Workbench User's Guide

Workbench Elasticsearch Authentication

4/20/2025

Contents

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

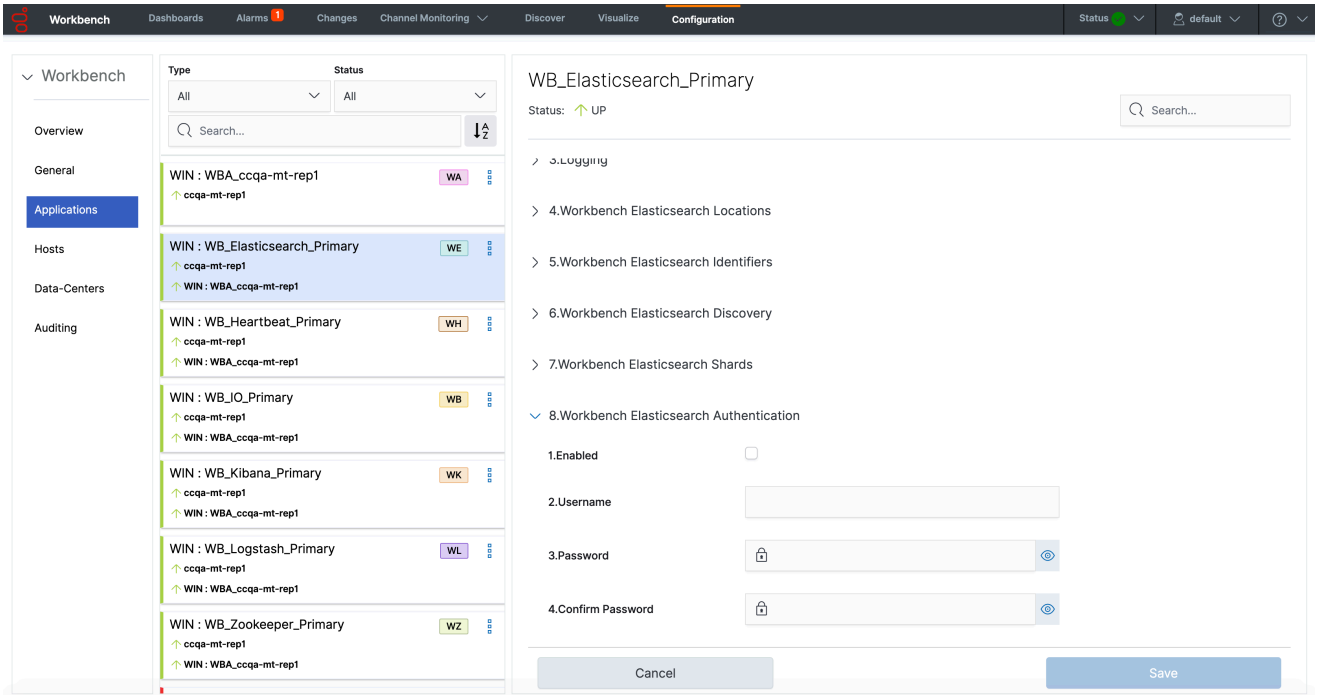
Recommended Procedure

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.