Splunk

Terms in this set (131)

90	Machine data makes up for more than __% of the data accumulated by organizations.
False	True/False. Machine data is always structured.
False	True/False. Machine data is only generated by web servers.
Indexers, Forwarders, Search Heads	What are the three main processing components of Splunk?
Indexer	What are search requests processed by?
Clustering	Which function is not a part of a single instance deployment?
Forwarders	In most Splunk deployments, _____ serve as the primary way data is supplied for indexing.
Input, Parsing, Indexing, and Searching	What does a single-instance deployment of Splunk Enterprise handle?
User, Power, Admin	What are the three main default roles in Splunk Enterprise?

Splunk

Roles	_____ define what users can do in Splunk.
User	This role will only see their own knowledge objects and those that have been shared with them.
Home app and Search & Reporting	Which apps ship with Splunk Enterprise?
source type	Splunk uses _____ to categorize the type of data being indexed.
True	True/False. The monitor input option will allow you to continuously monitor files.
once	Files indexed using the the upload input option get indexed ____.