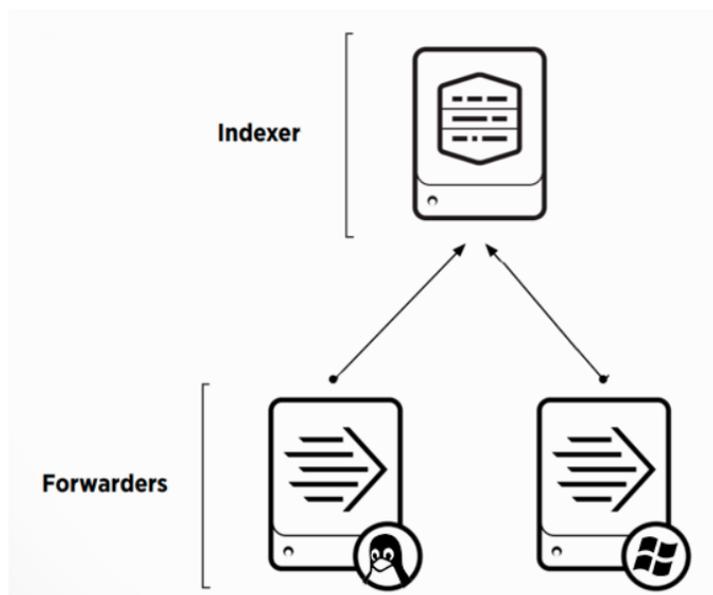


C315. Splunk — Приложения и надстройки (Apps и Add-ons)

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;

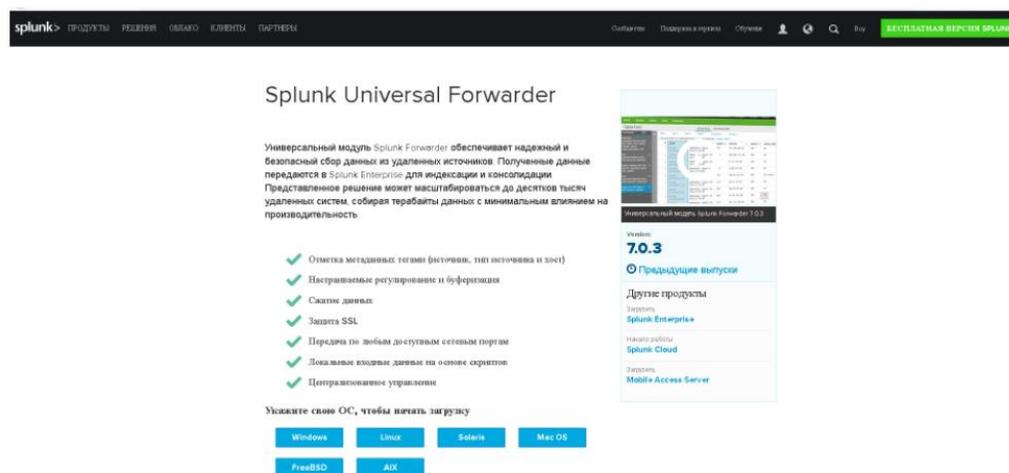
На этом этапе мы заканчиваем предварительную настройку индексера и переходим к

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» ПРОДУКТЫ РЕШЕНИЯ ОБЪЕКТЫ КЛИЕНТЫ ПАРТНЕРЫ

Outposts Поддержка и услуги Обучение Поиск Войти [КАТЕГОРИИ РЕШЕНИЙ SPLUNK](#)

Splunk Universal Forwarder

Универсальный модуль Splunk Forwarder обеспечивает надежный и безопасный сбор данных из удаленных источников. Полученные данные передаются в Splunk Enterprise для индексации и консолидации. Представленное решение может масштабироваться до десятков тысяч удаленных систем, собирая терабайты данных с минимальным влиянием на производительность.

- ✓ Отметка метаданных тегов (источник, тип источника и host)
- ✓ Настраиваемые расписания и буферизация
- ✓ Сжатие данных
- ✓ Защита SSL
- ✓ Передача по любым доступным сетевым портам
- ✓ Локальное хранение данных на основе шифрования
- ✓ Централизованное управление

Укажите свою ОС, чтобы начать загрузку

[Windows](#) [Linux](#) [Solaris](#) [Mac OS](#)
[FreeBSD](#) [AIX](#)

Версия: **7.0.3**
Последние выпуски

Другие продукты

- Загрузить [Splunk Enterprise](#)
- Найти работы [Splunk Cloud](#)
- Загрузить [Mobile Access Server](#)

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