Lab 2: FortiAnalyzer Architecture

In this lab, you will configure a FortiAnalyzer Fabric topology that contains one supervisor, two members, and a single downstream collector that will send logs to one of the members.

This lab includes two exercises. In the first exercise, you will configure FAZ-SiteA to operate in collector mode, which will forward its logs to FAZ-MSSP, configured in analyzer mode. Then, you will generate logs to confirm the configuration is working.

In the second exercise, you will add FAZ-MSSP and FAZ-SiteB as Fabric members to form a FortiAnalyzer Fabric with FAZ-Supervisor. Then, you will generate logs to confirm the supervisor can see logs from the member devices.

Objectives

- Enable administrative domains (ADOMs)
- Configure FortiAnalyzer to operate in collector mode
- Enable log forwarding
- Modify data policy and disk utilization
- Configure the FortiAnalyzer Fabric
- Verify FortiAnalyzer Fabric sync

Time to Complete

Estimated: 50 minutes

LAB-2 > FortiAnalyzer Architecture