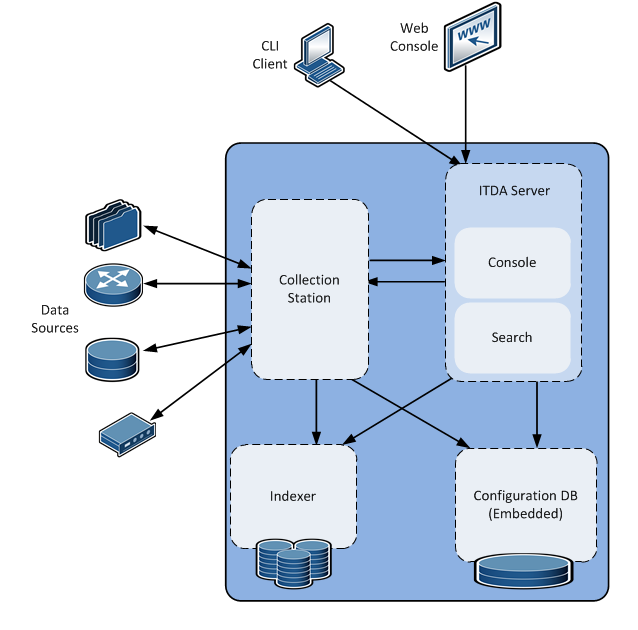
ITDA

\*\*\*\*\*\* Architechture \*\*\*\*\*\*\*

The following diagram illustrates the overall architecture of the BMC TrueSight IT Data Analytics product.



The various components of the product are described as follows:

|  |  |
| --- | --- |
| **Component** | **Description** |
| Collection Station | The Collection Station is responsible for collecting and receiving data from target hosts and then indexing the data using the Indexer.  This component fetches data collector details from the Configuration Database and then depending on the data collector configuration fetches local (or remote) log file data. All data collectors created in the system translate into actions performed by the Collection Station.  All Collection Agents read data from the data sources based on the data collector configuration; the Collection Agents and then forward this data to the Collection Station for indexing.  This component interacts with the Indexer and the Configuration Database. All Collection Agents interact with the Collection Station for data collector configuration and sending the collected log data. |
| Console Server | This is the administrative console for the BMC TrueSight IT Data Analytics product.  The Console Server component serves as the user interface for performing all actions in the BMC TrueSight IT Data Analytics product. The Console Server also acts as the gatekeeper for all actions that can be performed by using the CLI. The authentication and authorization checks for all operations are performed by the Console Server.  It enables various functions such as, configuration of data collectors, searching across all the stored log data, collaboration by using the workspace, and creating saved searches for creating views and scheduling notifications.  The Console Server stores all the configuration details in the Configuration Database. This components interacts with all the other product components. |
| Search | The Search component is responsible for processing searches that are executed by the user. In addition, this component is responsible for executing the scheduled notifications and reports. The data displayed on the **Views** tab is processed by the Search component.  The Search component searches data available in the Indexer component. The primary function of this component is to understand the user’s search query and fetch required data from the Indexer by applying search commands.  This component can interact will multiple Indexer instances and aggregate the search results. This component interacts with the Indexer and Configuration Database. |
| Indexer | The Indexer component acts as an internal datastore used by BMC TrueSight IT Data Analytics, for storing all the data that is collected by using Collection Stations and Collection Agents.  This component provides the indexing capability for all the log data. The Indexer stores the data in a way that makes searching it easier. It also stores the raw log data that can be seen in the search results. All the data is stored in a time series way to enable faster searching. The Collection Station interacts with the Indexer to send all the configured log data. Primarily the Search and Collection Station components interact with the Indexer for searching and indexing data.  Each Indexer operates within the Indexer cluster, which is a group of multiple Indexers that can communicate with each other and help you collect and search data more effectively. Data collected and searched is distributed across all the Indexers present in the cluster. For more information, see [Indexer cluster](https://docs.bmc.com/docs/display/itda11/Indexer+cluster). |
| Configuration Database | All configurations of data collectors, views, and saved searches that are used in BMC TrueSight IT Data Analytics are stored in the Configuration Database.  The Configuration Database is a lightweight component in terms of resource usage.  It does not contain the data collected by using the Collection Stations and Collection Agents. |

\*\*\*\*\*\* Search \*\*\*\*\*\*\*

Speed up MTTR (mean time to repair) by using advanced analytics with your log data

=>Compare data

-Focus on whats not normal by comparing to a known normal(good)

-Visually identify the needle in the haystack in seconds

-Drill down on differences with a single click

=>Coalesce data (classify data based on pattern)

-Reduce millions of log messages to dozens

-Identify "top talkers"

-Expose all messages within a pattern with a single click

=>Anomalies

-Takes coalesces to the next level

-Is there anything unsual in the log data? More of a particular type of mesage? Less?

-Anything I have never, or have rarely, seen before?

\*\*\*\*\*\* Collection \*\*\*\*\*\*\*

Monitor File on Collection Agent

Monitor File over SSH

Monitor File over Windows Share

Monitor Script Output over SSH

Monitor Script Output on Collection Agent

Monitor Remote Windows Events

Monitor Local Windows Events

Monitor using External Configuration

Receive over TCP/UDP

Receive over HTTP/HTTPS

Upload File