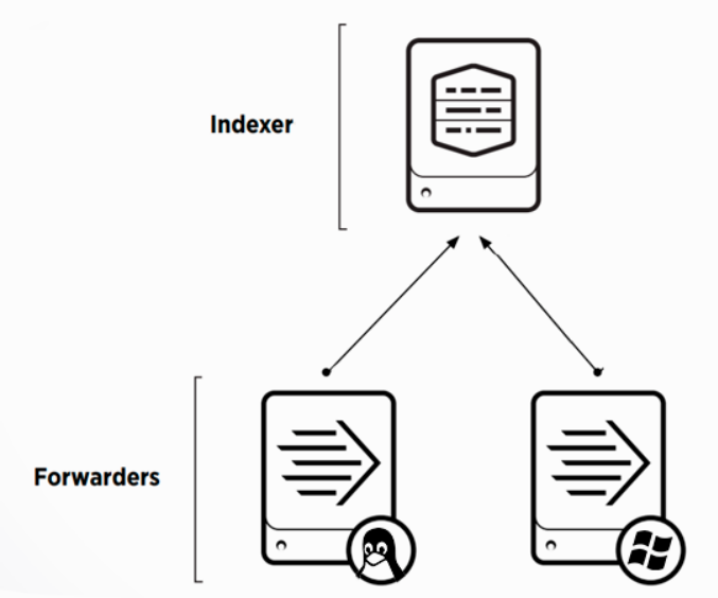
С315. Splunk — Приложения и надстройки (Apps и Add-ons)

Одними из самых распространенных источников, представляющих интерес, оказались логи **Windows** и **Linux**, которые позволяют отслеживать неполадки операционных систем и управлять ими. Загружая данные в Splunk, Вы можете анализировать работу всех систем в одном месте, даже когда у Вас десятки или сотни различных источников.
Для того, чтобы начать собирать данные нам необходимы следующие элементы системы:

- Splunk – Indexer
- Windows сервер
- Linux сервер



Для того, чтобы загружать логи в Splunk, необходимо сначала предварительно настроить индексер, для этого потребуется:

• Установить и настроить Splunk-indexer на прием данных;

• Создать приложение «Send to indexer», которое будет настраивать пересылку на всех источниках, отправляющих данные в индексер;

•Сформировать конфигурационный файл outputs.conf

• Настроить Deployment Server для управления приложением «Send to indexer» и другими приложениями;

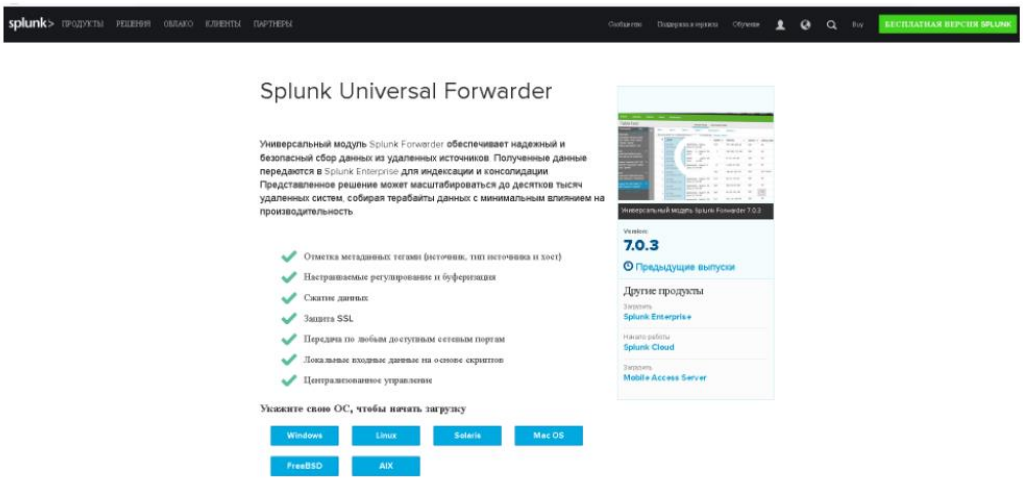
На этом этапе мы заканчиваем предварительную настройки индексера и переходим к

установке агентов на машины Windows и Linux.

WINDOWS

Универсальным инструментом для загрузки логов является специальный агент – **Splunk Universal Forwarder**. Universal Forwarder представляет собой версию Splunk Enterprise с существенно ограниченным функционалом, единственной задачей которого является сбор данных с хоста и отправка их.

Скачать его можно по этой ссылке.



Splunk – Установка агентов для сбора логов Windows и Linux / Блог компании TS Solution / Хабр (habr.com)