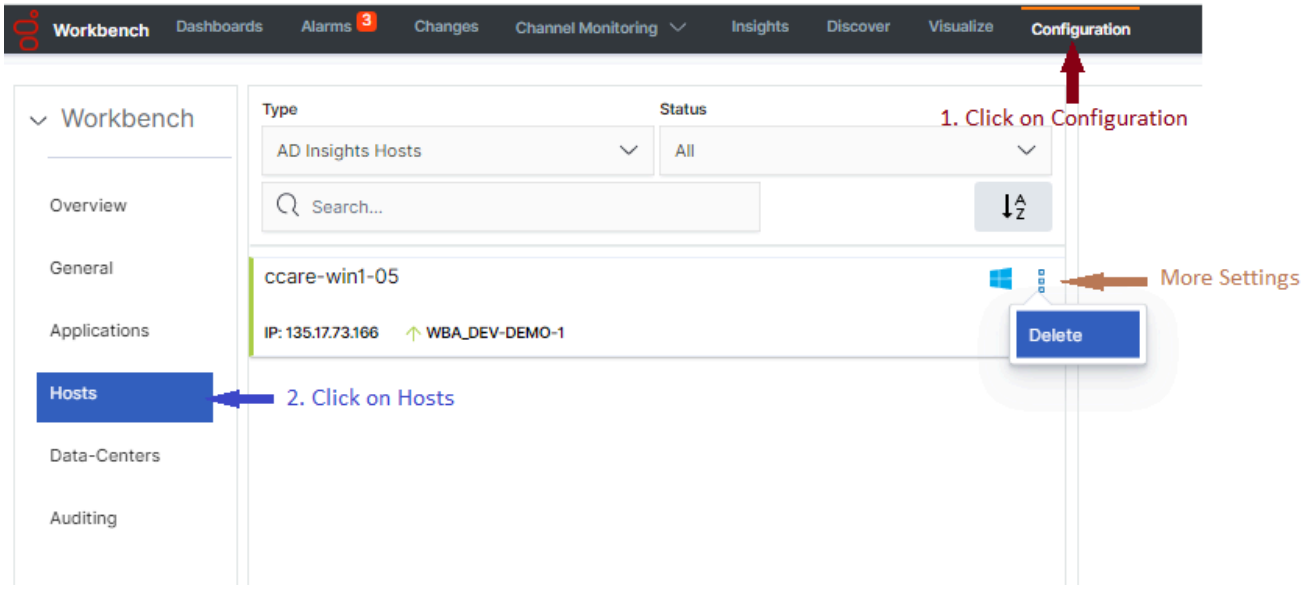
The instructions below apply to both Windows and Linux installations and are required to remove the configuration of the AD applications and the host where AD is installed.

1. Log into Workbench
2. Via the top menu bar - navigate to **Configuration**
3. Select **Applications**
4. **Identify** the AD Application(s) to be deleted
   *by scrolling through the list of all WB Applications
   *or by filtering for "Workbench Insights" Objects
5. For each AD Application to be deleted, click the **vertical ellipsis** icon to the right of the AD application, then click on **Delete**
6. Check the **Impact(s) Understood and Accepted** checkbox
7. Click **Delete** if you wish to continue and the selected AD Application Object and associated configuration data will be permanently deleted



Removing the AD Host(s)

1. Log into Workbench
2. Via the top menu bar - navigate to **Configuration**
3. Select **Hosts**
4. **Identify** the AD Host(s) to be deleted
   *by scrolling through the list of all WB Hosts
   *or by filtering for "AD Insights Hosts" Objects
5. For each AD Host to be deleted, click the **vertical ellipsis** icon to the right of the AD Host, then click on **Delete**
6. Check the **Impact(s) Understood and Accepted** checkbox
7. Click **Delete** if you wish to continue and the selected AD Host Object and associated configuration data will be permanently deleted



AD Configuration Options

This section describes the configuration options used to configure Workbench Anomaly Detection, including

- AD Configuration Dependencies
- AD Application Options

AD Configuration Dependencies

AD has dependencies with the following Workbench components.

AD Insights Application Objects

- If/when changing the AD Application **Sensitivity Level** setting, ensure ALL respective synchronized Workbench AD Applications are the same
  - i.e. do not set Workbench AD in APAC to Medium and EMEA to High - ensure both AD Applications have the same Sensitivity Level and are restarted post change

Workbench Logstash - Configuration Dependencies

- The Anomaly Detection (AD) components/feature receives Metric data via the Workbench Logstash component, therefore AD is dependent on the Workbench Logstash pipeline configuration.
- If/when there is a change to the AD Logstash connection / Logstash Port, from the AD Insights application object, the Workbench Logstash component and AD server component will be automatically restarted

Workbench IO - Configuration Dependencies

- AD communicates with Workbench IO over HTTP to store "Insights" and create AD related Alarms; therefore AD uses the Workbench IO Host and Port for communication

AD Application Options

Configuration Section	Option	Type	Default Value	Valid Value	Changes Take Effect	Description
General	Workbench Application Name	Editable	WB_AD_<HOST NAME}>	Any String name (i.e. "EMEA_WB_AD_HOST-1")	Immediately	The name of the Workbench Insights (AD) Application
	Data-Center	Read-Only	#DC	Any String(i.e. EMEA)	After AD server startup	The name of the Data-Centre associated with this Insight application; #DC will be created during the Workbench Primary node installation
	Workbench Application Type	Read-Only	Workbench Insights	Valid Workbench Application Type	After AD server startup	Workbench Application Type
	Workbench Version	Read-Only	9.2.000.00	Installed WB vesion	After AD server startup	The Workbench Application Version
	Associated Workbench Agent Application	Read-Only	<DC> : WBA_<HOST>	Name of associated Workbench Agent application	After AD server startup	The name of the Workbench Agent associated with this application
	Host Name	Read-Only	*<Hostname>* of the Workbench AD application associated host (i.e. "LAB-WB-VM1")	Valid Hostname	After AD server startup	The name of the host where this AD Insight application is running
	Host IP Address	Read-Only	*<IP Address>* of the	Valid IP Address	After AD server startup	The IPv4 Address of the host

Configuration Section	Option	Type	Default Value	Valid Value	Changes Take Effect	Description
			Workbench AD application associated host (i.e. "10.20.30.40")			where this Workbench Insight application is running
	Host Time-Zone	Read-Only	*<Time-Zone>* of the Workbench Insight application associated host (i.e. "Europe/ London")	Valid Host Time-Zone	After AD server startup	The Time-Zone of the host where this Workbench Insight application is running
	Sensitivity Level	Editable	Medium	High, Medium or Low This parameter controls the capacity of AD models to respond to anomalies. AD models define scores based on distance of each metric value form common behaviors learned form history. doing that, with this parameter it's defined the region from where they start detecting anomalies. Selecting High will increase the number of insights generated compared to selecting Low. Important **Sensitivity Level Selection** Selected sensitivity level affects all metrics and are **not** defined per	After AD server startup	The Anomaly Detection model Sensitivity Level. If/when changed, ensure ALL synchronized Workbench AD instances are the same - i.e. do not have APAC set to Medium and EMEA set to High.

Configuration Section	Option	Type	Default Value	Valid Value	Changes Take Effect	Description
				measured metric. Choosing high sensitivity level may result in too many insights, or selecting low may result in insights not being included. Ensure the correct selection based on your environment.		
Deployment	Installation Directory	Read-Only	<AD_HOME>/AD	Valid Path (i.e. /opt/Genesys/Workbench_AD_9.2.000.00/AD")	After AD server restart	Absolute path of the folder where this application is installed
	Configuration Directory	Read-Only	<AD_HOME>/AD/configs	Valid Path (i.e. /opt/Genesys/Workbench_AD_9.2.000.00/AD/configs)	After AD server restart	Absolute path of the folder where the configuration file of this application is located
Logging	Log Level	Editable	INFO	INFO, DEBUG, ERROR, WARNING, CRITICAL, NOTSET, OFF	After AD server restart	Application Logging Level
	Log File Location	Editable	<AD_HOME>AD/logs	Valid Path (i.e. "/opt/Genesys/Workbench_AD_9.2.000.00/AD/logs")	After AD server restart	Absolute path of the folder where the AD application log file is located
	Segment (MB)	Editable	10	Valid positive integer	After AD server restart	Maximum size of the log file before it is rotated/cycled
	Expire	Editable	10	Valid positive integer	After AD server restart	Maximum count of log files before rotated/cycled
AD	Node Name	Editable	WAD:	Valid String	After AD	This is a

Configuration Section	Option	Type	Default Value	Valid Value	Changes Take Effect	Description
Identifiers			Workbench Anomaly Detection		server startup	human readable identifier for this instance of AD Process.
	Server Address	Read-Only	Hostname/IP Address of the AD application associated (i.e. "LAB-AD-VM1")	Valid HostName/ IP Address	After AD server startup	The Hostname of this AD application is running.
	Server Port	Editable	50000	Valid free port integer	After AD server startup	AD application Port to bind to for incoming requests.
AD Logstash Connection	Logstash Host	Read-Only	Hostnames of the Workbench Logstash Applications	Valid Hostname and port: "{host}:{port}" AD is able to connect with different Logstash Nodes. For these cases use the format: "{hostname1}:{port1},{hostname2}:{port2}"	After AD server startup	<Hostname> of the destination Workbench Logstash application
AD Cluster	Cluster Node Names	Read-Only	AD cluster Informations	Any String	After AD server startup	AD server cluster details(i.e. Server1, Server2, Server3)

AD Additional Information

This section provides additional information for users and administrators that are deploying, configuring and using Workbench Anomaly Detection.

- Anomaly Detection (AD) **FAQ’s**
- Anomaly Detection (AD) **Known Issues and Limitations**
- Anomaly Detection (AD) **Best Practices**
- Anomaly Detection (AD) **Troubleshooting**
- Anomaly Detection (AD) **GDPR**

AD FAQ's

This section provides a useful list of Workbench Anomaly Detction AD Frequently Asked Question's (FAQ's):

Anomaly Detection Host/Server Operating System Support

- Which Operating Systems are supported by AD?
  - Answer: Windows 2012 and 2016 - RHEL 7 - CentOS 7

Anomaly Detection Deployment

- Does AD need its own dedicated host infrastructure?
  - Answer: Yes; please review the documentation Planning section
- Can I install the AD components on the Workbench core component hosts?
  - Answer: No - use separate Hosts for the AD components
- Is the Workbench Agent application required on the AD hosts?
  - Answer: Yes, and is included in the AD Installer.
- What is the maximum number of hosts supported by Anomaly Detection
  - Answer: Please review the AD Sizing section.
- Does AD support an upgrade capability
  - Answer: No
- Does Workbench AD use the Elastic Machine Learning component's/feature?
  - Answer: No - Workbench AD is a proprietary Genesys Machine Learning model

Workbench Data-Centers

- Does each Workbench Data-Center need its own AD Node(s)/Host(s)
  - Answer: Yes

AD Infrastructure/Footprint

- How many dedicated AD Nodes/Hosts are required?
  - Answer: Please review the documentation Planning section - at a high level:
    - If AD redundancy is required then more than 1 AD Node/Host will need to be deployed at each Workbench Data-Center/Site
    - Also, depending on the number of Hosts sending Metrics to Workbench and the ingestion frequency of those Metrics, additional AD Nodes/Hosts may be required at each Data-Center

AD Alarms

- What types of alarms are generated by AD?
  - Answer: AD can generate four types of alarms:
    - AD is not able to connect with Workbench Logstash.
    - AD is connected to Workbench Logstash but is not receiving metric data.
    - AD is not receiving data from a particular workbench host.
    - AD is not receiving data from one metric source

Dashboards and Visualizations

- Does AD ship with example Visualizations/Widgets for Workbench?
  - Answer: Yes.

AD Data Retention

- How/when is data purged/deleted from AD?
  - Answer: The default AD “Retention Period” is 30 days - this AD Retention Period is not configurable.

AD Ports

- Which Ports are used by Workbench Anomaly Detection (AD)?
  - Answer:
    - **50000 - 51000**: Nodes and Internal Process Communication
    - **8182**: AD API

- **9091 & 5067**: Workbench Agent and Metricbeat Ports on each AD Host
- **9090**: AD Pipeline Port on the Logstash Application
- Do not use Ports below 1024 for AD as these ports are typically used for system services

GDPR

- How does AD accommodate the GDPR policy?
  - Answer: Please review the Additional Information/GDPR section of the documentation.

Licenses

- Does Anomaly Detection need a license?
  - Answer: No - currently it's included with Workbench and needs its own dedicated Node(s)/Host(s).

AD Known Issues and Limitations

Given Anomaly Detection is a Workbench Component, details of Workbench 9 **Known Issues and Limitations** can also be found on the Genesys Customer Care Portal via Workbench Release Notes

---

ID: CCWB-5281 - https://genesys.my.salesforce.com/articles/Product_Advisories/Apache-Log4j-2-Java-library
Advisory on CVE-2021-44228 | a zero-day in the Apache Log4j 2 Java library

- Workbench Anomaly Detection (AD) is developed using Python and does not use log4j
- However the Workbench Agent 9.x component is installed on the AD Hosts, therefore either upgrade to Workbench and Anomaly Detection release 9.2.000.10 or review this page for details on Workbench Agent 9.x log4j vulnerability mitigations:
  - https://docs.genesys.com/Documentation/ST/current/WorkbenchUG/KnownIssuesandLimitations

---

AD Best Practices

The following *Best Practises* are recommended by Genesys:

Warning

- The Workbench core components should be installed prior to installing the Workbench AD components
- Please review the AD *Planning and Deployment* sections of this document before starting Anomaly Detection installation
- The AD network ports can be edited via the Workbench Configuration Console - and selecting/editing the respective Workbench application object
- AD nodes/hosts requires machines with a minimum of 8 CPU cores
- Install AD on dedicated nodes/hosts that are separate to the Workbench nodes/hosts.
- Post a Workbench Data-Center sync, only Active insights will be synced
- Review the AD configuration dependencies; Logstash and Workbench IO

AD Troubleshooting

General

Important

- Workbench uses the Hostname for component configuration
- Please ensure hostname resolution between Workbench components, including AD and Engage Hosts is accurate and robust
- If the Workbench Hosts have multiple NIC's, please ensure the Hostname resolves to the desired IP Address **prior** to Workbench installation
- Double-check network ports that are used by AD are from a firewall perspective, **open and not already in use** by other applications
- AD Nodes/Hosts require a minimum of 8 CPU cores
- Install the AD components on dedicated hosts - not on the same Nodes/Hosts as the Workbench core components.

Logs for Troubleshooting

AD automatically creates the file *ad_monitoring.log* in the {LOG_PATH} folder configured.

The structure for this log file is using this format:

```
'%(asctime)s | %(levelname)s | %(processName)s | %(message)s')
```

- Time format: 2021-09-20 03:15:46,291
- The default Log_Level is INFO. DEBUG mode can be used to see details about the process executed by AD. Doing that will reduce the performance of some components like streaming consumers and collectors.
- processName tell the AD component that is generating the event

Below a few tips of Log information for troubleshooting:

- AD start: check if AD is running as a primary or additional node

```
2021-09-08 16:16:21,446 | INFO | application_manager | WB-AD starting

2021-09-08 16:16:21,447 | INFO | application_manager | AD compilation time:
210908-192852

2021-09-08 16:16:21,447 | INFO | application_manager | configuration path: configs

2021-09-08 16:16:21,447 | INFO | application_manager | main path: /Installation/path

2021-09-08 16:16:22,172 | INFO | application_manager | App Manager started

2021-09-08 16:16:22,173 | INFO | application_manager | local data storage initialized

2021-09-08 16:16:22,173 | INFO | application_manager | AD --.--.--.-- as primary node

2021-09-08 16:16:22,173 | INFO | application_manager | app_manager class initialized
```

- AD components are started in this order: ad_api, streaming consumer, collector, model_manager, anomaly_detector and alarm_monitoring.

```
2021-09-20 03:03:47,939 | INFO | application_manager | New ad_api process started
with pid 49852

2021-09-20 03:03:47,941 | INFO | ad_api | starting AD API: -------:8182

2021-09-20 03:03:47,943 | INFO | application_manager | New
streaming_consumer_logstash0 process started with pid 49853

2021-09-20 03:03:47,952 | INFO | application_manager | New collector process started
with pid 49854

2021-09-20 03:03:47,953 | INFO | streaming_consumer_logstash0 | Streaming Consumer
initialized

2021-09-20 03:03:47,957 | INFO | collector | AD Collector initialized

2021-09-20 03:03:48,021 | INFO | model_manager | Model Manager initialized

2021-09-20 03:03:48,011 | INFO | application_manager | New model_manager process
started with pid 49855

2021-09-20 03:03:48,036 | INFO | application_manager | New anomaly_detector process
started with pid 49856

2021-09-20 03:03:48,059 | INFO | application_manager | New alarm_monitoring process
started with pid 49857

2021-09-20 03:03:48,063 | INFO | anomaly_detector | Anomaly Analyzer initialized

2021-09-20 03:03:48,072 | INFO | application_manager | modules initialized

2021-09-20 03:03:48,072 | INFO | anomaly_detector | Anomaly Detector initialized
```

```
2021-09-20 03:03:48,087 | INFO | alarm_monitoring | Alarm Monitoring initialized
```

- Commons errors detected:
  - Trying to connect with Logstash TCP server: must be confirmed with an Alarm generated by AD.

```
2021-09-20 02:32:44,139 | ERROR | streaming_consumer_logstash0 | error collecting
messages. Traceback (most recent call last): File "core/streaming_consumer.py", line
133, in main SC.streaming_process() File "core/streaming_consumer.py", line 67, in
streaming_process message = self.broker.get_message() File "core/
streaming_consumer.py", line 24, in get_message message = self.socketFile.readline()
File "/Library/Frameworks/Python.framework/Versions/3.6/lib/python3.6/socket.py",
line 586, in readinto return self._sock.recv_into(b)socket.timeout: timed out

error collecting messages. Traceback (most recent call last): File
"streaming_consumer.py", line 131, in main File "streaming_consumer.py", line 60, in
set_broker File "streaming_consumer.py", line 19, in __init__ConnectionRefusedError:
[Errno 111] Connection refused
```

Important events:

- New source detected
- AD model trained or updated
- New alarm sent
- New anomaly (insight) created
- change detected in AD config file
- restating AD components
- AD component terminated
- Additional AD Nodes:
  - new source added from primary
  - AD model updated from primary
  - Primary node is not responding
  - sending request to update primary node in WB

AD API for Troubleshooting

Additional AD API endpoints were added to monitor AD status. Per default ad_api is running on port 8182

- /ad_api/status: return the current status for AD an components.
- /ad_api/get_sources_summary: return the list of sources (metrics) collected by AD.
- /ad_api/get_alarms: return the alarms generated by AD in status open.

- /ad_api/get_last_error: return the last error detected in logs
- /ad_api/get_last_insight: return basic information about the source of last insight detected.

AD GDPR

Important

- Anomaly Detection does **NOT** store any sensitive or PII (personally identifiable information) data.
- The AD feature/Nodes/Hosts has data retention period of 30 days.