C314. Splunk — Источники данных, индексирование данных и понятие индекса

Индексирование — это механизм, позволяющий ускорить процесс поиска, присваивая числовые адреса фрагменту данных, в котором выполняется поиск. Индексирование Splunk аналогично концепции индексации в базах данных. Установка Splunk создает три индекса по умолчанию следующим образом.

main — это индекс по умолчанию в Splunk, где хранятся все обработанные данные.

Внутренний — в этом индексе хранятся внутренние журналы и показатели обработки Splunk.

аудит — этот индекс содержит события, связанные с монитором изменений файловой системы, аудитом и всей историей пользователей.

main — это индекс по умолчанию в Splunk, где хранятся все обработанные данные.

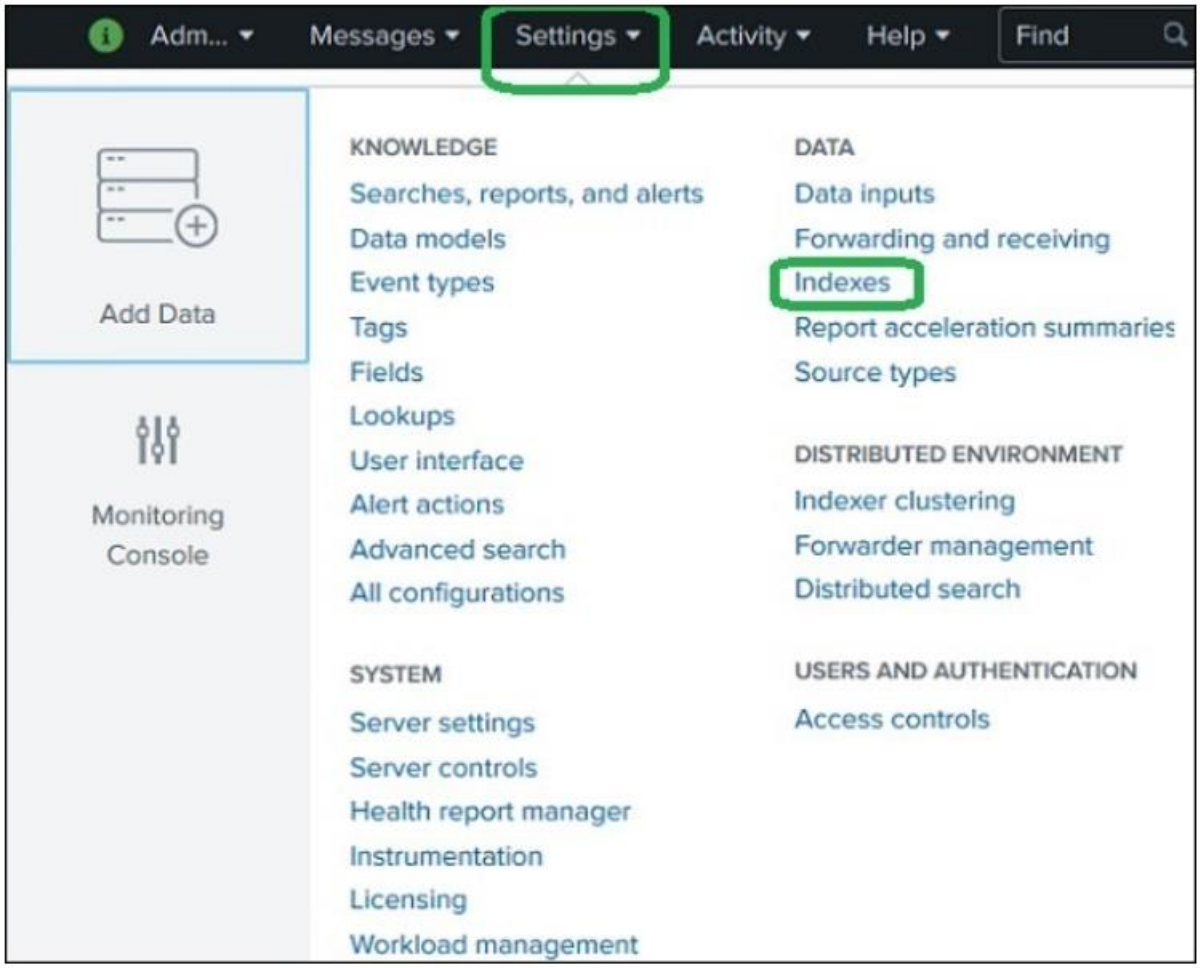
Внутренний — в этом индексе хранятся внутренние журналы и показатели обработки Splunk.

аудит — этот индекс содержит события, связанные с монитором изменений файловой системы, аудитом и всей историей пользователей.

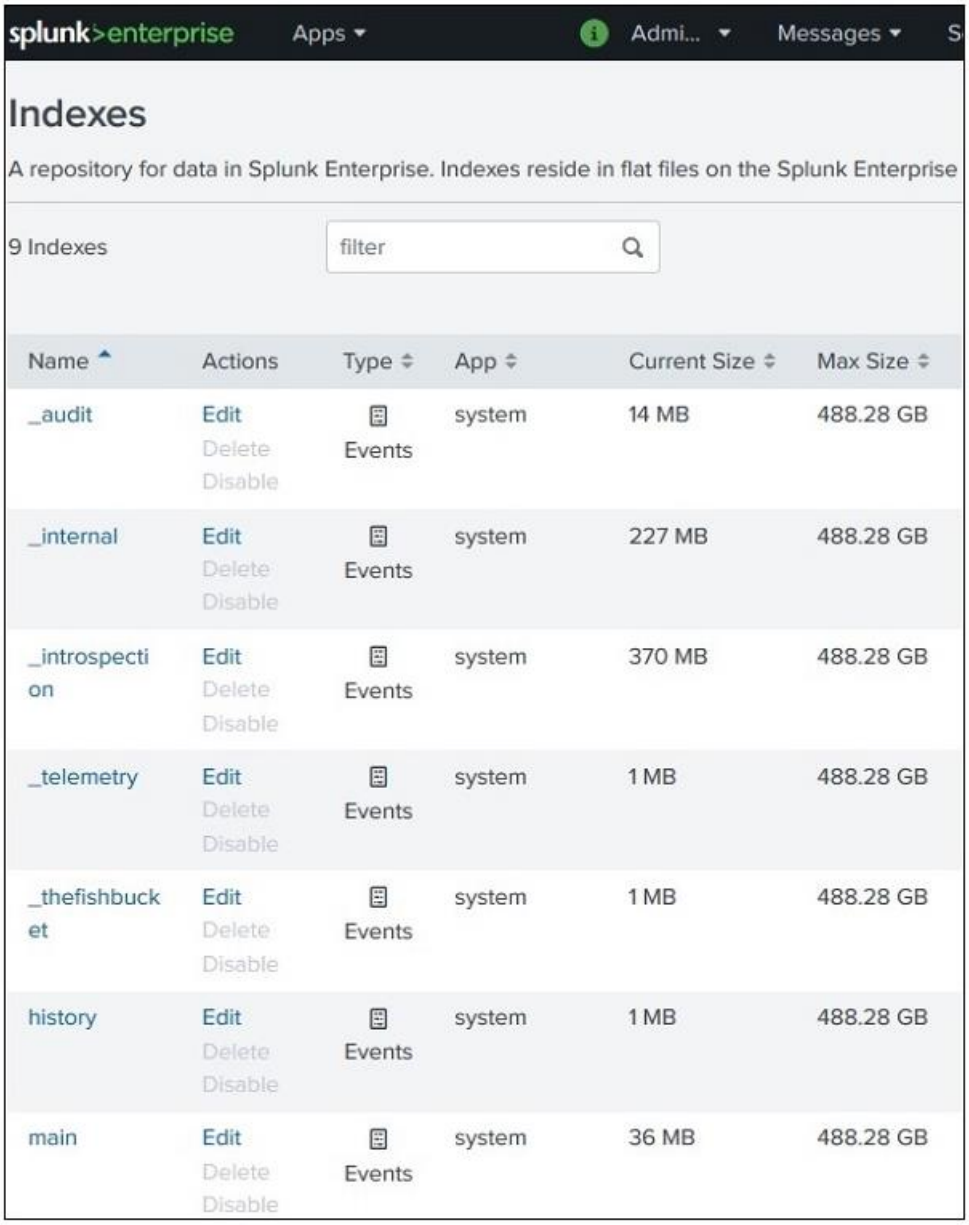
Индексаторы Splunk создают и поддерживают индексы. Когда вы добавляете данные в Splunk, индексатор обрабатывает их и сохраняет их в назначенном индексе (по умолчанию, в основном индексе или в том, который вы идентифицируете).

Проверка индексов

Мы можем взглянуть на существующие индексы, перейдя в **Настройки → Индексы** после входа в Splunk. На изображении ниже показана опция.



При дальнейшем нажатии на индексы, мы можем увидеть список индексов, которые Splunk поддерживает для данных, которые уже захвачены в Splunk. На рисунке ниже показан такой список.



Splunk - Управление индексами - CoderLessons.com