SYSTEM-ADMINS

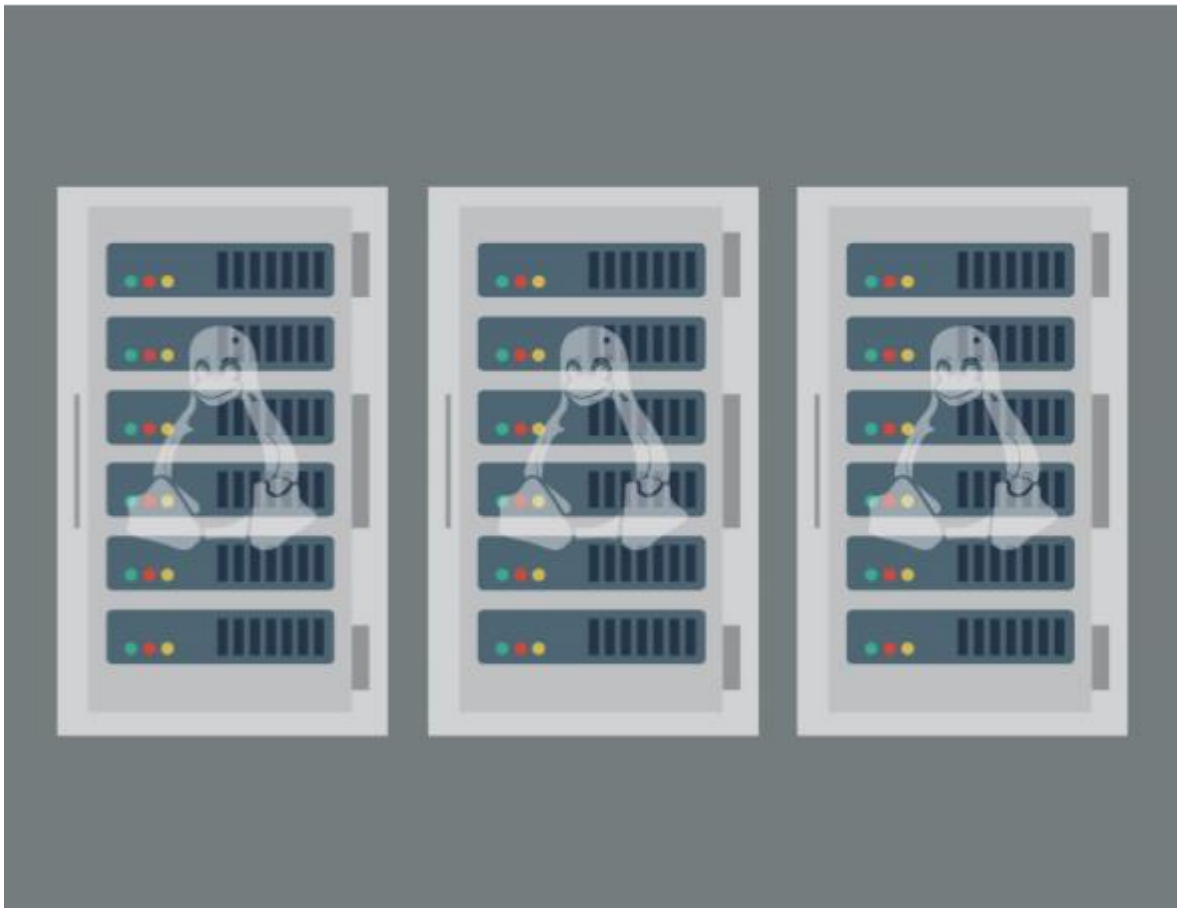
office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants

ПОДРУЧНАЯ КНИГА

10 ШАГОВ ПО КОНФИГУРИРОВАНИЮ НОВОГО СЕРВЕРА

КОНТРОЛЬНЫЙ СПИСОК

office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants



ВМЕСТО ВВЕДЕНИЯ

Вы установили свежий Linux сервер и… это будет стыдно, если с ним что-нибудь случится. Он может выполнять все, что нужно, «из коробки», но перед тем как отдать его в эксплуатацию мы рекомендуем выполнить 10 шагов, чтобы Вы были уверенны в том, что сервер сконфигурирован безопасно. Детали каждого из шагов могут меняться для различных дистрибутивов Linux, но концептуально они подходят к широкому кругу образов Linux и не только. Пройдя эти шаги на каждом вновь установленном сервере, Вы можете быть уверены, что Ваша инфраструктура имеет, по крайней мере, базовую защиту от наиболее распространенных атак.

office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants

1. **КОНФИГУРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.**

   Самая первая вещь, которую Вы должны сделать (если это конечно не часть установки ОС) – это изменить пароль учетной записи root. Это должно быть само собой разумеющимся, но может быть удивительно просто упущено из виду во время обычной установки сервера. Пароль должен состоять минимум из 8ми символов, использовать комбинации из заглавных и строчных букв, цифр и знаков. Также, если Вы планируете использовать локальные учетные записи, Вы должны настроить политики безопасности паролей, которые определяют их срок жизни, параметры блокировки, историю паролей и требование к их сложности. В большинстве случаев Вы должны полностью заблокировать учетную запись пользователя root и создать учетную запись непривилегированного пользователя с возможностью использования повышения прав (sudo).

2. **КОНФИГУРАЦИЯ СЕТИ.**

   Одна из базовых конфигураций, которую Вы должны сделать – это включить сетевое соединение, назначив серверу имя и IP адрес. Если вы хотите, чтоб клиенты всегда могли найти Ваш ресурс по одному и тому же адресу - используйте статический IP для Вашего сервера. Если Ваша сеть использует VLANы, учитывайте это для наиболее подходящего выбора IP адреса и сети, в которую будет подключен сервер. Если вы не используйте IPv6 – выключите его. Укажите имя сервера, его домен и DNS сервера. Желательно использовать два или более DNS сервера для обеспечения избыточности и отказоустойчивости. Потрудитесь проверить корректное разрешение доменных имен с помощью утилиты nslookup.

3. **УПРАВЛЕНИЕ ПАКЕТАМИ ПРИЛОЖЕНИЙ.**

   Конечно же, Вы устанавливаете новый сервер для некоторой конкретной цели. Убедитесь, что пакеты, которые Вы планируете установить, не являются частью дистрибутива. Это могут быть такие компоненты, как PHP, MongoDB, ngnix и др. Кроме того, любые посторонние пакеты, которые установлены в Вашей системе, должны быть удалены, чтобы уменьшить «след» сервера. Для упрощения дальнейшего управления все это должно быть сделано через «родной» инструмент управления пакетами, например yum или apt.

office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants

4. НАСТРОЙКА И УСТАНОВКА ОБНОВЛЕНИЙ

После того, как все нужные пакеты установлены на сервер, Вы должны убедиться, что все обновлено, в том числе ядро и пакеты, установленные по умолчанию. Кроме случаев, когда Вам требуется некоторая специфическая версия продукта, мы рекомендуем использовать последнюю стабильную версию ПО для обеспечения максимальной безопасности Вашей системы. Обычно инструмент управления пакетами предлагает последнюю поддерживаемую версию ПО. Если ПО, которое Вы используйте, поддерживает автоматическую установку обновлений с помощью стандартного инструмента управления пакетами, то рассмотрите эту возможность для применения в Вашей системе.

5. НАСТРОЙКА NTP

Настройте свой сервер на синхронизацию времени с NTP серверами в сети. Это могут быть внутренние серверы, если таковые имеются в Вашей инфраструктуре, или внешние сервера времени, которые доступны каждому. Важно предотвратить расхождения во времени сервера с реальным временем. Это поможет решить (или не допустить) большое количество проблем, в том числе связанных с аутентификацией, где разница во времени между сервером-клиентом и сервером аутентификации может послужить причиной отказа предоставления доступа. Кажется, что это простая настройка, но на самом деле – это критически важный кирпичик надежной инфраструктуры.

6. FIREWALL И IPTABLES

В зависимости от выбора дистрибутива iptables / firewall по умолчанию могут блокировать все соединения и требовать открытия необходимых портов для обеспечения работы Ваших сервисов. Но, несмотря на стандартную конфигурацию, Вы должны обязательно проверить и убедиться, что эти настройки подходят для Вашего решения. Помните, что всегда нужно придерживаться принципа выделения минимальных привилегий и открывать только те порты, которые Вам однозначно нужны для ПО, работающего на Вашем сервере. Если Ваш сервер находится за отдельно стоящим Брандмауэром (в каком либо виде), не забудьте сконфигурировать этот брандмауэр аналогично правилам, настроенным на сервере.

office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants

7. БЕЗОПАСНОСТЬ SSH

SSH - это главный способ удаленного доступа для серверов Linux, таким образом он должен быть достаточно защищен. Необходимо отключить возможность удаленного подключения root через SSH, даже если вы отключили этот аккаунт. Это делается на всякий случай. Если по каким либо причинам учетная запись root станет доступна на сервере, сервер останется неуязвим удаленно. Если у Вас есть ограниченный набор клиентских IP, с которых будет выполняться соединение, Вы также можете ограничить SSH некоторыми диапазонами IP адресов. При желании Вы можете изменить порт SSH по умолчанию, но, если честно, простое сканирование выявит новый порт для любого, кто захочет его найти. Наконец, вы можете отключить аутентификацию по паролю и использовать аутентификацию, основанную на сертификатах, чтобы еще больше снизить угрозу взлома через SSH.

8. НАСТРОЙКА ДЕМОНОВ.

Вы уже привели в порядок пакеты ПО, которое используется на сервере, но также важно установить нужные приложения в автозагрузку при старте системы. Убедитесь, что все ненужные сервисы выключены. Одним из ключевых моментов обеспечения безопасности сервера является уменьшение поверхности атаки. Таким образом, запущенными нужно оставить только те демоны, которые реально используются для работы сервера. После того как это будет сделано, оставшиеся рабочие сервисы должны быть максимально защищены, чтобы обеспечить устойчивость к атакам.

9. SELINUX И ПОСЛЕДУЮЩИЕ НАВОРОТЫ

Если вы когда-нибудь использовали дистрибутив Красной Шапочки☺, Вы наверняка сталкивались с SELinux – утилитой ядра, которая защищает систему от различных операций. SELinux – отлично работает против неавторизованного доступа и несанкционированного использования ресурсов системы. Но она также отлично мешает приложениям нормально работать, поэтому протестируйте Вашу финальную конфигурацию с включенным SELinux и проверьте логи, чтобы убедиться, что

ничего нужного не было заблокировано. Помимо этого Вы должны изучить возможности защиты используемых Вами приложений, таких как MySQL или Apache. Наверняка, у каждого из них есть свои «Best Practices», которым стоит следовать.

office@system-admins.ru
https://system-admins.ru
Skype: vkarabedyants

10. ЛОГИРОВАНИЕ.

Напоследок включите нужный Вам уровень логирования событий в системе. Вы должны убедиться, что у Вас есть достаточно ресурсов для корректной работы в таком режиме. Поскольку в дальнейшем, вероятно, Вы будете поддерживать этот сервер, то сейчас самое время обеспечить себе удобство решения проблем и построить правильную структуру логирования. Большинство ПО имеет настраиваемую систему фиксирования событий, но Вы должны самостоятельно пройти путем проб и ошибок, чтобы выбрать правильный баланс между недостаточностью и избытком информации для мониторинга работы системы. Есть достаточно много сторонних систем и утилит сбора логов, которые полезны в решении различных задач, начиная от агрегирования и заканчивая визуализацией. Но каждая инфраструктура требует индивидуального подхода к своим потребностям, зная их, Вы можете подобрать именно те утилиты, которые максимально удовлетворят эти потребности.

ВЫВОДЫ.

Каждый из перечисленных шагов может занять некоторое время на выполнение, особенно если Вы делаете это в первый раз. Но если каждый раз, при установке нового сервера, Вы будете выполнять эту процедуру начальной конфигурации, Вы будете уверены, что сервера в Вашей инфраструктуре устойчивы к уязвимостям. Невыполнение хотя бы одного из шагов может привести к серьезным последствиям, в случае если Ваш сервер окажется объектом атаки. Однако даже если Вы сделаете все вышеперечисленное - это не гарантирует полной безопасности, поскольку утечки данных случаются. Но соблюдение этих простых правил значительно усложняет взлом Вашего сервера и требует достаточной степени мастерства, для того, чтобы это сделать.