Действия после установки НАЙС ОС

После завершения установки НАЙС ОС, администратор должен выполнить ряд важных шагов для обеспечения безопасности и функциональности системы. Не все функции безопасности активированы по умолчанию, поэтому необходимо настроить систему в соответствии с политиками безопасности вашей организации и специфическими задачами, которые будет решать сервер. Рассмотрим основные действия, которые следует выполнить после установки:

Основные шаги после установки

- **Настройка мониторинга событий безопасности:**
  - Определите перечень событий безопасности, которые необходимо отслеживать, такие как попытки несанкционированного доступа, изменения в конфигурации системы и другие важные события.
- **Настройка реакций на критические события:**
  - Определите меры, которые система должна предпринимать при обнаружении критических событий, например, уведомление администратора, блокировка учетной записи или запуск других защитных мер.
- **Обеспечение целостности данных аудита:**
  - Настройте систему для предотвращения потери или изменения данных аудита, используя защищенные методы хранения и передачи данных.
- **Защищенная передача данных аудита:**
  - Убедитесь, что передача данных аудита осуществляется по защищенным каналам, таким как SSL/TLS, для предотвращения несанкционированного доступа и модификации.
- **Создание учетных записей и групп:**
  - Создайте пользователей, группы и роли, распределяя права доступа в соответствии с функциональными обязанностями и необходимыми полномочиями.
- **Настройка прав доступа:**
  - Установите права доступа к новым каталогам и файлам, чтобы ограничить доступ только авторизованным пользователям.
- **Управление установкой и запуском программного обеспечения:**
  - Определите правила установки и запуска программ, ограничив возможность использования неавторизованных приложений и компонентов.
- **Настройка механизмов аутентификации и авторизации:**
  - Настройте используемые методы аутентификации и авторизации, установите сроки действия учетных записей и паролей, а также требования к их безопасности.
- **Создание резервных копий:**
  - Организуйте регулярное создание резервных копий данных и системных настроек, а также проводите периодические проверки их работоспособности.
- **Синхронизация времени:**
  - Настройте систему на использование доверенных серверов точного времени для синхронизации системных часов, что важно для корректной работы журналов и событий.
- **Проверка целостности системы:**
  - Проводите регулярные проверки целостности важных данных и системных файлов, используя контрольные суммы и другие методы.
- **Организация отказоустойчивости:**

    - При необходимости, настройте отказоустойчивый кластер для обеспечения высокой доступности и надежности системы.
- **Настройка квот и приоритетов:**
    - Определите квоты на использование ресурсов и приоритеты для различных пользователей и групп, чтобы предотвратить злоупотребления и обеспечить справедливое распределение ресурсов.
- **Ограничение сеансов пользователей:**
    - Установите ограничения на длительность сеансов пользователей и количество одновременных подключений для повышения безопасности.
- **Настройка тайм-аута сеансов:**
    - Определите время бездействия, после которого сеанс пользователя будет автоматически заблокирован или завершен, чтобы минимизировать риски несанкционированного доступа.

Дополнительные рекомендации

- **Обновление системы:**
    - Регулярно проверяйте и устанавливайте обновления для операционной системы и установленных приложений, чтобы защитить систему от известных уязвимостей.
- **Настройка журналов событий:**
    - Настройте и регулярно проверяйте журналы событий для своевременного обнаружения и реагирования на инциденты безопасности.
- **Обучение пользователей:**
    - Проводите регулярное обучение пользователей по вопросам безопасности и правилам работы в системе, чтобы повысить их осведомленность и уменьшить риски человеческого фактора.
- **Мониторинг системы:**
    - Настройте системы мониторинга для отслеживания производительности, доступности и безопасности системы в режиме реального времени.

Эти действия помогут обеспечить безопасность, надежность и эффективность работы вашей системы НАЙС ОС, соответствуя требованиям политики безопасности вашей организации.