

Forwarding & Receiving >

Types of forwarders

- Universal Forwarder
 - Most popular
 - Installs easily in Windows, Linux, Unix (AIX and HP-UX), Solaris, and FreeBSD
 - Installed at the local machine, and can be configured using a deployment server
 - Default ports: **8089** for management and **9997** for indexing

Forwarding & Receiving >

Types of forwarders

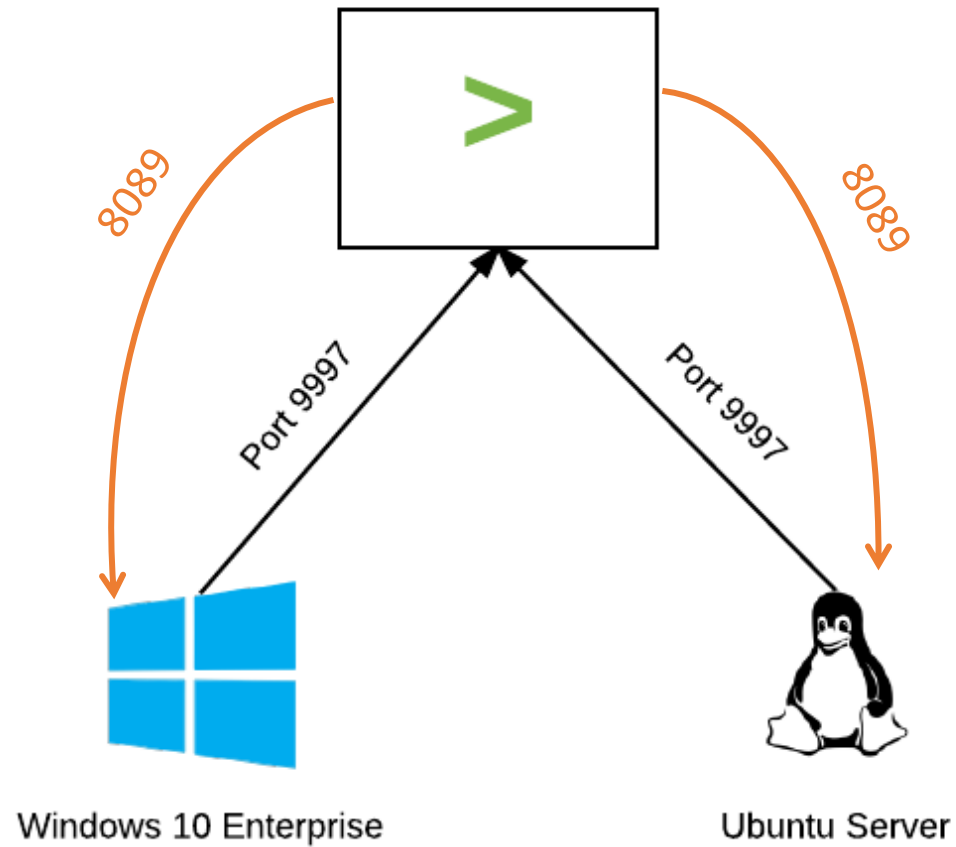
- Heavy Forwarder
 - A complete installation of the Splunk software, but with a forwarder license applied
 - Does much of the “heavy lifting” at the source
 - Can be configured at the source, and through a deployment server

Forwarding & Receiving >

Configure receiving

- Forwarding data to a Splunk indexer or search head won't work unless you configure that indexer or search head to receive data!
- Settings > Forwarding and Receiving > Add New

Forwarding & Receiving >





Demo: Universal Forwarders

Thanks, Splunkers!

