splunk>

**Splunk® Enterprise Security: Руководство по установке и обновлению 5.1.0**

Подготовлено: 14 мая 2018г. в 19:58

Авторское право (с) 2018. Splunk Ink. Все права защищены.

**Содержание**

|  |  |
| --- | --- |
| **Введение** | **1** |
| О системе Splunk Enterprise Security | 1 |
| Пересылка пользовательских данных в Splunk для Splunk Enterprise Security | 1 |
| **Планирование** | **4** |
| План развертывания | 4 |
| Планирование источника данных для Splunk Enterprise Security | 13 |
| **Установка** | **16** |
| Установка Enterprise Security | 16 |
| Установка Splunk Enterprise Security в среду кластера в строке поиска | 19 |
| Развертывание надстроек, включенных в Splunk Enterprise Security | 24 |
| Импорт пользовательских приложений и надстроек в Splunk Enterprise Security | 31 |
| Интеграция Splunk Stream в Splunk Enterprise Security | 33 |
| Конфигурация и внедрение индексов | 34 |
| Конфигурация пользователей и ролей | 35 |
| Конфигурация моделей данных для Splunk Enterprise Security | 42 |
| **Обновление** | **47** |
| Планирование обновления системы Splunk Enterprise Security | 47 |
| Обновление системы Splunk Enterprise Security | 49 |
| Обновление системы Splunk Enterprise Security в кластерной среде строки поиска | 52 |

**Введение**

**О системе Splunk Enterprise Security**

Splunk Enterprise Security использует возможности поиска и составления отчетности платформы Splunk для предоставления специалисту по безопасности общей картины безопасности организации. Enterprise Security использует **корреляционные запросы поиска**, чтобы обеспечить видимость угроз, связанных с безопасностью, и генерировать **существенные события** для отслеживания выявленных угроз. Вы можете определять, отслеживать и создавать отчеты на основании данных с устройств, систем и приложений в вашей среде.

Данное руководство предназначено для пользователя, который может устанавливать, настраивать и администрировать программное обеспечение Splunk. Если вам нужна подготовка на платформе Splunk и Enterprise Security, см. «Образовательные курсы для клиентов Enterprise Security».

Другие руководства для Splunk Enterprise Security включают:

• Пояснения

• Использование системы Splunk Enterprise Security

• Администрирование Splunk Enterprise Security

• Случаи использования

• Ссылка на программный интерфейс неактивных данных (API REST)

**Пересылка пользовательских данных в Splunk для Splunk Enterprise Security**

Когда Splunk Enterprise Security развернута на Splunk Enterprise, платформа Splunk отправляет анонимные данные для использования в Splunk Inc. («Splunk»), чтобы помочь улучшить Splunk Enterprise Security в будущих версиях. Сведения о том, как выбирать или отключать и как собирать, хранить и управлять данными см. в разделе «Совместное использование данных в Splunk Enterprise».

**Как собираются данные**

Splunk Enterprise Security использует сохраненные поисковые запросы для сбора данных с целью анонимного использования. Эти поисковые запросы выполняются в фоновом режиме независимо от того, хотите ли вы отказаться от отправки данных использования в Splunk. Данная функция не оказывает существенного влияния на производительность системы.

**Какие данные собираются**

Splunk Enterprise Security собирает следующую базовую информацию для использования:

|  |  |  |
| --- | --- | --- |
| **Наименование** | **Описание** | **Пример** |
| app.SplunkEnterpriseSecuritySuite.active\_users | Сообщает о количестве активных пользователей | {  "version": "1.0",  "end": 1521483766,  "begin": 1521396000,  "data": {  "analyst\_count": 0,  "count": 1,  "admin\_count": 1,  "user\_count": 0  }  } |
| app.SplunkEnterpriseSecuritySuite.feature\_usage | • Время загрузки страницы: отображает время, необходимое для загрузки страницы  • Использование функций: выводит данные об использовании функций | {  "end": 1521483766,  "begin": 1521396000,  "version": "1.0",  "data": {  "count": 1,  "avg\_spent": 515,  "view": "ess\_home"  }  } |
| app.SplunkEnterpriseSecuritySuite.search\_  execution | Сообщает среднее время выполнения поиска, чтобы помочь оценить производительность. | {  "end": 1521483766,  "begin": 1521396000,  "data": {  "avg\_run\_time": 0.75,  "count": 2,  "search\_alias": "Access - Authentication Tracker - Lookup Gen"  },  "version": "1.0",  } |
| app.SplunkEnterpriseSecuritySuite.search\_actions | Сообщает о том, что было введено в качестве запроса на поиск | {  "data": {  "total\_scheduled": 70,  "action": "output\_message",  "is\_adaptive\_response": 1,  "count": 6  },  "version": "1.0"  } |
| app.SplunkEnterpriseSecuritySuite.datamodel\_  distribution | Выполняет проверку модели данных, чтобы определить, какие модели наиболее используются. | {  "data": {  "size": 2265088,  "datamodel": "Change\_Analysis",  "perc": 49.33  },  "version": "1.0"  } |

**Планирование**

**План развертывания**

Разверните Splunk Enterprise Security на настроенной платформе Splunk для установки. Перед развертыванием Enterprise Security ознакомьтесь с требованиями к системе и оборудованию, а также настройками поиска и индексатора.

**Доступные архитектуры развертывания**

Вы можете развернуть Splunk Enterprise Security в виде единичной копии или выполнить развертывание с распределенным поиском. Splunk Enterprise Security также доступна в Splunk Cloud. Перед развертыванием Splunk Enterprise Security на предприятии ознакомьтесь с компонентами развертывания платформы Splunk. См. раздел «Компоненты развертывания Splunk Enterprise» в *Руководстве планирования емкости*.

***Развертывание единичной копии***

Для простого и небольшого развертывания установите Splunk Enterprise Security на единичной копии платформы Splunk. Единичная копия функционирует как строка поиска, так и индексатор. Используйте серверы пересылки (агент ПО, используемый для сбора данных с серверов) для сбора ваших данных и отправки их в один центр для анализа, хранения и поиска.

Вы можете использовать развертывание единичной копии для лабораторной или тестовой среды, а также для небольшой системы из одного или двух пользователей, выполняющих параллельные поисковые запросы.

***Развертывание с распределенным поиском***

Для развертывания и запуска Splunk Enterprise Security рекомендуется развертывание с распределенным поиском.

• Установите Splunk Enterprise Security на выделенную строку поиска или кластер для поиска.

• С помощью индексного кластера и распределения нагрузки на поиск данных по нескольким узлам необходимо повысить эффективность поиска. Использование нескольких индексаторов позволяет собирать данные, собранные серверами пересылки, и нагрузку на обработку данных, которые должны быть распределены между индексаторами.

• Используйте серверы пересылки для сбора ваших данных и отправки их в индексаторы.

При развертывании с распределенным поиском и для внедрения кластеров с функцией поиска провидите конфигурацию поиска, чтобы перенаправить все данные в индексаторы. См. «Перенаправление данных поиска на уровень индексатора» в руководстве «*Распределенный поиск*».

Чтобы правильно масштабировать развертывание распределенного поиска с помощью Splunk Enterprise Security, см. «Введение в планирование емкости для Splunk Enterprise» в *Руководстве планирования емкости* и «Оценка масштабирования индексатора для Splunk Enterprise Security».

***Развертывание облаков***

Splunk Enterprise Security доступна как услуга в Splunk Cloud. Архитектура развертывания Splunk Cloud варьируется в зависимости от данных и нагрузки поиска. Клиенты Splunk Cloud работают с поддержкой Splunk для настройки, управления и поддержки инфраструктуры облака. Сведения о развертываниях, управляемых Splunk Cloud, см. в разделе «Типы развертывания Splunk Cloud» в *Руководстве пользователя* Splunk Cloud.

***Гибридное развертывание поиска***

Гибридная конфигурация поиска с Splunk Enterprise Security пока не поддерживается в Splunk Cloud. Вы можете настроить локальную строку поиска Splunk Enterprise Security для поиска индексаторов в другой среде облака. Любая конфигурация развертывания гибридного поиска должна учитывать дополнительные задержки, проблемы с полосой пропускания и включать в себя подходящее оборудование для поддержки нагрузки поиска.

**Системные требования Splunk Enterprise**

Splunk Enterprise Security требует установки 64-битной ОС во всех поисковых системах и индексаторах. Список поддерживаемых операционных систем, браузеров и файловых систем см. в разделе «Системные требования для использования Splunk Enterprise на предприятии» *Руководства по установке* Splunk Enterprise.

Используйте таблицу ниже, чтобы определить совместимость версий Enterprise Security 5.0.x с версиями платформы Splunk.

|  |  |
| --- | --- |
| **Версия Splunk Enterprise Security** | **Версия платформы Splunk** |
| 5.0.0 | 6.6.х и 7.0.х |
| 5.1.0 | 7.1.0 |

**Требования к оборудованию**

Splunk Enterprise Security требует минимальных технических характеристик оборудования, которые вы увеличиваете в соответствии с вашими потребностями и принципами использования Splunk Enterprise Security. Данные спецификации также применяются для развертывания единичной копии Splunk Enterprise Security.

|  |  |  |
| --- | --- | --- |
| **Функция оборудования** | **Минимум ЦП** | **Минимум ОЗУ** |
| Функция поиска | 16 ядер | 32 Гб |
| Индексатор | 16 ядер | 32 Гб |

Индексирование – это интенсивный процесс ввода/вывода. Индексаторы требуют достаточного объема диска ввода/вывода для эффективного и быстрого анализа данных при ответе на запросы поиска. Для получения информации о последних требованиях IOPS (операций ввода-вывода в секунду) для запуска Splunk Enterprise см. раздел «Информация об оборудовании: индексирование» в *Руководстве планирования емкости*.

Возможно, вам придется увеличить технические характеристики развертывания Enterprise Security и превысить минимальных требований к оборудованию в зависимости от вашей среды. В зависимости от конфигурации вашей системы, обратитесь к средним или высоким параметрам рекомендуемого оборудования платформы Splunk. См. «Спецификацию среднего уровня и спецификацию высокой производительности» в *Руководстве планирования емкости*.

Если количество ядер процессора индексатора в вашем развертывании превышает минимальные требования, указанные в спецификации оборудования, вы можете реализовать один из параметров параллелизации, чтобы улучшить производительность индексатора для конкретных случаев использования. См. «Настройки параллелизации» в *Руководстве планирования емкости*.

**Особенности строки поиска в Splunk Enterprise Security**

Установите Splunk Enterprise Security в специальную поисковую функцию или выделенный кластер для поиска. Вы можете установить только совместимые приложения или надстройки Общей информационной модели (CIM) в поисковую функцию для Splunk Enterprise Security. Например, приложение Splunk для PCI Compliance (для Splunk Enterprise Security) или надстройка Splunk для Facebook ThreatExchange может быть установлено в той же поисковой строке, что и Splunk Enterprise Security.

Все **поисковые запросы в режиме реального времени** в Splunk Enterprise Security используют индексированные настройки реального времени для повышения производительности индексирования. См. «Поиск в режиме реального времени и создании отчетов» в *Руководстве по поиску.* Отключение индексации в режиме реального времени уменьшает общую производительность ваших индексаторов. Чтобы просмотреть влияние результатов поиска в режиме реального времени, см. «Известные

ограничения поиска в реальном времени» в *Руководстве по поиску*.

Для Splunk Enterprise Security требуется KV Store. Дополнительные сведения о KV Store, включая системные требования, см. в разделе «Хранилище значений ключа приложения» в *Руководстве администратора* Splunk Enterprise. Splunk Enterprise Security хранит некоторые файлы справочника в KV Store. В среде кластера поисковой системы синхронизация больших KV Store справочников в элементах кластера может привести к сбою и быстрому устареванию KV Store. Чтобы не допустить такого развития событий, можно увеличить размер журнала операций. См. раздел «Предотвращение устаревания элементов путем увеличения размера журнала операций» в *Руководстве администратора* Splunk Enterprise.

Splunk Enterprise Security не поддерживает объединение в поисковые системы.

**Splunk Enterprise Security и кластеризация строки поиска**

Splunk Enterprise Security поддерживает установку только в кластерных строках поиска Linux. В настоящее время кластеры строки поиска Windows не поддерживаются Splunk Enterprise Security.

Кластеры строк поиска увеличивают нагрузку поиска на индексаторы. Добавьте больше индексаторов или выделите дополнительные ядра ЦП для индексаторов при реализации кластера строки поиска. См. «Требования к системе и другие рекомендации по развертыванию для кластеров строки поиска» в *Руководстве по распределенному поиску* Splunk Enterprise и «Архитектура кластеризации строки поиска» в *Руководстве по распределенному поиску*.

***Рекомендации по масштабированию строки поиска для Splunk Enterprise Security***

|  |  |
| --- | --- |
| **Фактор** | **Увеличение данной спецификации** |
| Большое количество одновременных поисковых запросов | Увеличить ядра ЦП  Увеличить ОЗУ |
| Большое количество поисковых запросов, обрабатываемых в режиме реального времени  Большое количество пользователей, одновременно входящих в систему | Увеличить ядра ЦП |
| Большое количество активных корреляционных поисков | Увеличить ОЗУ |
| Большие файлы поиска ресурсов и выполнения идентификации справочников | Увеличить ОЗУ |

**Масштабирование индексатора для Splunk Enterprise Security**

Увеличьте количество индексаторов в своем развертывании до необходимых масштабов с увеличением нагрузки поиска и параллелизма поиска. Поскольку набор индексаторов может обслуживать более одной поисковой строки (функции), дополнительные функции поиска, использующие те же индексаторы, что и поисковая строка Enterprise Security, могут повлиять на общую производительность вашего индексатора и сократить ресурсы, доступные для Enterprise Security.

Платформа Splunk использует индексаторы для масштабирования по горизонтали. Количество индексаторов, требуемых при развертывании Enterprise Security, зависит от объема данных, типа данных, требований хранения, типа поиска и параллельности (одновременности) поиска.

Необходимо поработать с Splunk Professional Services, чтобы провести оценку архитектуры развертывания, если вы планируете использовать 1 терабайт (1 ТБ) в день или более данных в Enterprise Security.

***Результаты теста на производительность***

Изучите результаты тестов на производительность, чтобы более точно оценить производительность, которую вы можете ожидать от своей системы, на основе сочетания данных в вашей платформе Splunk и развертывания Enterprise Security. Индексаторы, используемые для этих тестов на производительность, соответствуют аппаратным средствам с 32 ГБ ОЗУ и 16 ядрами ЦП.

При определении размера Splunk Enterprise Security необходимо учитывать два существенных фактора.

• Нагрузка корреляционного поиска, основанная на количестве корреляционных запросов и поддерживающих запросов, включенных в ваше развертывание.

• Ускорение нагрузки модели данных на основе количества ускоряемых моделей данных, типа моделируемых данных, мощности моделируемых данных и объема ускоряемых данных.

В зависимости от набора данных объем масштабирования может варьироваться от 40 до 100 ГБ на один индексатор, в противном случае ускорение модели данных отстает от приема данных.

Основываясь на общем сценарии с сочетанием данных модели, проведенный тест показал, что каждый индексатор поддерживал скорость приема данных на уровне 100 ГБ в день с низкой задержкой в ​​ускорениях модели данных и отклика пользовательского интерфейса.

|  |  |
| --- | --- |
| **Соединение модели данных тестирования** | |
| Типы данных |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Выбор источников данных с различными коэффициентами был произведен и ускорен на четырех моделях данных.  • Web: 65% всех данных  • Сетевой трафик: 25% всех данных  • Анализ изменений: 1% всех данных | | | | |
|  | Аутентификация: 1% всех данных с любым оставшимся процентом, не применимым к какой-либо модели данных. | | | | |
| Нагрузка поиска | Было найдено 60 корреляционных запросов. Дополнительная загрузка пользователя не была добавлена. | | | | |
| Результаты масштабирования: объем данных | 100 | 300 | 500 | 800 | 1000 |
| Результаты масштабирования: количество индексаторов | 1 | 3 | 5 | 8 | 10 |

На основе сценария, в котором единственными данными в Enterprise Security была одна модель данных высокой мощности или с уникальными данными, тест показал, что каждый индексатор поддерживал скорость приема данных на уровне 40 ГБ в день при низкой задержке ускорения модели данных и отклика пользовательского интерфейса.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тест: максимальное использование для одной модели данных** | | | | | |
| Типы данных | Загружать и ускорять данные только в модели данных сетевого трафика. | | | | |
| Нагрузка поиска | Было найдено 60 корреляционных запросов. Дополнительная загрузка пользователя не была добавлена. | | | | |
| Результаты масштабирования: объем данных | 40 | 120 | 200 | 320 | 400 |
| Результаты масштабирования: количество индексаторов | 1 | 3 | 5 | 8 | 10 |

***Поддержка кластеризации индексатора***

Splunk Enterprise Security поддерживает как кластерные архитектуры однопользовательского, так и многопользовательского индексатора. См. «Основы архитектуры кластера индексатора и многопользовательской кластерной архитектуры» в разделе *Управление индексаторами и кластерами индексаторов*.

Архитектура кластера однопользовательского и многопользовательского индексатора может иметь одну строку поиска или один кластер поиска при запущенной системе Enterprise Security. Дополнительные запросы поиска отдельных станций не могут запускаться в Enterprise Security.

Для кластерной архитектуры многопользовательского индексатора Splunk рекомендует следующее:

• Активировать итоговую репликацию. См. «Реплицированные отчеты» в разделе *Управление индексаторами и кластерами индексаторов*.

• Установить строку поиска Enterprise Security на site0, чтобы отключить сродство поиска. См. «Отключение сродства поиска» в разделе *Управление индексаторами и кластерами индексаторов*.

Если вы используете кластеризацию индексатора, метод, применяемый для развертывания приложений и файлов конфигурации для одинаковых индексаторов, отличается. См. «Управление общими конфигурациями для всех кластеров» и «Управление развертыванием приложений во всех одинаковых кластерных индексаторах» в разделе *Управление индексаторами и кластерами индексаторов.*

***Ускорение модели данных***

Splunk Enterprise Security ускоряет модели данных для предоставления результатов поисков на витрине, панели и в корреляции. Ускорение модели данных использует индексаторы для обработки и хранения данных, сохраняя ускоренные данные в каждом индексаторе.

Возможно использование лимитированного ускорения модели данных (конкретные модели данных) для определенных индексаторов с целью повышения производительности ускорения модели данных и снижения нагрузки индексатора, особенно при масштабировании. См. раздел «Настройка надстройки общей информационной модели Splunk» для более подробной информации о том, как ограничить модели данных для конкретных индексаторов.

См. Моделирование ускорения и хранения данных модели данных для расчета дополнительного хранилища для ускорения модели данных.

***Индексная совместимость с TSIDX***

Политика хранения для индексных TSIDX-файлов доступна в Splunk Enterprise 6.4.x. Дополнительные сведения см. в разделе «Сокращение использования дискового пространства tsidx» в руководстве *Управление индексаторами и кластерами индексаторов* Splunk Enterprise. Настройка политики хранения для файлов TSIDX не влияет на сохранение

ускорения модели данных.

Некоторые поиски, предоставляемые Splunk Enterprise, не работают на кодах с уменьшенными TSIDX-файлами.

|  |  |  |
| --- | --- | --- |
| **Панель/наименование поиска** | **Диапазон времени по умолчанию** | **Способы имитации** |
| Панель проверки сервера пересылки: счет событий в течение времени пребывания в системе основного компьютера | -30d | Установите сохранение TSIDX на уровне, большем, чем временной диапазон. |
| Сохраненный поиск: Проверка – счет событий в течение времени пребывания в системе 10 основных компьютеров | -30d | Установите сохранение TSIDX на уровне, большем, чем временной диапазон. |
| Сохраненный поиск: Проверка – счет событий в день – генерирование справочника | -1d | Установите сохранение TSIDX на уровне, большем, чем диапазон времени по умолчанию. |
| Сохраненный поиск: крайняя точка – коэффициент времени дельта 2 – отчет | -1d | Установите сохранение TSIDX на уровне, большем, чем диапазон времени по умолчанию. |

**Использование сервера развертывания с Splunk Enterprise Security**

Splunk Enterprise Security включает приложения и надстройки. Если сервер развертывания управляет этими приложениями или надстройками, Enterprise Security не завершит установку.

• Для надстроек, включенных в Splunk Enterprise Security, разверните их с помощью средства управления распределенной конфигурацией. См. раздел Развертывание надстроек, включенных в Splunk Enterprise Security, в данном руководстве.

• Для других приложений и надстроек, установленных в вашей среде, при необходимости разверните их при помощи сервера развертывания. См. «Сведения об управлении сервером развертывания и управлении пересылкой» в ​​разделе *Обновление программы Enterprise Splunk*.

Если надстройки, входящие в пакет Enterprise Security, управляются сервером развертывания, удалите конфигурацию клиента развертывания перед установкой Enterprise Security.

1. Удалите файл deploymentclient.conf, содержащий ссылки на сервер развертывания.

2. Перезапустите службы Splunk.

**Виртуализированное оборудование**

Если вы устанавливаете Splunk Enterprise Security в виртуализованной среде, вам необходимо иметь такое же распределение памяти и процессора, как и в не виртуализованной среде для платформы без ОС.

• Зарезервируйте все ресурсы ЦП и памяти.

• Не перегружайте оборудование.

• Проверьте IOPS (операции ввода-вывода в секунду) хранения во всех узлах индексатора платформы Splunk одновременно, чтобы убедиться, что IOPS соответствует спецификации рекомендуемого оборудования, используемой в вашей среде. См. «Рекомендуемое оборудование» в *Руководстве по планированию емкости*

Недостаточная производительность хранилища является общей причиной плохого ответа на поиск и задержек при масштабировании платформы Splunk в виртуализованной среде.

Сведения о конфигурации VMware см. в технической документации: «Развертывание Splunk в виртуализованной среде: настройка виртуального оборудования VMware для запуска Splunk», доступных в Splunk Resources.

**Панель мониторинга**

Если вы активируете панель мониторинга в строке поиска Enterprise Security, она должна оставаться в автономном режиме. Подробнее о том, когда и как настраивать панель мониторинга в распределенной среде, см. раздел «В какой программе должна размещаться консоль?» в разделе *Мониторинг Splunk Enterprise*.

**Совместимость Enterprise Security с другими приложениями**

Enterprise Security основана на поддержке поиска и поддержке общей информационной модели (CIM), генерируемой надстройками. Надстройки отвечают за определение обработки событий, необходимых для оптимизации, нормализации и категоризации данных безопасности для использования с CIM. Только приложения, совместимые с CIM-приложениями, совместимы с Splunk Enterprise Security. Другие приложения и надстройки, не совместимые с CIM, могут включать в себя данные, которые не нормализованы для CIM, делая работу поисковых систем и панелей мониторинга, которые основаны на этих полях, невозможным.

Splunk Enterprise Security и компонент SA-VMNetAppUtils надстройки Splunk для VMware не могут быть установлены в одной и той же строке поиска. Конфликты с идентично названными файлами могут прервать правильную работу некоторых функций Splunk Enterprise Security.

**Планирование источника данных для Splunk Enterprise Security**

Объем, тип и количество источников данных влияют на общую архитектуру платформы Splunk, количество и размещение серверов, оценочную нагрузку, а также оказывают влияние на сетевые ресурсы.

Splunk Enterprise Security требует, чтобы все источники данных соответствовали общей информационной модели Splunk (CIM). Enterprise Security предназначена для использования стандартных моделей данных CIM как при поиске данных для заполнения панелей управления и представлений, так и при предоставлении данных для поиска корреляции.

**Сопоставление надстроек с источниками данных**

Надстройки, входящие в состав Splunk Enterprise Security, предназначены для анализа и классификации известных источников данных и других технологий для соответствия требованиям CIM.

Для каждого источника данных:

1. Определите надстройку: определите технологию и соответствующую надстройку. Основными источниками надстроек являются технологические специальные надстройки, поставляемые с Enterprise Security, и совместимый с CIM контент, доступный на Splunkbase. Если надстройка, которую вы хотите использовать, еще не совместима с CIM, измените ее, чтобы поддерживать схемы данных CIM. Пример см. в разделе «Использование CIM для нормализации данных во время поиска» в *Руководстве надстройки общей информационной модели*.

2. Установите надстройку: установите надстройку в строке поиска Enterprise Security. Установите надстройки, которые выполняют обработку индексным методом для каждого индексатора. Если архитектура сервера включает в себя отправку данных через синтаксический разбор или тяжелый сервер, возможно, может понадобиться надстройка для тяжелого сервера. Клиенты Splunk Cloud должны работать с поддержкой Splunk для установки надстроек в строках и индексаторах, а также несут ответственность за локальные серверы.

3. При необходимости сконфигурируйте сервер, устройство или технологию: активируйте журнал или сбор данных для устройства или приложения и/или настройте выход для сбора программой Splunk. Обратитесь к документации поставщика для получения пошаговой инструкции.

4. Настройте надстройку там, где это необходимо: может потребоваться наладка надстройки, например, настройка местоположения или источника данных, выбор того, находятся ли данные в файле или в базе данных или другие уникальные настройки.

5. Настройте ввод данных Splunk и подтвердите настройки для типа источника. Файл README надстройки содержит информацию об установках типа источника,

связанных с данными, и может содержать примечания по настройке параметров ввода.

***Рекомендации для ввода данных***

Программы платформы Splunk предоставляют несколько типов входных конфигураций для приема данных. В зависимости от собираемой технологии или источника выберите метод ввода, который соответствует требованиям к инфраструктуре, исходя из влияния производительности, простоты доступа к данным, стабильности, минимизации задержки источника и ремонтопригодности.

• **Мониторинг файлов**. Разверните сервер пересылки Splunk на каждой системе, в которой размещены файлы, и установите тип источника на сервере с использованием конфигурации ввода. Если у вас имеется большое количество систем с одинаковыми файлами, используйте сервер развертывания Splunk Enterprise для настройки стандартизованных входных файлов в больших группах серверов.

• **Мониторинг сетевых портов**: используйте стандартные инструменты, такие как сервер syslog, или создайте порты прослушивания на сервере. Отправка нескольких сетевых источников на один и тот же порт или файл усложняет ввод текста. Для получения дополнительной информации см. Документацию к платформе Splunk.

• Для Splunk Enterprise см. «Получение данных из портов TCP и UDP в Splunk Enterprise» *Получение данных*.

• Для Splunk Cloud см. «Получение данных из портов TCP и UDP в Splunk Cloud» *Получение данных*.

• **Мониторинг данных Windows**: сервер может получать информацию с программ Windows с использованием различных параметров конфигурации. Для получения дополнительной информации см. Документацию к платформе Splunk.

• Для Splunk Enterprise см. раздел «Как получить данные Windows в Splunk Enterprise» в Splunk Enterprise *Получение данных*.

• Для Splunk Cloud см. раздел «Как получить данные Windows в Splunk Enterprise» в Splunk Cloud *Получение данных*.

• **Мониторинг сетевых данных**: Splunk Stream поддерживает сбор данных в реальном времени. См. «О Splunk Stream» в *Руководстве по установке и настройке Splunk Stream*.

• **Входные данные в виде скрипта**: используйте скрипт сходных данных для получения данных из ПИ (пользовательский интерфейс) или других удаленных интерфейсов данных и очередей сообщений. Настройте сервер для вызова скриптов оболочки, скриптов Питона, командных файлов Windows, PowerShell или любой другой

утилиты, которая может форматировать и передавать данные, которые вы хотите подвергнуть индексированию. Вы также можете записать собранные данные при помощи любого скрипта в файл для непосредственного мониторинга с помощью сервера. Для получения дополнительной информации см. Документацию к платформе Splunk.

• Для Splunk Enterprise см. «Получение данных из ПИ и других удаленных интерфейсов данных через сценарий ввода данных в Splunk Enterprise» *Получение данных*.

• Для Splunk Cloud см. «Получение данных из ПИ и других удаленных интерфейсов данных через сценарий ввода данных в Splunk Cloud» *Получение данных*.

**Сбор данных и идентификация**

Splunk Enterprise Security сравнивает данные и идентификаторы с событиями на платформе Splunk для обеспечения обновления данных и дополнительного контекста для анализа. Собирайте и добавляйте информацию о своих данных и идентификаторах в Splunk Enterprise Security, чтобы воспользоваться преимуществами обновления данных. См. «Добавление данных и идентификаторов для Splunk Enterprise Security» в разделе *Администрирование Splunk Enterprise Security*.

**Установка**

**Установка Enterprise Security**

Установите Splunk Enterprise Security на локальный поисковый сервер. Клиенты Splunk Cloud должны работать с Splunk Support для координации доступа к строке поиска Enterprise Security.

**Предварительные требования к установке**

• Изучите требования платформы Splunk для Splunk Enterprise Security. См. раздел Планирование развертывания.

• Если сервер развертывания управляет любыми приложениями или надстройками, входящими в состав Splunk Enterprise Security, удалите файл deploymentclient.conf, содержащий ссылки на сервер развертывания и перезапустите службы Splunk. Если вы этого не сделаете, установка не будет завершена.

• Ваша учетная запись пользователя должна иметь роль администратора и функцию edit\_local\_apps. У роли администратора есть данная функция по умолчанию.

**Шаг 1. Загрузите Splunk Enterprise Security**

1. Зарегистрируйтесь на сайте splunk.com под вашим именем и паролем на Splunk.com.

2. Загрузите последний продукт Splunk Enterprise Security. Вы должны быть лицензированным клиентом Enterprise Security для загрузки продукта.

3. Нажмите «**Download**» и сохраните файл продукта Splunk Enterprise Security на рабочем столе.

4. Войдите в раздел поиска в качестве администратора.

**Шаг 2. Установите Splunk Enterprise Security**

1. На панели инструментов Splunk выберите «**Apps**» > «**Manage Apps**» и нажмите «**Install App from File**».

2. Нажмите «**Choose File**» и выберите файл продукта Splunk Enterprise Security.

3. Нажмите «**Upload**», чтобы начать установку.

4. Нажмите «**Set up now**», чтобы начать настройку «Splunk Enterprise Security».

**Шаг 3. Настройка безопасности Splunk Enterprise Security**

1. Нажмите «**Start**».

2. На странице «**Конфигурация после установки Splunk Enterprise Security»** указывается статус перемещения программы по этапам установки.

3. Выберите опцию «исключить выбранные надстройки из установки» или отключите их. Когда настройка будет завершена, страница предложит вам перезапустить службы платформы Splunk.

4. Нажмите «**Restart Splunk**», чтобы завершить установку.

Установка Enterprise Security включает протокол SSL в строке поиска. Вы должны изменить URL-адрес Splunk на https для доступа к строке поиска после установки ES.

По завершении установки просмотрите журнал установки:

$SPLUNK\_HOME/var/log/splunk/essinstaller2.log.

**Шаг 4. Конфигурация Enterprise Security**

Чтобы продолжить настройку Splunk Enterprise Security, см. следующие данные:

1. Развертывание надстроек, включенных в Splunk Enterprise Security

2. Настроить и развернуть индексы

3. Настроить пользователей и роли

4. Настроить модели данных

Обзор источников данных и рекомендаций по сбору данных для Enterprise Security см. в разделе Планирование источника данных.

**Установка Splunk Enterprise Security из командной строки**

Установите Splunk Enterprise Security с помощью командной строки Splunk. Подробнее о командной строке Splunk см. В разделе «CLI».

1. Выполните шаг 1: Загрузка Splunk Enterprise Security, чтобы загрузить Splunk Enterprise Security и поместить его в строку поиска.

2. Запустите процесс установки в строке поиска. Выполните шаг 2: установите Splunk Enterprise Security или выполните вызов REST, чтобы запустить установку из командной строки сервера.

Например: curl -k -u admin:password

https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v

3. В строке поиска используйте командную строку программного обеспечения Splunk для запуска следующей команды:

splunk search '| essinstall' -auth admin:password

Вы также можете запустить эту команду поиска из Splunk Web и просмотреть результаты установки в виде результатов поиска.

| essinstall

4. (Опциональный). Вы можете использовать дополнительные параметры для указания надстроек для установки, пропустить установку или отключиться после установки.

|essinstall --install-ta <ta-name>+ --skip-ta <ta-name>+ --disable-ta <ta-name>+

Укажите имя надстройки для установки, пропуска или отключения или используйте \* в качестве подстановочного знака. Используйте +, чтобы указать несколько надстроек для установки.

Если вы запустите команду поиска для установки Enterprise Security в Splunk Web, вы можете просмотреть ход установки в виде результатов поиска. Если вы запустите команду поиска из командной строки, вы можете просмотреть журнал установки:

$SPLUNK\_HOME/var/log/splunk/essinstaller2.log.

***Тестирование установки и настройки Splunk Enterprise Security***

Вы можете протестировать установку и настройку Splunk Enterprise Security:

1. Выполните шаг 1: Загрузка Splunk Enterprise Security, чтобы загрузить Splunk Enterprise Security и поместить его в строку поиска.

2. Запустите процесс установки в строке поиска. Выполните шаг 2: установите Splunk Enterprise Security или выполните вызов REST, чтобы запустить установку из командной строки сервера.

Например: curl -k -u admin:password

https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v

3. Из Splunk Web откройте приложение «Поиск и отчетность».

4. Введите следующий поиск, чтобы выполнить пробный прогон установки и настройки.

|essinstall --dry run

5. (Опциональный). Вы можете использовать дополнительные параметры для указания надстроек для установки, пропустить установку или отключиться после установки.

|essinstall --install-ta <ta-name>+ --skip-ta <ta-name>+ --disable-ta <ta-name>+

Укажите имя надстройки для установки, пропуска или отключения или используйте \* в качестве подстановочного знака. Используйте +, чтобы указать несколько надстроек для установки.

**Установка Splunk Enterprise Security в среду кластера в строке поиска**

Splunk Enterprise Security имеет специфические требования и процессы для реализации кластеров в системе поиска.

• Обзор кластеризации строки поиска см. в главе «Архитектура кластера поиска» в *Руководстве по распределенному поиску*.

• Полный список требований к кластеризации строки поиска см. в разделе «Требования к системе и другие рекомендации по развертыванию для кластеров строки поиска» в *Руководстве по распределенному поиску*.

Если вы устанавливаете Enterprise Security в существующую кластерную среду поиска, в которой могут быть установлены другие приложения, следуйте инструкциям в этом разеделе. Будьте осторожны, чтобы не изменить и не удалить папку $SPLUNK\_HOME/etc/shcluster/apps.

**Необходимые условия для установки Enterprise Security в среде кластера поиска.**

Перед установкой Enterprise Server в среду кластера поиска, убедитесь, что у вас есть:

• Функция развертывания и одна промежуточная версия (экземпляр) (где сначала установлена ​​ Enterprise Security)

• На функции развертывания, промежуточной версии и узлах кластера строки поиска находится такая же версия Splunk

• На узлах кластера развертывания и узлах поиска такое же приложение (не включая Enterprise Security)

• На функции развертывания, промежуточной версии и узлах SHC такая же версия Enterprise Security

• Выполнено резервное копирование etc/shcluster/apps в функции развертывания перед установкой Enterprise Security

• Выполнено резервное копирование файлов etc/apps из одного из узлов кластера строки поиска

• Выполнено резервное копирование KVstore из одного из узлов кластера строки поиска

**Установка Enterprise Security в среду кластера в строке поиска**

Чтобы установить Enterprise Security в кластер для поиска:

1. Подготовьте промежуточную версию. Используйте промежуточную версию для подготовки Enterprise Security для функции развертывания. Если у вас нет промежуточной версии, вы можете использовать версию для тестирования или QA Splunk Enterprise, которая не имеет других установленных приложений. Промежуточную версию нельзя подключить к производственным индексаторам или поисковым узлам. Используйте промежуточную версию для изменений конфигурации и обновлений.

2. Установите Enterprise Security в промежуточной версии.

3. Перенесите установку Enterprise Security в функцию развертывания. Скопируйте приложения, SA, DA и TA, связанные с Splunk Enterprise Security Suite, из $SPLUNK\_HOME/etc/apps на промежуточной версии в $SPLUNK\_HOME/etc/shcluster/apps в функции развертывания. Не копируйте всю папку, чтобы не включать приложения по умолчанию, такие как приложение для поиска.

4. Используйте функцию развертывания для развертывания Enterprise Security для элементов кластера. Из функции развертывания выполните следующую команду: splunk apply shcluster-bundle

**Управление изменениями конфигурации в кластере поиска**

Некоторые изменения конфигурации системы должны быть развернуты с помощью функции развертывания.

1. Вместо внесения изменений в элемент кластера в поисковой системе внесите изменения в промежуточную версию.

2. Проверьте изменения конфигурации в промежуточной версии.

3. Перенесите необходимые файлы в функцию развертывания кластера поиска.

4. Разверните обновленную конфигурацию в кластере поиска.

Изменения конфигурации, которые должны быть развернуты с помощью развертывающего устройства:

|  |  |
| --- | --- |
| **Изменение конфигурации** | **Измененный файл** |
| Включение или отключение индексированных поисков в режиме реального времени на странице «Общие настройки». | inputs.conf |
| Изменение индексированной задержки синхронизации диска в реальном времени на странице «Общие настройки». | inputs.conf |
| Отправка существенных событий в Splunk UBA на странице настройки UBA. | inputs.conf |

Большинство изменений конфигурации, которые вы делаете в кластере поисковой системы, автоматически реплицируются в другие элементы кластера. Например:

• Добавление, изменение и отключение источников угроз

• Добавление, изменение и отключение списков источников и идентификаторов

• Изменения в пользовательском интерфейсе

• Изменения в результатах поиска

См. раздел «Как изменения конфигурации распространяются в кластере поиска» в *Руководстве по распределенному поиску*.

**Перенесение существующего развертывания**

Вы не можете добавить элемент поиска Enterprise Security или элемент заголовка поиска непосредственно в кластер функции поиска. Чтобы перенести конфигурации ES в кластер для поиска:

1. Определите любые пользовательские конфигурации и модификации в предыдущей установленной ES. Удостоверьтесь, что локальная копия ess\_setup.conf, которая может конфликтовать с параметром по умолчанию при развертывании Enterprise Security в кластере, отсутствует.

2. Введите новый кластер строки поиска.

3. Разверните последнюю версию Enterprise Security в кластере поиска.

4. Просмотрите и перенесите настроенные конфигурации в функцию развертывания кластера поиска, чтобы выполнить репликацию для элементов кластера.

5. Завершите работу старой строки поиска ES.

Для получения дополнительной информации см. раздел «Перенос из автономной поисковой системы в кластер строки поиска» в *Руководстве по распределенному поиску* Splunk Enterprise.

Для получения помощи в планировании развертывания Splunk Enterprise Security обратитесь в службу Splunk Professional Services.

**Резервное копирование и восстановление Splunk Enterprise Security в среде кластера строки поиска**

Создайте резервную копию и восстановите среду кластера строки поиска Splunk Enterprise Security (SHC) с, по меньшей мере, тремя узлами SHC. Все узлы в SHC должны работать с той же версией Splunk Enterprise Security. В случае сбоя может потребоваться восстановление среды SHC. Вам также может потребоваться восстановить одну строку поиска, если вы добавите узел в SHC.

Возьмите регулярные резервные копии из SHC, чтобы у вас была резервная копия с момента, когда среда функционировала правильно. Например, вы можете автоматизировать прием резервных копий каждый час. Выберите частоту создания резервных копий на основе целей точки восстановления.

Чтобы проверить работоспособность среды, вы можете использовать один из следующих способов:

• Команда CLI: ./splunk show shcluster-status ?verbose

• ОЗУ: /services/shcluster/status?advanced=1

На выходе найдите следующие поля:

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| dynamic\_captain | Имеет ли кластер динамически выбранный руководящий элемент. |
| stable\_captain | Находится ли руководящий элемент кластера в стабильном состоянии. |
| service\_ready\_flag | Имеет ли кластер достаточное количество элементов для поддержки коэффициента репликации. |
| splunk\_version | Все ли элементы, включая руководящий элемент кластера, запускают Splunk версию 7.1.0. |
| out\_of\_sync | Все ли узлы в настоящее время синхронизированы. |

***Резервное копирование среды кластера строки поиска***

Резервное копирование среды SHC путем резервного копирования хранилища KV, функции развертывания и узлов SHC. Процедура резервного копирования не требует отключения кластера SHC или любого узла в кластере.

**Резервное копирование хранилища KV**

Чтобы создать резервную копию хранилища KV, запустите следующую команду из CLI с узла SHC с последними данными:

splunk backup kvstore -auth "admin:<password>"

Эта команда создает файл архива в

$SPLUNK\_HOME/var/lib/splunk/kvstorebackup. Например, файл может быть назван kvdump\_example.tar.gz.

**Резервное копирование узлов кластера развертывания и поиска**

1. В функции развертывания выполните резервное копирование файлов в справочнике $SPLUNK\_HOME/etc/shcluster.

2. На узле SHC с самыми последними данными обратите внимание на идентификатор GUID из строфы shclustering из

$SPLUNK\_HOME/etc/system/local/server.conf. Эта информация необходима во время процесса восстановления.

3. На узле SHC с самыми последними данными выполните резервное копирование файлов в

$SPLUNK\_HOME/var/run/splunk/snapshot/$LATEST\_TIME-$CHECKSUM.bundle.

4. Создайте файл tar.gz из этих резервных копий.

***Восстановление из резервной копии среды кластера поиска***

Для восстановления из резервной копии необходима следующая информация:

• GUID из файла server.conf от одного из членов SHC до того, как вы начнете восстановление.

После восстановления кластера восстановленный кластер будет иметь тот же идентификатор GUID, что и резервная копия кластера.

• Резервная копия функции развертывания.

• Резервная копия узла SHC с последними данными.

• Резервная копия хранилища KV с узла SHC с последними данными.

Процедура восстановления требует закрытия SHC, но не хранилища KV.

**Восстановление функции развертывания**

1. В функции развертывания извлеките файл резервной копии функции развертывания в

$SPLUNK\_HOME/etc/shcluster.

2. Примените пакет с помощью следующей команды:

splunk apply shcluster-bundle

**Восстановление узлов кластера строки поиска**

Выполните следующие шаги для каждого узла SHC, который вы хотите восстановить:

1. Выполните следующую команду, чтобы остановить Splunk Enterprise Security:

stop splunk

2. Создайте временную папку и назовите ее temp.

3. Извлеките файл резервной копии узла SHC в справочник temp.

4. Переместите файл config.bundle из справочника temp в $SPLUNK\_HOME/etc.

5. Извлеките файл config.bundle в справочник $SPLUNK\_HOME/etc.

**Восстановление хранилища KV**

1. На узле SHC проверьте справочник

$SPLUNK\_HOME/var/lib/splunk/kvstorebackup, чтобы убедиться, что в нем есть файл резервной копии kvdump\_example.tar.gz, который вы хотите использовать для восстановления.

Если он не находится в этом справочнике, вручную скопируйте туда файл tar.gz. Обратите внимание, что резервный файл хранилища KV автоматически не реплицируется в каждом элементе SHC.

2. Убедитесь, что установлена Splunk Enterprise Security. Файл collections.conf необходим для завершения восстановления.

3. Для восстановления хранилища KV выполните следующую команду:

splunk restore kvstore -archiveName kvdump\_example.tar.gz

4. Восстановите пакет снимков, извлекая резервный файл tar из справочника

$SPLUNK\_HOME/var/run/splunk/snapshot в

$SPLUNK\_HOME/etc.

5. Повторите эти шаги на каждом узле SHC, который вы хотите восстановить. Восстановление KV-хранилища на одном узле SHC не приводит к тому, что хранилище KV автоматически реплицируется через каждый элемент SHC.

Записи, которые присутствуют в текущем хранилище KV и в резервной копии, обновляются и заменяются записями в резервной копии. Записи, находящиеся в текущем хранилище KV, но не в резервной копии, не удаляются и не затрагиваются каким-либо образом.

**Полное восстановление среды кластера строки поиска**

Завершите восстановление Splunk Enterprise Security из резервной копии в среде SHC.

1. В файле $SPLUNK\_HOME/etc/system/local/server.conf найдите shclustering.

2. Обновите идентификатор поля в этой строфе с помощью GUID, скопированного из файла server.conf во время резервного копирования.

3. Выполните следующую команду для перезапуска Splunk: splunk restart

**Развертывание надстроек, включенных в Splunk Enterprise Security**

В пакет Splunk Enterprise Security входит набор надстроек.

• Надстройки, содержащие «SA-» или «DA-» в названии, составляют структуру Splunk Enterprise Security. Вам не нужно предпринимать никаких дополнительных действий для развертывания или настройки этих надстроек, поскольку их установка и настройка обрабатываются как часть процесса установки Splunk Enterprise Security. Не запрещайте никаких надстроек, которые составляют базу Splunk Enterprise Security.

• Остальные надстройки содержат в названии «TA-» и являются технологическими, они предоставляют данные, совместимые с CIM, необходимые

для включения этих исходных данных в Enterprise Security.

Дополнительные сведения о взаимодействии различных типов надстроек с Splunk Enterprise Security см. в разделе «Об архитектуре решения ES на портале разработчиков Splunk». Специфичные технологические надстройки поддерживаются иначе, чем надстройки, составляющие структуру Splunk Enterprise Security. См. раздел «Поддержка безопасности Splunk Enterprise Security и дополнительные надстройки» в *Руководстве по версии.*

Развертывание технологических надстройки зависит от архитектуры развертывания платформы Splunk.

**Необходимые условия**

Установите Splunk Enterprise Security в свой поисковый сервер или в поисковый кластер. См. Установка Enterprise Security. Когда вы устанавливаете Splunk Enterprise Security в распределенной среде, устройство устанавливает и включает надстройки, входящие в пакет Enterprise Security, в строке поиска или кластере поиска.

**Стадии**

1. Определите, какие надстройки необходимы для установки на серверах

2. Выполните развертывание надстроек для серверов

3. Выполните развертывание надстроек для индексаторов

**Определение надстроек для установки на серверах пересылки**

Установите надстройки, которые собирают данные на серверах пересылки. Определите, какие надстройки необходимы для установки на серверах пересылки, и какой тип конфигурации серверов требуется каждой надстройке, просмотрев документацию для надстроек.

Большинство надстроек включают параметры ввода для определенного источника данных. Просмотрите inputs.conf, включенный в надстройку, и разверните надстройку для сервера. Некоторые надстройки необходимо развернуть на серверах, установленных непосредственно в системе источника данных. Другие надстройки требуют тяжелых серверов. См. документацию или файл README для каждой надстройки, чтобы получить более подробную информацию и инструкции.

• Для надстроек с веб-документацией следуйте приведенным ниже ссылкам, чтобы определить, где их нужно установить и настроить.

• Для надстроек, которые не имеют веб-документации, см. файл README, входящий в корневую папку надстройки.

**Развертывание надстроек для серверов пересылки**

См. «Установка надстройки в распределенном развертывании Splunk Enterprise» в документации по надстройкам Splunk.

***Специфичные технологические надстройки, поставляемые с Enterprise Security***

Splunk Enterprise Security включает следующие надстройки безопасности и CIM-совместимые надстройки.

• Надстройка Splunk для Blue Coat ProxySG

• Надстройка Splunk для Bro IDS

• Надстройка Splunk для McAfee

• Надстройка Splunk для Juniper

• Надстройка Splunk для Microsoft Windows

• Надстройка Splunk для Tenable

• Надстройка Splunk для NetFlow

• Надстройка Splunk для Oracle

• Надстройка Splunk для OSSEC

• Надстройка Splunk для RSA SecurID

• Надстройка Splunk для Sophos

• Надстройка Splunk для FireSIGHT

• Надстройка Splunk для Symantec Endpoint Protection

• Надстройка Splunk для UBA

• Надстройка Splunk для Unix и Linux

• Надстройка Splunk для WebSense Content Gateway

• TA-AirDefense

• TA-alcatel

• TA-cef

• TA-fortinet

• TA-ftp

• TA-nmap

• TA-tippingpoint

• TA-trendmicro

**Развертывание надстроек для индексаторов**

Splunk рекомендует устанавливать надстройки, поддерживаемые Splunk, на все развертывание платформы Splunk, а затем включать и настраивать входные данные только там, где они требуются. Дополнительные сведения см. в разделе «Где устанавливать надстройки Splunk» в документации по надстройкам Splunk.

Процедура, используемая для развертывания надстроек для вашего индексатора, может зависеть от развертывания платформы Splunk. Выберите вариант, соответствующий вашей ситуации или предпочтениям.

|  |  |
| --- | --- |
| **Ситуация развертывания** | **Процедура** |
| Splunk Enterprise Security работает на Splunk Cloud. | Обратитесь в службу поддержки Splunk и попросите их установить необходимые дополнения к вашим индексаторам. |
| Вы предпочитаете развернуть надстройки для индексаторов вручную. | См. «Установка надстройки в распределенном развертывании Splunk Enterprise». |
| Ваши индексаторы кластеризованы, вы используете мастер кластера для развертывания надстроек для единичных узлов вашей локальной установки Splunk-платформы, дополнительная сложность развертывания отсутствует. | Создайте Splunk\_TA\_Forlndexers и управляйте развертыванием вручную |
| Ваши индексаторы не кластеризованы, вы используете сервер развертывания для управления настройками индексатора вашей локальной установки Splunk-платформы, дополнительная сложность развертывания отсутствует. | Создайте и настройте автоматическое развертывание Splunk\_TA\_Forlndexers |
| Splunk Enterprise Security работает на сложном развертывании, например, одна поисковая строка Enterprise Security и одна поисковая строка для других поисков, используется один и тот же набор индексов. | Обратитесь в службу поддержки Splunk и попросите их установить необходимые дополнения к вашим индексаторам. |

***Создание Splunk\_TA\_Forlndexers и выполнение управления развертыванием вручную.***

Используйте эту процедуру только в том случае, если Splunk Enterprise Security работает на сервере Splunk Enterprise, а не в Splunk Cloud, индексирование кластеризовано, и дополнительная сложность развертывания отсутствует. Если это не соответствует вашей ситуации развертывания, см. раздел «Развертывание необходимых надстроек для индексаторов» для выбора другого метода развертывания.

Управление распределенной конфигурацией собирает индексно-временные конфигурации и определения основных индексов в пакет Splunk\_TA\_Forlndexers, чтобы упростить развертывание дополнительных конфигураций локальным индексаторам. Splunk\_TA\_ForIndexers включает в себя все параметры indexex.conf и индексно-временные props.conf и transforms.conf файлы из всех включенных приложений и надстроек в строке поиска, объединяет их в единые файлы indexex.conf, props.conf и transforms.conf и помещает файлы в одну надстройку для загрузки. Система работает аналогично выходным данным

./splunk cmd btool <conf\_file\_prefix> list.

Эта процедура развертывает все надстройки, которые включены в вашем поисковой строке, для ваших индексаторов. Если вы хотите ограничить перечень надстроек, которые вы развертываете для своих индексаторов, только до подмножества, которые строго необходимы для индексаторов, выберите «**Apps > Manage Apps**» и отключите все надстройки, которые не требуются для индексаторов, прежде чем приступить к этой процедуре, затем снова включите их после завершения процедуры.

Перед развертыванием Splunk\_TA\_Forlndexers убедитесь, что существующие надстройки, установленные на индексаторах, не включены в пакет Splunk\_TA\_Forlndexers. Развертывание одних и тех же надстроек дважды может привести к конфликтам конфигурации, особенно если надстройки представляют собой разные версии.

1. В строке меню Enterprise Security выберите «**Configure > General > Distributed Configuration Management**».

2. Нажмите «**Download the Package**».

3. Выберите содержимое для пакета. Для загрузки пакета необходимо выбрать хотя бы один из следующих вариантов.

1. (Опциональный) Установите флажок **Include index time properties,** чтобы включить файлы props.conf и transforms.conf в пакет.

2. (Опциональный) Установите флажок **Include index definitions**, чтобы включить файл indexes.conf в пакет.

4. Нажмите «**Download the Package**», чтобы создать и загрузить Splunk\_TA\_ForIndexers.

5. После загрузки надстройки вы можете изменить содержимое пакета. Например, измените indexes.conf, чтобы файл соответствовал настройкам сохранения сайта и другим параметрам хранилища.

6. Используйте мастер кластера для развертывания Splunk\_TA\_Forlndexers или надстроек для единичных узлов кластера. См. «Управление общими конфигурациями для всех единичных узлов» и «Управление развертыванием приложений для всех единичных узлов» в разделе «*Управление индексаторами и кластерами индексаторов*».

Когда вы устанавливаете новую надстройку для использования с Enterprise Security, повторите эти шаги, чтобы создать обновленную версию Splunk\_TA\_ForIndexers.

***Создание и настройка автоматического развертывания Splunk\_TA\_Forlndexers***

Используйте эту процедуру только в том случае, если Splunk Enterprise Security работает на сервере Splunk Enterprise, индексирование не кластеризовано, и дополнительная сложность развертывания отсутствует. Если это не соответствует вашей ситуации развертывания, см. раздел «Развертывание необходимых надстроек для индексаторов» для выбора другого метода развертывания.

Управление распределенной конфигурацией собирает индексно-временные конфигурации и определения основных индексов в пакет Splunk\_TA\_Forlndexers, чтобы упростить развертывание дополнительных конфигураций локальным индексаторам. Splunk\_TA\_ForIndexers включает в себя все параметры indexex.conf и индексно-временные props.conf и transforms.conf файлы из всех включенных приложений и надстроек в строке поиска, объединяет их в единые файлы indexex.conf, props.conf и transforms.conf и помещает файлы в одну надстройку Splunk\_TA\_ForIndexers для загрузки. Если ваши конфигурации хранения и хранения индексатора одинаковы во всех индексаторах, вы можете добавить в пакет конфигурации indexes.conf.

Эта процедура развертывает все надстройки, которые включены в вашем поисковой строке, для ваших индексаторов. Если вы хотите ограничить перечень надстроек, которые вы развертываете для своих индексаторов, только до подмножества, которые строго необходимы для индексаторов, выберите «**Apps > Manage Apps**» и отключите все надстройки, которые не требуются для индексаторов, прежде чем приступить к этой процедуре, затем снова включите их после завершения процедуры.

Перед развертыванием Splunk\_TA\_Forlndexers убедитесь, что существующие надстройки, установленные на индексаторах, не включены в пакет Splunk\_TA\_Forlndexers. Развертывание одних и тех же надстроек дважды может привести к конфликтам конфигурации, особенно если надстройки представляют собой разные версии.

1. Настройте строку поиска Splunk Enterprise Security в качестве клиента развертывания сервера развертывания. См. раздел «Настройка клиентов развертывания» в *Руководстве по обновлению версий* Enterprise Splunk.

2. В строке меню Enterprise Security выберите «**Configure > General > Distributed Configuration Management**».

3. На вопрос **Do you want to use auto deployment?** выберите «**Yes**».

4. Выберите «**Add new credential»**, чтобы добавить учетную запись администрирования Splunk для использования с сервером развертывания. У учетной записи администратора должна быть роль администратора на сервере развертывания.

1. Введите пользователя (**User**) и пароль (**Password**) для учетной записи.

2. Установите **приложение** в SplunkEnterpriseSecuritySuite.

3. Сохраните учетные данные учетной записи.

5. Нажмите «**Select** **credentials**» и выберите учетные данные, которые вы добавили в шаге 4.

6. Выберите индексаторы, которые могут получать надстройку spiunk\_ \_TA\_ForIndexers.

7. (Опциональный). Добавьте дополнительные имена индексаторов, введя их в поле **Select Splunk Indexers**.

8. (Опциональный) Установите флажок **Push indexes.conf**, чтобы включить конфигурации indexes.conf в дополнительный пакет Splunk\_TA\_Forindexers. Поскольку для параметров индекса могут потребоваться конфигурации хранилища, indexes.conf по умолчанию не входит в пакет. Если вы не развертываете indexes.conf с Splunk\_TA\_Forindexers, управляйте конфигурациями индекса вручную.

9. Нажмите «**Save**», чтобы создать надстройку Splunk\_ TA\_ForIndexers.

Если вы отключили автоматическое развертывание Splunk\_TA\_ForIndexers после настройки автоматического развертывания, надстройка Splunk\_TA\_ForIndexers останется на сервере развертывания. Удалите надстройку на сервере вручную.

**Устранение неполадок автоматического развертывания Splunk\_TA\_ForIndexers**

Если вы настроили автоматическое развертывание Splunk\_TA\_ForIndexers, но оно не работает должным образом, выполните следующие действия для устранения неполадок.

|  |  |  |
| --- | --- | --- |
| **Проблема** | **Причина** | **Решение** |
| Строка поиска не взаимодействует с сервером развертывания. | Классы серверов, возможно, не были созданы процессом управления распределенной конфигурацией. | Проверьте serverclass.conf на сервера развертывания, чтобы определить, были ли успешно созданы классы серверов. |
| Приложение Splunk\_TA\_ForIndexers не было развернуто для индексаторов. | Проверьте репозиторий приложений развертывания на сервере развертывания. Возможно, приложение не было создано в репозитории приложений развертывания на сервере развертывания. | Проверьте es\_deployment\_manager.log для выявления ошибки, связанной с неудачным развертыванием конфигураций индекса-времени. |
| Автоматическое развертывание  не работает | Возможно, проблема с сервером развертывания, один из них не настроен. | Обратитесь в службу поддержки Splunk Support, чтобы устранить неисправность конфигурации сервера развертывания или настроить сервер развертывания для развертывания Splunk. См. «Управление сервером развертывания и управление сервером пересылки» в ​​разделе *Обновление версий Enterprise Splunk*. |

Ошибки и успешные загрузки приложения Splunk\_TA\_ForIndexers регистрируются в

es\_deployment\_manager.log.

**Импорт пользовательских приложений и надстроек в Splunk Enterprise Security**

Вы можете расширить функциональность Splunk Enterprise Security с помощью приложений и надстроек. Загрузите приложения и надстройки из Splunkbase или создайте собственную надстройку с помощью такого инструмента, как Splunk Add-on Builder. Клиенты Splunk Cloud должны работать с поддержкой Splunk для установки надстроек в строке поиска.

**Использование модульного ввода Update ES**

Splunk Enterprise Security объединяет конфигурации приложений и надстроек, установленных в одной и той же строке поиска. Модульный ввод Update ES отвечает за импорт всех приложений и надстроек, соответствующих фильтру регулярных выражений. Фильтр определен в пути приложения

SplunkEnterpriseSecuritySuite/default/inputs.conf.

|  |  |
| --- | --- |
| **Модульный ввод** | **Функция** |
| app\_imports\_update://update\_es | Импортирует и обновляет метаданные для поддержки надстроек. |
| app\_imports\_update://update\_es\_da | Импортирует и обновляет метаданные для домена надстроек. |
| app\_imports\_update://update\_es\_main | Импортирует и обновляет метаданные для SplunkEnterpriseSecuritySuite. |

**Импорт является транзитивным**

Импорт приложений является транзитивным. Это означает, что приложение (A), которое импортирует другое приложение (B), также импортирует все приложения (C), импортированные этим приложением.

1. Если приложение A импортирует B,

2. и приложение B импортирует C,

3. то A импортирует C.

Поскольку поддерживающие надстройки импортируют друг друга, вы можете увидеть только одну поддерживающую надстройку с обновленным файлом local.meta. Этим файлом является SA-AccessProtection, так как это первая поддерживающая надстройка в списке приложений.

**Просмотр существующих импортированных приложений**

Используйте команды поиска | rest для просмотра существующих импортированных приложений. Для выполнения этой команды у вас должны быть разрешения администратора Splunk. Например, для просмотра импорта для приложения SplunkEnterpriseSecuritySuite при аутентификации в качестве пользователя-администратора:

| rest

/servicesNS/admin/system/apps/local/SplunkEnterpriseSecuritySuite/import splunk\_server=local | fields import

**Соглашения о присвоении наименования приложениям и надстройкам**

Модульные вводы будут автоматически импортировать приложения и надстройки с с любыми из следующих префиксов: DA-ESS-, SA-, TA-, Splunk\_SA\_, Splunk\_TA\_ и Splunk\_DA-ESS\_.

**Импорт надстроек с другим соглашением о наименованиях**

Если в пользовательском дополнении не используются обычные соглашения об именах ES, вы должны добавить название или соглашение об именах к модулю ввода импорта.

1. На панели инструментов Enterprise Security откройте «**Configure > General**» и выберете «**App Imports** **Update**».

2. Отредактируйте ввод update\_es.

3. Обновите поле «**Application Regular Expression**», добавив соглашение о наименованиях вашей надстройки в список поддерживаемых соглашений о наименованиях с помощью регулярного выражения.

1. Например, чтобы импортировать новую надстройку с наименованием My\_datasource обновите поле «**Application Regular Expression**»:

(appsbrowser)|(search)|([ST]A-.\*)|(Splunk\_[ST]A\_.\*)|(DA-ESS-.\*)|(Splunk\_DA-ESS\_.\*)|(My\_datasou

2. При изменении поля «**Application Regular Expression**» всегда добавляйте к регулярному выражению по умолчанию, в противном случае импорт существующего приложения не будет выполнен.

4. Сохраните.

5. Проведите предварительный просмотр изменений

|rest services/data/inputs/app\_imports\_update | table title app\_regex app\_exclude\_regex updated

6. Перезапустите службы Splunk Enterprise, чтобы активировать изменения.

**Удаление надстройки из импорта приложения.**

Исключите надстройку из процесса импорта приложения.

1. На панели инструментов Enterprise Security откройте «**Configure > General**» и выберете «**App Imports** **Update**».

2. Отредактируйте ввод update\_es.

3. Обновите поле «**Application Exclusion Regular Expression**», добавив соглашение о наименованиях вашей надстройки в список поддерживаемых соглашений о наименованиях с помощью регулярного выражения.

1. Например, чтобы исключить новую надстройку с наименованием TA\_new\_test обновите поле «**Application Exclusion Regular Expression**»:

|TA\_new\_test

4. Сохраните.

5. Проведите предварительный просмотр изменений

|rest services/data/inputs/app\_imports\_update | table title app\_regex app\_exclude\_regex updated

6. Перезапустите службы Splunk Enterprise, чтобы активировать изменения.

**Интеграция Splunk Stream в Splunk Enterprise Security**

Enterprise Security интегрируется с Splunk Stream для сбора и анализа данных сетевого трафика. Splunk Stream включает приложение (splunk\_app\_stream), которое вы устанавливаете в строке поиска и два параметра пересылки.

1. Установите приложение Splunk App для Stream в строку поиска Enterprise Security.

♦ Для развертывания Splunk Enterprise см. «Установка Splunk Stream» в *Руководстве по установке и настройке* Splunk Stream.

♦ Для развертывания Splunk Cloud см. «Развертывание потока Splunk в Splunk Cloud» в *Руководстве по установке и настройке* Splunk Stream.

2. Активируйте шаблон конфигурации для Splunk Enterprise Security на серевере пересылке Splunk Stream, который вы используете. Вы можете использовать надстройку Splunk для Stream (Splunk\_TA\_stream) или независимый сервер пересылки Stream. См. «Использование шаблонов конфигурации Stream».

**Использование Stream в Enterprise Security**

После настройки Splunk Stream вы можете запустить задание захвата потока в результате поиска корреляции. См. «Начать захват потока с помощью Splunk Stream» в документе *Администрирование Splunk Enterprise Security*. Вы также можете запустить задание захвата потока из существенного события на панели мониторинга событий. См. «Начать захват потока» в разделе «*Использование технологии Splunk Enterprise Security*».

Вы можете просматривать и анализировать данные потока, записанные в Splunk Enterprise Security, на панелях мониторинга протокола. См. «Панель мониторинга протокола Intelligence» в разделе «*Использование технологии Splunk Enterprise Security»*.

**Конфигурация и внедрение индексов**

Splunk Enterprise Security реализует пользовательские индексы для хранения событий. Индексы определены в приложениях, предоставляемых Splunk Enterprise Security.

• При развертывании одной версии установка Enterprise Security создает индексы в пути по умолчанию для хранения данных.

• При развертывании Splunk Cloud клиенты работают с поддержкой Splunk для настройки, управления и поддержки своих параметров индекса облака. См. раздел «Управление индексами Splunk Cloud» в *Руководстве пользователя Splunk Cloud*.

• В распределенном развертывании создайте индексы для всех индексаторов платформы Splunk или для однотипных функций поиска.

**Конфигурация индекса**

Индексы, определенные в Splunk Enterprise Security, не предоставляют параметры конфигурации для:

• Нескольких путей хранения

• Ускоренных моделей данных

• Хранения данных

• Размера корзины

• Использования параметров громкости.

Подробные примеры настройки индексов см. в indexes.conf.example в *Руководстве администратора* Splunk Enterprise.

**Индексы, создаваемые приложением**

|  |  |  |
| --- | --- | --- |
| **Контекст приложения** | **Индекс** | **Описание** |
| DA-ESS-AccessProtection | gia\_summary | Сводный индекс, используемый витриной «Географически невероятный доступ» на панели мониторинга доступа к аномалиям. |

|  |  |  |
| --- | --- | --- |
| DA-ESS-ThreatIntelligence | ioc | Не используется в этой версии. |
| threat\_activity | Содержит события, которые являются результатом сопоставления списка угроз. |
| SA-EndpointProtection | endpoint\_summary | Итоговый индекс защиты конечной точки. |
| SA-ThreatIntelligence | notable | Содержит существенные события. |
| notable\_summary | Содержит сводку статистических данных о существенных событиях, используемых на отдельных витринах. |
| risk | Содержит события модификатора риска. |
| SA-NetworkProtection | whois | Индекс данных WHOIS. |
| Splunk\_SA\_CIM | cim\_summary | Не используется в этой версии. |
| cim\_modactions | Содержит события адаптивного реагирования. |
| Splunk\_SA\_ExtremeSearch | xtreme\_contexts | Содержит контексты для экстремального поиска. |

Надстройки могут включать пользовательские индексы, определенные в файле indexes.conf.

***Разворачивание индекса***

Splunk Enterprise Security включает в себя инструмент для настройки сбора indexes.conf и индексирования времени index-time: transforms.conf из всех активных приложений надстроек в строке поиска, а также позволяет объединить их в одной надстройке. Для получения дополнительной информации см. раздел «Развертывание надстроек, включенных в Splunk Enterprise Security» в данном руководстве.

**Конфигурация пользователей и ролей**

Splunk Enterprise Security использует систему управления доступом, интегрированную с платформой Splunk. Авторизация платформы Splunk позволяет добавлять пользователей, назначать пользователям роли и назначать эти роли для пользовательских **возможностей** обеспечения гранулярного контроля доступа на основе ролей для вашей организации.

Splunk Enterprise Security использует пользователя admin для запуска сохраненных поисков. Если вы планируете удалить пользователя admin, обновите объекты знаний, принадлежащие этому пользователю, прежде чем вы произведете такое удаление.

• Для Splunk Enterprise см. раздел «Переназначение одного или нескольких общих объектов знаний новому владельцу» в *Руководстве управления знаниями*.

• Для Splunk Cloud см. раздел «Переназначение одного или нескольких общих объектов знаний новому владельцу» в *Руководстве управления знаниями*.

**Настройка ролей пользователей**

Splunk Enterprise Security добавляет три роли к ролям по умолчанию, предоставляемым платформой Splunk. Новые роли позволяют администратору Splunk назначать доступ к определенным функциям в ES на основе требований пользователя к доступу. Администратор платформы Splunk может назначать группам пользователей те роли, которые наилучшим образом соответствуют задачам, которые пользователи будут выполнять в системе Splunk Enterprise Security. Существует три категории пользователей.

|  |  |  |
| --- | --- | --- |
| **Пользователь** | **Описание** | **Роль ES Splunk** |
| Директор по безопасности | Понимание текущей ситуации безопасности организации, просмотр основной панели мониторинга безопасности, центра защиты и проверки. Директор службы безопасности не настраивает продукт и не управляет событиями. | ess\_user |
| Аналитик по безопасности | Использует панели мониторинга безопасности и проверки событий для управления и расследования инцидентов безопасности. Аналитики по безопасности также несут ответственность за проверку центров защиты и определяют сущность события. Они также определяют пороговые значения, используемые поисками корреляции и панелями мониторинга. Аналитик по безопасности должен иметь возможность редактировать корреляционные поиски и создавать ограничения. | ess\_analyst |
| Администратор по принятию решений | Устанавливает и поддерживает установки платформы Splunk и Splunk Apps. Этот пользователь отвечает за настройку рабочих процессов, добавление новых источников данных, настройку и устранение неполадок приложения. | admin или  sc\_admin |

Каждая индивидуальная роль в Splunk Enterprise Security наследуется от ролей платформы Splunk и добавляет возможности, характерные для Splunk ES. Не все три роли, которые настраиваются для Splunk ES, могут быть назначены пользователям.

|  |  |  |  |
| --- | --- | --- | --- |
| **Роль ES Splunk** | **Наследственные признаки от роли в платформе Splunk** | **Добавленные возможности в ES Splunk** | **Может быть назначено пользователям** |

|  |  |  |  |
| --- | --- | --- | --- |
| ess\_user | user | Поиск в режиме реального времени, кластеризация списка строки поиска | Да. Заменить роль user для ES пользователей |
| ess\_analyst | user,  ess\_user,  power | Наследует ess\_user и добавляет возможности для создания, редактирования и владения существенными событиями, выполняет все переходы, редактирование системы «стеклянный стол», создание и изменение расследований. | Да. Заменить роль power для ES пользователей |
| ess\_admin | user,  ess\_user,  power,  ess\_analyst | Наследует ess\_analyst и добавляет несколько других возможностей. | **Нет**. Для администрирования установки Enterprise Security необходимо использовать роль администратора платформы Splunk. |

См. возможности, характерные для Splunk Enterprise Security, для получения более подробной информации о том, какие функции назначены для ролей по умолчанию.

Роль admin платформы Splunk наследует все уникальные возможности ES. В развертывании Splunk Cloud роль администратора платформы Splunk называется sc\_admin. Используйте admin или sc\_admin для администрирования установки Enterprise Security.

|  |  |  |  |
| --- | --- | --- | --- |
| **Роль в платформе Splunk** | **Наследственные признаки от роли** | **Добавленные возможности** | **Принимает назначение пользователя** |
| admin | user, ess\_user, power, ess\_analyst, ess\_admin | Все | Да |
| sc\_admin | user, ess\_user, power, ess\_analyst, ess\_admin | Все | Да |

***Наследование ролей***

Наследование роли предварительно сконфигурировано в Enterprise Security. Если возможности какой-либо роли будут изменены, другие наследственные роли также будут изменены. Дополнительные сведения о ролях см. документации к платформе Splunk.

• Для Splunk Enterprise см. раздел «Добавление и изменение ролей» в документе *Безопасность Splunk Enterprise*.

• Для Splunk Cloud см. раздел «Управление ролями Splunk Cloud» в *Руководстве пользователя* *Splunk Cloud*.

**Добавление возможностей в роль**

Возможности контролируют уровень доступа, который роли обеспечивают к различным функциям в Splunk Enterprise Security. Используйте страницу «**Permissions**» в Enterprise Security для просмотра и изменения возможностей, назначенных ролям.

1. В строке меню Splunk Enterprise Security выберите «**Configure > General > Permissions**».

2. Найдите роль, которую вы хотите обновить.

3. Найдите **Component ES**, который вы хотите добавить.

4. Установите флажок для компонента для роли.

5. Сохраните.

***Возможности, специфичные для Splunk Enterprise Security***

Splunk Enterprise Security использует настраиваемые возможности для управления доступом к функциям Splunk Enterprise Security.

Добавьте возможности на странице разрешений в Splunk Enterprise Security, чтобы убедиться, что списки управления доступом (ACL) обновлены. Страница разрешений делает изменения ACL для вас. Если вы добавите эти пользовательские возможности на странице настроек платформы Splunk, вы должны обновить ACL самостоятельно.

|  |  |  |
| --- | --- | --- |
| **Функция в ES** | **Описание** | **Способность** |
| Создание новых существенных событий | Создание ситуативных событий на основе результатов поиска. См. «Создать вручную существенное событие в Splunk Enterprise Security». | edit\_notable\_events |
| Изменение настроек расширенного поиска | Редактирование приоритета расписания и окна расписания поиска корреляции в Content Management. | edit\_search\_schedule\_priority  edit\_search\_schedule\_window |
| Редактирование поиска корреляции | Редактирование поиска корреляции в Content Management. См. раздел «Настройка поиска корреляции в программе Splunk Enterprise Security». Пользователи с этой возможностью могут также экспортировать контент из Content Management в качестве приложения. См. раздел «Экспорт содержимого в виде приложения из Splunk Enterprise Security». | edit\_correlationsearches  schedule\_search |

|  |  |  |
| --- | --- | --- |
| Редактирование управления  распределенной  конфигурацией | Использование распределенного управления конфигурацией. См. раздел «Развертывание надстроек, входящих в состав Splunk Enterprise Security». | edit\_modinput\_es\_deployment\_manager |
| Редактирование навигации ES | Внесение изменений в навигацию Enterprise Security. См. «Настройка панели меню в Splunk Enterprise Security». | edit\_es\_navigation |
| Редактирование системы «стеклянный стол» | Создание и изменение системы «стеклянный стол». См. «Создание системы «стеклянный стол». | edit\_glasstable |
| Редактирование вида конфигурации | Управление конфигурацией поиска идентичности и ограничение корреляции активов и идентификаций. См. раздел «Добавление данных об активах и идентификационных данных для Splunk Enterprise Security» и «Настройка корреляции активов и идентификаций в Splunk Enterprise Security». | edit\_identitylookup |
| Редактирование просмотра инцидентов (событий) | Внесение изменений в настройки проверки инцидентов. См. «Настроить обзор инцидентов в Splunk Enterprise Security». | edit\_log\_review\_settings |
| Изменение просмотра | Создание и внесение изменений в файлы таблицы поиска. См. раздел «Создание и управление поиском в Splunk Enterprise Security». | edit\_lookups, edit\_managed\_configurations |
| Редактирование статусов | Внесение изменений в статусы, доступные для проведения расследований и существенных событий. См. «Управление статусами существенных событий». | edit\_reviewstatuses |
| Редактирование запретов существенных событий | Создание и редактирование запретов существенных событий. См. раздел «Создание и управление запретами существенных событий». | edit\_suppressions |

|  |  |  |
| --- | --- | --- |
| Редактирование существенных событий | Внесение изменений в существенные события, такие как их назначение и переход между статусами.  transition\_reviewstatus-X\_to\_Y  способность также позволяет аналитикам переходить между статусами расследования. См. «Заметки о событиях, связанных с инцидентом, в журнале Splunk Enterprise Security». | edit\_notable\_events  transition\_reviewstatus-X\_to\_Y |
| Редактирование фильтров для витрины | Разрешение роли обновления фильтров на панели мониторинга. См. раздел «Настройка фильтрации на каждой витрине в Splunk Enterprise Security». | edit\_per\_panel\_filters |
| Редактирование загрузок | Измените настройки загрузки справки. См. Загрузка загрузочного фида угроз из Интернета в Splunk Enterprise Security и загрузка фида интеллектуальных данных из Интернета в Splunk Enterprise Security. | edit\_modinput\_threatlist  edit\_modinput\_threat\_intelligence\_manager |
| Редактирование БД угроз | Загрузка информации об угрозах и выполнение операции CRUD в БД угроз с использованием REST API. См. «Загрузка пользовательского CSV-файла с информацией об угрозе в Splunk Enterprise Security» и «Справочная информация об угрозе в API». | edit\_threat\_intel\_collections |
| Управление всеми расследованиями | Позволяет роли просматривать и вносить изменения во все расследования. См. «Управление расследованиями безопасности в Splunk Enterprise Security». | manage\_all\_investigations |
| Собственные существенные события | Позволяет роли быть владельцем существенным событий. См. раздел «Назначить существенные события». | can\_own\_notable\_events |
| Поисковые запросы | Создание таблиц поиска, которые могут быть заполнены результатами поиска. См. раздел «Создание поисковых просмотров в Splunk Enterprise Security». | edit\_managed\_configurations  schedule\_search |
| Управление вашими расследованиями | Создание и редактирование расследования. Роли с этой возможностью могут вносить изменения в расследования, в которых они являются сотрудниками. См. «Расследование в сфере безопасности Splunk Enterprise». | edit\_timelines |

|  |  |  |
| --- | --- | --- |
| Менеджер учетных данных | Управление учетными данными и сертификатами для Splunk Enterprise Security и других приложений. Невозможно установить на странице «Permissions». См. «Управление учетными данными в Splunk Enterprise Security». | admin\_all\_objects  list\_storage\_passwords  list\_app\_certs  edit\_app\_certs  delete\_app\_certs |

**Регулирование параллельных поисков для роли**

Платформа Splunk определяет предел одновременного выполнения поисковых запросов для user и power по умолчанию. Возможно, вы захотите изменить эти параллельные поисковые запросы для некоторых ролей.

1. В строке меню Splunk Enterprise Security выберите «**Configure > General > General Settings**».

2. Просмотрите ограничения для ролей и измените их по желанию.

|  |  |
| --- | --- |
| **Параметр** | **Описание** |
| Поиск дисковой квоты (admin) | Максимальная емкость диска (МВ), которые пользователь с ролью admin может использовать для хранения результатов рабочих поисков |
| Поиск рабочей квоты (admin) | Максимальное количество одновременных поисковых запросов для пользователей с ролью admin |
| Поиск рабочей квоты (power) | Максимальное количество одновременных поисковых запросов для пользователей с ролью admin |

Чтобы изменить ограничения для ролей, отличных от user и power, отредактируйте файл authorize.conf, чтобы обновить квоту поиска по умолчанию. См. файл authorize.conf.example в *Руководстве администратора* Splunk Enterprise.

**Конфигурация ролей для поиска множества индексов**

Платформа Splunk хранит запатентованные источники данных во множестве индексов. Распределение данных на несколько индексов позволяет использовать контроль доступа на основе ролей и изменять политики хранения для источников данных. Платформа Splunk настраивает все роли для поиска по умолчанию только для индекса main. Дополнительные сведения о работе с ролями см. в документации для платформы Splunk.

• Для Splunk Enterprise см. раздел «О настройке доступа пользователей на основе ролей» в *Руководстве по безопасности Splunk Enterprise*.

• Для Splunk Cloud см. «Управление пользователями и ролями в Splunk Cloud» в *Руководстве пользователя Splunk Cloud*.

Чтобы позволить ролям в Splunk Enterprise Security искать дополнительные индексы, присвойте соответствующим ролям индексы, содержащие соответствующие данные безопасности.

1. Выберите «**Settings > Access Controls**».

2. Нажмите «**Roles**».

3. Выберите имя роли, которое вы хотите разрешить для поиска дополнительных индексов.

4. Выберите индексы и индексы по умолчанию (**Indexes searched by default** и **Indexes**), которые может выполнять эта роль. Не включайте сводные индексы, так как это может вызвать цикл поиска и сгенерировать составной индекс.

5. Сохраните изменения.

6. Повторите процедуру для дополнительных ролей по мере необходимости.

Если вы не обновляете роли с правильными индексами, поисковые запросы и другие объекты знаний, которые полагаются на данные из неназначенных индексов, не будут обновлять или отображать результаты.

Дополнительные сведения о причинах необходимости множественных индексов см. в разделе «Почему необходимо множество индексов?» в докуете «*Управление индексами и кластерами индексов в Splunk Enterprise*».

**Конфигурация моделей данных для Splunk Enterprise Security**

Splunk Enterprise Security использует **ускоренные модели данных** для заполнения витрин и представлений и предоставления результатов корреляционного поиска. Модели данных определены и представлены в надстройке «Общая информационная модель» (Splunk\_SA\_CIM), которая включена в установку Splunk Enterprise Security. Enterprise Security также устанавливает уникальные модели данных, которые применяются только к материалу Splunk Enterprise Security.

**Поиск ускорения загрузки модели данных**

Модель данных ускоряется посредством запланированного процесса поиска суммирования, инициированного в строке поиска. Поиск суммирования выполняется на индексаторах в результате поиска новых индексированных данных при использовании модели данных в качестве фильтра. Полученные совпадения хранятся на диске вместе с индексом для быстрого доступа.

На платформах Splunk 6.3 и более поздних версиях для каждой модели данных для каждого индексатора может быть выполнено до двух одновременных запросов суммирования. Для получения дополнительной информации см. «Параллельное

суммирование» в *Руководстве по планированию емкости* Splunk Enterprise. Чтобы настроить параметры параллельного суммирования в Splunk Cloud, обратитесь в службу поддержки.

**Ограничение поиска модели данных по конкретным индексам**

Надстройка общей информации Splunk позволяет вам получать индексы, найденные моделью данных, для повышения производительности. См. раздел «Настройка надстройки общей информационной модели Splunk» в *Руководстве пользователя* для надстройки стандартной информационной модели Splunk.

**Конфигурация ускорения модели данных для моделей данных CIM**

Надстройка для Общей информационной модели в Splunk позволяет настраивать параметры ускорения модели данных для каждой модели данных, включая время обратного наполнения, максимальный одновременный поиск, ручные переопределения и приоритет планирования. Если вы используете платформу Splunk версии 6.6.0, настройте опцию «Белый список тегов», чтобы включить любые пользовательские теги, которые вы используете с моделями данных CIM. См. «Ускорение моделей данных CIM» в *Руководстве пользователя* для надстройки стандартной информационной модели Splunk.

**Ускорение хранения данных и сохранения данных**

Ускорение модели данных использует индексаторы для обработки и хранения, помещая ускоренные данные вместе с каждым индексом. Чтобы рассчитать емкость дополнительного хранилища, необходимого для индексаторов, исходя из общего объема данных, используйте формулу:

Хранилище ускоренной модели данных/год = Объем данных в день \* 3,4

Эта формула предполагает, что вы используете рекомендуемые скорости хранения для моделей с ускоренными данными.

Например, если вы обрабатываете 100 ГБ/день объема данных для использования с помощью Enterprise Security, вам потребуется примерно 340 ГБ дополнительного пространства для всех индексаторов, чтобы обеспечить ускорение модели хранения данных и сохранения исходных данных до одного года.

***Конфигурация объемов хранения***

Емкость хранения ускорения модели данных управляются в indexes.conf с помощью параметра tstatsHomePath. Путь хранения ускорения модели данных по умолчанию соответствует пути индекса по умолчанию для платформы Splunk $SPLUNK\_HOME/var/lib/splunk, если не задано иное. Хранилище, используемое для ускорения модели данных, не добавляется к расчетам

размеров индекса для задач технического обслуживания, таких как корзина и проверка свободного места.

Чтобы управлять хранилищем ускорения модели данных независимо от настроек индекса, вы должны определить новый путь хранения с помощью [volume:] выходов. Пример определения емкости и сохранения ускорения модели данных см. в документации к платформе Splunk.

• Для Splunk Enterprise см. раздел «Настройка хранения на основе размера» для суммирования моделей данных в *Руководстве по управлению знаниями* Splunk Enterprise Knowledge Manager.

• Для Splunk Cloud см. раздел «Настройка хранения на основе размера» для суммирования моделей данных в *Руководстве по управлению знаниями* Splunk Cloud.

***Удержание по умолчанию модели данных***

Параметры удержания (сохранения) модели данных зависят от прецедента и источников данных. Более короткое удержание использует меньше дискового пространства и требует меньшего времени обработки для поддержания в обмен на ограничение временного диапазона ускоренных данных.

|  |  |
| --- | --- |
| **Модель данных** | **Диапазон суммирования** |
| Предупреждения | Все время |
| Состояние приложения | 1 месяц |
| Данные и идентификаторы **(ES)** | Нет |
| Авторизация | 1 год |
| Сертификаты | 1 год |
| Анализ изменений | 1 год |
| БД | Нет |
| Предотвращение потери данных | 1 год |
| Анализ домена **(ES)** | 1 год |
| Электронная почта | 1 год |
| Управление событиями (**ES)** | Все время |
| Сообщения между процессами | 1 год |
| Определения вмешательства | 1 год |
| Приспособления | Нет |
| Виртуальные машины Java | Все время |
| Вредоносное ПО | 1 год |
| Разрешение сети (DNS) | 3 месяца |

|  |  |
| --- | --- |
| Сетевые сеансы | 3 месяца |
| Сетевой трафик | 3 месяца |
| Производительность | 1 месяц |
| Анализ рисков **(ES)** | Все время |
| Журналы проверки Splunk | 1 год |
| Угроза **(ES)** | Все время |
| Управление билетами | 1 год |
| Обновления | 1 год |
| Аналитика поведения пользователей и компаний **(ES)** | Все время |
| Уязвимость | 1 год |
| Web | 3 месяца |

Используйте страницу **CIM Setup** в приложении Splunk Common Information Model (стандартная информационная модель), чтобы изменить настройку хранения для моделей данных CIM. Дополнительные сведения см. в разделе «Изменение суммарного диапазона для ускорения модели данных» в *Руководстве пользователя* для надстройки стандартной информационной модели Splunk. Чтобы изменить суммируемый диапазон или другие настройки в пользовательской модели данных, вручную отредактируйте файл datamodels.conf, поставляемый с приложением или надстройкой.

• Инструкции по редактированию этих параметров в Splunk Enterprise см. в файле спецификации datamodels.conf в *Руководстве администратора* Splunk Enterprise.

• Если вы используете Splunk Cloud, обратитесь в службу поддержки, чтобы настроить эти параметры.

**Поведение восстановления модели данных**

В платформе Splunk, если изменяется конфигурация модели данных или основной поиск, создающий изменения модели данных, начинатся полная перестройка ускорения модели данных. Enterprise Security изменяет поведение по умолчанию, применяя изменения конфигурации модели данных только к самым последним ускорениям и предотвращая удаление предыдущих ускорений. Индексаторы сохраняют все существующие модели ускоренных данных с предварительной конфигурацией до тех пор, пока не будет достигнут определенный период хранения или отправлены в корзину индексов. Для улучшения производительности не изменяйте настройку вручную для любых моделей данных, используемых Splunk Enterprise Security.

• Параметры перестройки конфигурации управляются в файле datamodels.conf.

Дополнительные сведения об ускорении и восстановлении см. в документации к платформе Splunk.

• Для Splunk Enterprise см. раздел «Расширенные конфигурации для постоянно ускоренных моделей данных» в *Руководстве по управлению знаниями* Splunk Enterprise.

• Для Splunk Cloud см. раздел «Расширенные конфигурации для постоянно ускоренных моделей данных» в *Руководстве по управлению знаниями* Splunk Cloud.

• Используйте страницу **Data Models management**, чтобы принудительно выполнить полную перестройку. Перейдите в «**Settings > Data Models**», выберите модель данных, используйте стрелку влево, чтобы развернуть строку, и выберите ссылку «**Rebuild**».

• Чтобы просмотреть состояние ускорения для всех моделей данных, используйте панель мониторинга модели данных.

**Усиление ускорения модели данных**

Enterprise Security обеспечивает ускорение модели данных с помощью модульного ввода. Чтобы отключить ускорение для модели данных в ES:

1. На панели инструментов Splunk Enterprise откройте «**Settings > Data inputs** ивыберете **select Data Model Acceleration Enforcement Settings**».

2. Выберите модель данных.

3. Снимите флажок «**Acceleration Enforced** ».

4. Сохраните.

**Модели данных, используемые Splunk Enterprise Security**

Более детальная информация о моделях данных, используемых в Enterprise Security, см. «Модели данных, используемые ES» на портале разработчиков Splunk.

**Обновление**

**Планирование обновления системы Splunk Enterprise Security**

Планирование локального обновления Splunk Enterprise Security. Клиенты Splunk Cloud должны работать с поддержкой Splunk для координации обновлений для Enterprise Security.

Эта версия Splunk Enterprise Security поддерживает обновление версии 4.5.x или более поздней. Для обновления с более ранних версий выполните промежуточные обновления.

**Перед обновлением системы Splunk Enterprise Security**

1. Изучите совместимые версии платформы Splunk. См. Требования к системе Splunk Enterprise.

2. Изучите требования к оборудованию, чтобы убедиться, что ваше серверное оборудование поддерживает Splunk Enterprise Security. См. Требования к оборудованию.

3. Изучите известные проблемы с последней версией Splunk Enterprise Security. См. «Известные проблемы» в *Комментариях к версии* Splunk Enterprise Security.

4. Изучите устаревшие функции в последней версии Splunk Enterprise Security. См. «Устаревшие функции» в *Комментариях к версии* Splunk Enterprise Security.

5. Создайте резервную копию строки поиска, включая KV Store. Процесс обновления не создает резервную копию существующей установки перед обновлением. См. «Резервное копирование KV Store» для получения инструкций о том, как создать резервную копию хранилища KV в строке поиска.

**Рекомендации по обновлению безопасности Splunk Enterprise Security**

Обновите платформу Splunk и Splunk Enterprise Security в одном и том же окне. Ознакомьтесь с системными требованиями Splunk Enterprise, чтобы проверить, какие версии Splunk Enterprise Security и Splunk Enterprise поддерживаются друг другом.

1. Обновите Splunk Enterprise до совместимой версии. См. «Обновление распределенной среды Splunk Enterprise в *Руководстве по установке Splunk Enterprise*.

2. Обновите версии платформы Splunk.

3. Обновите систему безопасности Splunk Enterprise.

4. Изучите, обновите и разверните надстройки.

Обновление Enterprise Security, развернутое в кластере поиска, является многоступенчатым процессом. Рекомендуемая процедура подробно описана в разделе «Обновление Enterprise Security в кластере строки поиска».

**Примечания к обновлению**

• Обновление не будет выполнено, если сервер развертывания управляет приложениями или надстройками, входящими в пакет Enterprise Security. Перед запуском обновления удалите файл deploymentclient.conf, содержащий ссылки на сервер развертывания, и перезапустите службы Splunk.

• Обновление наследует любые изменения конфигурации и файлы, сохраненные в путях приложений /local и /lookups.

• Обновление поддерживает локальные изменения в навигации по меню.

• После обновления изменения конфигурации, унаследованные в процессе обновления, могут повлиять или переопределить новые параметры. Используйте панель мониторинга конфигурации ES, чтобы просмотреть параметры конфигурации, которые могут конфликтовать с новыми конфигурациями. См. «Конфигурации ES» в *Руководстве пользователя*.

• Процесс обновления зарегистрирован в

$SPLUNK\_HOME/var/log/splunk/essinstaller2.log

• Splunk Web может не запускаться, если у вас есть папки модулей AdvancedXML из версий Enterprise Security до 4.0.х. Вручную удалите эти файлы. Например, удалите

$SPLUNK\_HOME/etc/apps/SA-Utils/appserver/modules/SOLNLookupEditor.

Обновление заметок для надстроек, включенных в Splunk Enterprise Security:

• Процесс обновления перезаписывает все предыдущие или существующие версии приложений и надстроек.

• Обновление не перезаписывает более новую версию приложения или надстройки, установленных в вашей среде.

• Приложение или надстройка, которое было отключено в предыдущей версии, будет оставаться отключенным после обновления.

• Обновление отключает устаревшие приложения или надстройки. Устаревшее приложение или надстройка должно быть удалено вручную из Enterprise Security. После обновления в сообщениях отображается предупреждение, позволяющее идентифицировать все устаревшие элементы.

**Изменения в надстройках**

Список надстроек, включенных в эту версию Enterprise Security, см. в разделе «Специфичные для технологии надстройки, поставляемые с Enterprise Security».

***Обновление распределенных надстроек***

Splunk Enterprise Security включает последние версии существующих надстроек, на момент выхода данной версии.

В состав Splunk Enterprise Security входит копия последних надстроек. При обновлении Enterprise Security просмотрите все надстройки и разверните обновленные надстройки для индексаторов и серверов по мере необходимости. Процесс установки Enterprise Security не позволяет автоматически обновлять или переносить любые конфигурации, развернутые для индексаторов или серверов. См. раздел «Развертывание надстроек, входящих в состав Splunk Enterprise Security».

Вы должны перенести любые настройки, сделанные в предыдущие версии надстройки, вручную.

**Обновление системы Splunk** **Enterprise Security**

В этом разделе описывается, как обновить Splunk Enterprise Security в локальной поисковой строке с версии 4.5.x или более поздней версии до последней версии. Клиентам Splunk Cloud необходимо обратиться в службу поддержки Splunk для координации обновлений для Enterprise Security.

**Шаг 1. Изучите тему планирования**

1. Обзор процесса обновления и предварительных условий см. в разделе «Планирование обновления» в данном руководстве.

2. Перед обновлением выполните полную резервную копию строки поиска.

Чтобы отказаться от обновления, вы должны восстановить предыдущую версию Splunk Enterprise Security из резервной копии.

**Шаг 2. Загрузите Splunk Enterprise Security**

1. Откройте splunk.com и войдите в систему с вашим ID Splunk.com. Вы должны быть лицензированным клиентом Enterprise Security для загрузки продукта.

2. Загрузите последний продукт Splunk Enterprise Security.

3. Выберите «**Download**» и сохраните файл продукта Splunk Enterprise Security на свой рабочий стол.

4. Войдите в строку поиска Enterprise Security как администратор.

**Шаг 3. Установите последнюю версию Splunk Enterprise Security**

1. На странице поиска Splunk Enterprise выберите «**Apps > Manage Apps**» и выберите «**Install App from File**».

2. Выберите файл продукта Splunk Enterprise Security.

3. Нажмите «**Choose file**» и выберите файл продукта Splunk Enterprise Security.

4. Нажмите «**Upgrade app**», чтобы перезаписать установленную версию Splunk Enterprise Security.

5. Нажмите «**Upload**», чтобы начать установку.

6. При появлении запроса перезапустите Splunk Enterprise.

Если вы не запускаете процедуру установки сразу после завершения загрузки файла, Enterprise Security отображает ошибки.

**Шаг 4. Настройка Splunk Enterprise Security**

После того, как Splunk Web вернется после перезагрузки, настройте Splunk Enterprise Security.

1. Нажмите «**Continue to app setup page**», чтобы запустить настройку ES.

2. Нажмите «**Start**».

3. На странице «**Splunk Enterprise Security Post-Install Configuration**» отображается статус обновления, когда оно осуществляется по этапам.

4. Выберите опцию «исключить выбранные надстройки из установки» или отключите их.

Когда настройка будет завершена, страница предложит вам перезапустить службы платформы Splunk.

5. Нажмите «**Restart Splunk**», чтобы завершить установку.

**Шаг 5. Проверка обновления**

Процесс обновления Splunk Enterprise Security завершен. Объекты, отключенные во время процесса обновления, будут автоматически активированы.

1. В строке меню Enterprise Security выберите «**Audit > ES Configuration Health**».

2. Просмотрите возможные конфликты и измените настройки по умолчанию. См. «Конфигурация ES» в *Руководстве пользователя*.

3. Очистите кеш браузера, который вы используете для доступа к Splunk Web, чтобы убедитесь, что после обновления вы получаете доступ к новой версии Splunk Web. Если вы не очистите кеш браузера, некоторые страницы могут не загрузиться.

Splunk регистрирует обновление в $SPLUNKHOME$/var/log/splunk/essinstaller2.log

**Рекомендации по обновлению версии**

***После обновления до версии 5.1.0***

Вручную удалите файл

$SPLUNK\_HOME/etc/apps/splunk\_instrumentation/default/data/ui/views/search.xml.

После удаления файла выполните одно из нижеприведенных действий:

• Обновите Splunk Web:

http(s)://yoursplunkurl.com:8000/en-US/debug/refresh?entity=data/ui/views

• Обновите splunkd:

http(s)://yoursplunkurl.com:8089/services/data/ui/views/\_reload

***После обновления с версии до 5.0.x***

• Выберете «**Edit Lookups**» еще раз. Поскольку разрешение «**Edit Lookups**» теперь включает дополнительные возможности, разрешение по умолчанию не проверяется. У ролей все еще есть функция **edit\_lookups**. См. раздел «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*

• Активируйте поиск **Access - Geographically Improbable Access - Summary Gen**, чтобы просмотреть данные на витрине «**Geographically Improbable Access**» на панели мониторинга «**Access Anomalies**» или существенных событиях, созданных в результате поиска корреляционных данных с использованием **Geographically** **Improbable Access Detected**.

***После обновления с версии до 4.1.x***

• Конфигурации редактора корреляций могут быть несовместимы с настройками предварительного обновления, если процесс переноса поиска все еще работает.

Найдите внутренний индекс для поиска успешно перенесенных запросов и просмотрите состояние операции переноса.

index=\_internal sourcetype=configuration\_check

file="confcheck\_es\_modactions\*" migrated

• Включенные поиски корреляции, которые не настроены для создания существенных событий, возвращаются к созданию существенных событий.

Например, поиск корреляции, который по умолчанию создал существенное событие и модификатор риска, который вы настроили для создания только модификатора риска, после обновления создаст модификатор риска и существенное событие.

1. Перед обновлением обратите внимание на поддерживаемые запросы корреляции, которые не создают существенные события, используя следующий поиск.

| rest splunk\_server=local count=0 /services/saved/searches search="name=\"\*-Rule\"" | where disabled=0 AND

'action.summary\_index'=0 | table 'eai:acl.app',title

2. После завершения обновления обновите отслеживаемые запросы корреляции, чтобы поисковые запросы больше не создавали существенные события.

**Тестирование обновления и настройка Splunk Enterprise Security**

Перед выполнением полного обновления вы можете протестировать обновление и настройку Splunk Enterprise Security. Вы должны выполнить шаги 1-3, прежде чем вы сможете выполнить следующие шаги.

1. В Splunk Web откройте приложение «Поиск и отчетность» (Search and Reporting).

2. Введите следующий поиск, чтобы выполнить предварительный запуск обновления и настройки.

|essinstall --dry-run

3. Вы можете использовать дополнительные параметры для указания надстроек для установки, пропустить установку или отключиться после установки.

|essinstall --install-ta <ta-name>+ --skip-ta <ta-name>+ --disable-ta <ta-name>+

Укажите имя надстройки для установки, пропуска или отключения или используйте \* в качестве подстановочного знака. Используйте +, чтобы указать несколько надстроек для установки.

**Обновление системы Splunk Enterprise Security в кластерной среде строки поиска**

**Обновление Splunk Enterprise Security в кластере строки поиска**

Прежде чем обновлять кластер строки поиска Splunk Enterprise Security, изучите данные инструкции и порядок действий.

1. Подготовьте промежуточную версию.

2. Обновите экземпляр промежуточной версии до последней версии.

3. Перенесите обновленную версию в производственную функцию развертывания.

4. Разверните изменения для элементов кластера.

5. Подтвердите конфигурацию в кластере поиска.

Предыдущие версии данных инструкций и могли привести к тому, что после разворачивания приложений по умолчанию, включенных в Splunk Enterprise, вы разворачивали приложения поисковым партнерам

с помощью функции развертывания. Развертывание приложений по умолчанию, таким образом, не рекомендуется.

Если у вас возникли проблемы с развертыванием в результате этой неправильной конфигурации, перенесите параметры установки на новый кластер развертывания и поиска, аналогичный шагам для переноса автономной строки поиска в кластер поиска. См. «Перенос существующую строку поиска в кластер поиска» на этой странице.

***Рекомендации***

• Изучите надстройки, включенные в пакет Splunk Enterprise Security.

• При необходимости обновите Splunk Enterprise до последней версии, совместимой с текущей версией Splunk Enterprise Security.

♦ Для совместимых версий см. Системные требования Splunk Enterprise.

♦ Инструкции по обновлению Splunk Enterprise см. в разделе «Обновление кластера поиска» в *Руководстве по распределенному поиску* Splunk Enterprise.

***Подготовка промежуточной версии***

Перед обновлением вам необходимо сравнить копию Splunk Enterprise Security с развертыванием последней версии. Вы можете сделать это, выполнив обновление на промежуточной версии. Если у вас есть тестовая версия или QA в среде Splunk, содержащие только установленный Splunk Enterprise, вы можете использовать эту версию для настройки.

1. Подготовьте промежуточную версию Splunk Enterprise для установки обновления. Не связывайте версию с индексаторами или поисковыми узлами.

2. Скопируйте приложения в путь версии функции развертывания etc/shcluster/apps для пути промежуточной версии etc/apps

Например, тип функции развертывания: scp -r ~/etc/shcluster/apps

<staging\_machine>:~/etc/

Если развертывание включает приложения по умолчанию, такие как приложение поиска, удалите их из функции развертывания, прежде чем копировать папку в промежуточную версию.

Копия Splunk Enterprise Security для функции развертывания включает параметры конфигурации, которые развертываются в кластере поиска. Копия не включает изменения объекта знаний среды, реплицированные между узлами кластера строки поиска.

***Обновление промежуточной версии до последней версии***

1. Выполните шаги с первого по четвертый касательно процесса Обновление Splunk Enterprise Security.

2. Изучите панель мониторинга ES Configuration, чтобы определить изменения в конфигурациях и настройках между развернутой версией и последней версией Splunk Enterprise Security.

Установщик автоматически отключает устаревшие приложения или надстройки. Предупреждение отображается в сообщениях промежуточной версии и идентифицирует все устаревшие элементы.

Вы должны вручную удалить устаревшее приложение или надстройки из обновленной версии Enterprise Security.

***Перенос обновленной установленной ES в процессе развертывания***

Переместите приложения, содержащие Splunk Enterprise Security, из промежуточной версии в функцию развертывания.

1. В промежуточной версии скопируйте приложения, SA, DA и TA, связанные с Splunk Enterprise Security Suite, из справочника $SPLUNK\_HOME/etc/apps в справочник $SPLUNK\_HOME/etc/shcluster/apps в функцию развертывания.

1. Не копируйте устаревшие приложения или надстройки, которые вы отметили во время обновления при установке.

2. Не копируйте приложения по умолчанию, такие как поиск, запуск или запуск приложений.

Не копируйте приложения в справочнике $SPLUNK\_HOME/etc/apps, потому что вы не обновляете и развертываете приложения, входящие в состав Splunk Enterprise.

***Развертывание изменения для элементов кластера***

1. В функции развертывания разверните Enterprise Security с помощью -preserve-lookups true, чтобы сохранить содержимое файла справочника, сгенерированное в элементах кластера поиска. См. «Развертывание комплекса конфигурации» в разделе *Распределенный поиск*.

Дополнительную информацию об использовании этого параметра см. в разделе «Поддержка файлов справочника в обновлениях приложений» в *Руководстве по распределенному поиску* Splunk Enterprise.

***Проверка конфигурации в кластере поиска***

После того, как вы распределите копию Enterprise Security для функции развертывания на элементы кластера поиска, используйте панель мониторинга конфигурации ES, чтобы сравнить

объекты знаний, связанные с кластерами, с последней версией Enterprise Security.

1. Войдите в строку поиска кластера Splunk Web.

2. Откройте Enterprise Security.

3. В строке меню Enterprise Security выберите **Audit > ES Configuration Health**.

4. Просмотрите возможные конфликты и измените настройки по умолчанию.

См. раздел «Конфигурация системы ES» в *Руководстве по использованию Splunk Enterprise Security*.