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

Workbench User's Guide

Workbench ZooKeeper Authentication

4/13/2025

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

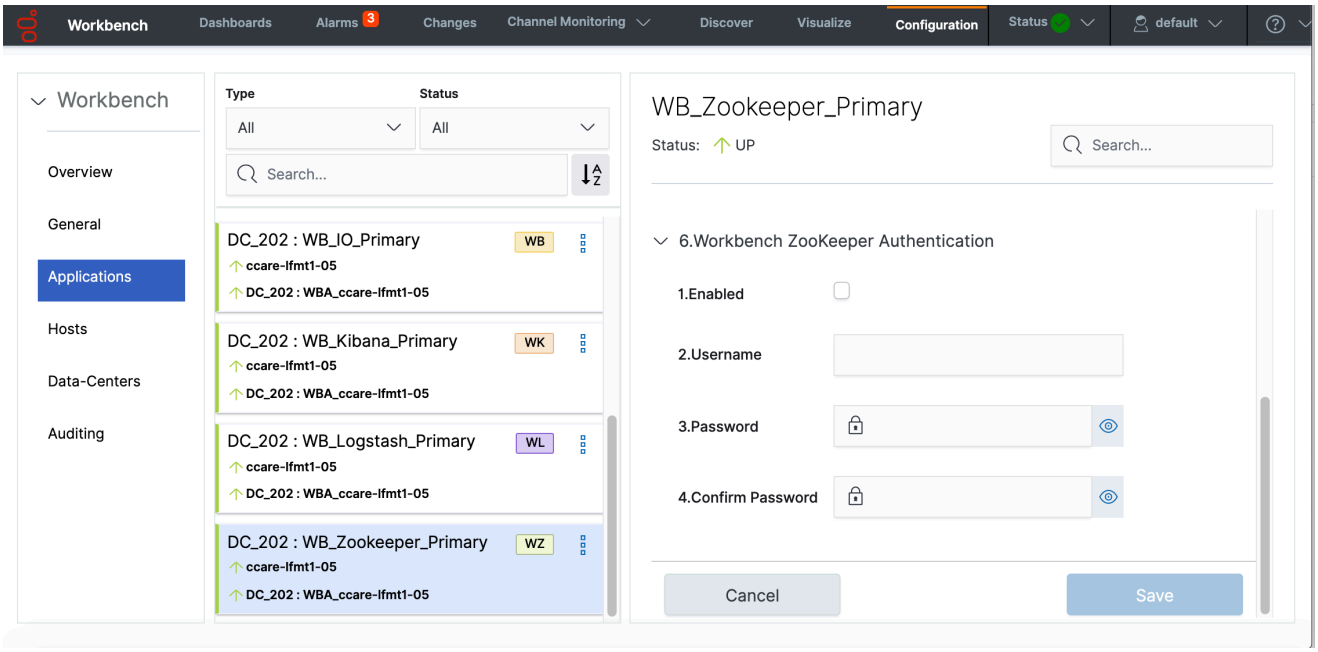
Warning

- 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