IBM BigInsights Security Implementation: Part 2 Securing the IBM BigInsights Cluster Perimeter

Big data analytics is network intensive because it runs on a cluster of nodes. Due to the high volumes of data exchanged between nodes in the IBM® BigInsights® cluster, network isolation is vital for the following reasons:

- To prevent sniffing attacks
- To reduce the network congestion so that the corporate network is not affected by the big data cluster traffic

Isolating the cluster network also gives administrators greater flexibility in enforcing the cluster access.

This IBM® Redbooks® Analytics Support web doc serves as a guide for system implementers who are creating a secure zone for an IBM BigInsights cluster by providing an example of current industry practices. This document applies to IBM BigInsights Version 4.2 and later.

IBM BigInsights cluster network deployment architecture

Figure 1 highlights one of the industry practices for network topology for IBM® BigInsights® clusters.
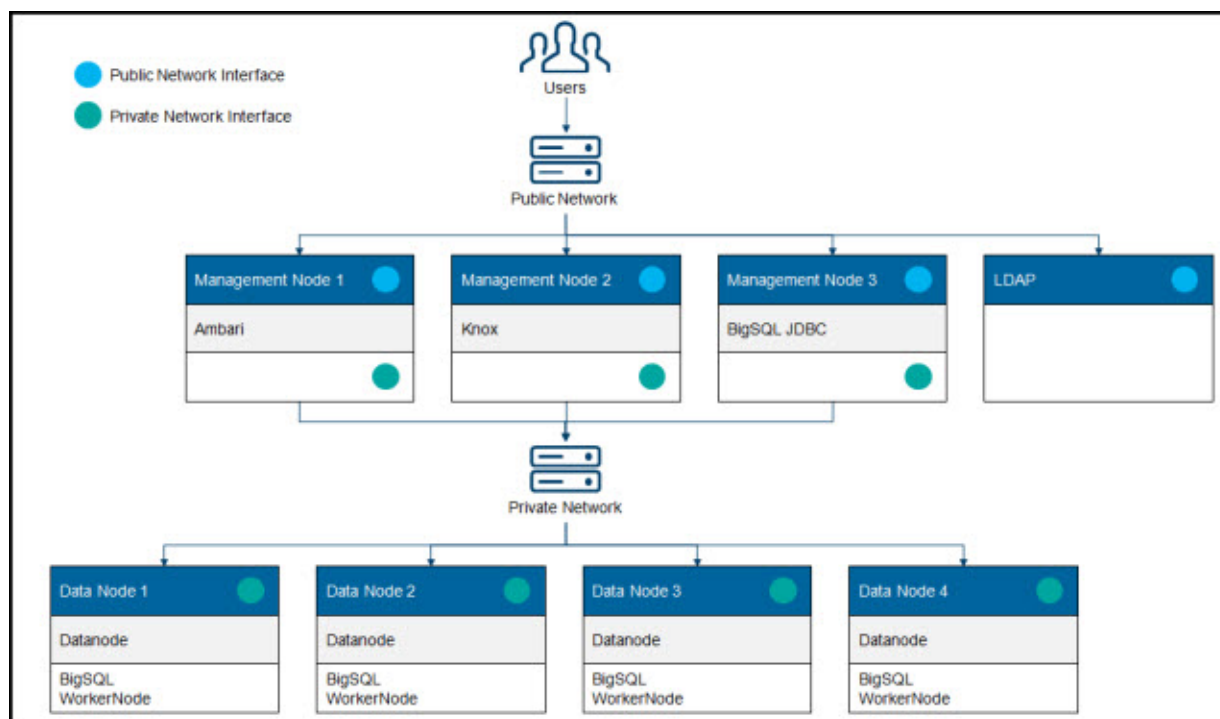

Figure 1. High-level IBM BigInsights network architecture

Users can access management nodes from the corporate network only after they authenticate with the